Учреждение образования
«Академия Министерства внутренних дел Республики Беларусь»

ТЕОРЕТИЧЕСКИЕ И ПРИКЛАДНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Материалы
Международной
научно-практической конференции
(Минск, 19 июня 2014 г.)

Минск
Академия МВД
2015

УДК 004:34
ББК 32.81
Т33

Т33 **Теоретические и прикладные аспекты информационной безопасности** : материалы Междунар. науч.-практ. конф. (Минск, 19 июня 2014 г.) / учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь» ; редкол.: В.Б. Шабанов (отв. ред.) [и др.]. – Минск : Акад. МВД, 2015. – 417, [3] с.

ISBN 978-985-427-890-2.

Рассматриваются вопросы, посвященные теоретическим и прикладным проблемам информационной безопасности, анализу перспективных методологических подходов к ее решению, вопросам создания и внедрения систем защиты информации в информационных системах правоохранительных органов, а также подготовке специалистов в сфере защиты информации.

Для научных работников, занимающихся проблемами информационной безопасности, сотрудников правоохранительных органов, а также специалистов в области защиты информации и подготовки кадров.

УДК 004:34
ББК 32.81

ISBN 978-985-427-890-2

ПРИВЕТСТВЕННЫЕ СЛОВА К УЧАСТНИКАМ КОНФЕРЕНЦИИ

Уважаемые участники и организаторы Международной научно-практической конференции «Теоретические и прикладные аспекты информационной безопасности»!

Разрешите передать вам самые теплые пожелания успешной работы от лица руководства Министерства внутренних дел Республики Беларусь.

Вопросы, вынесенные на обсуждение участников конференции, связаны с укреплением безопасности функционирования информационных систем как на национальной уровне, так и на уровне информационного пространства стран СНГ. Перечень обсуждаемых вопросов охватывает широкий спектр актуальных проблем. Это анализ перспективных методологических подходов к проблеме информационной безопасности и выработка адекватных средств по ее решению, предложения по совершенствованию законодательной базы информационного сообщества, особенности развития этой отрасли в наших странах, обсуждение технических вопросов информационной безопасности, включая проблемы криптографии и методы защиты информации, обмен практическим опытом создания и внедрения эффективных систем защиты информации и обсуждение инновационных подходов в подготовке специалистов в сфере информационной безопасности.

Нельзя не отметить высокую представительность научно-практической конференции. В ней принимают участие практически все заинтересованные стороны, представители государственных организаций, ведущих учебных и научных учреждений стран СНГ. Это достаточно красноречиво говорит о том, что данная конференция признается важным элементом международного взаимодействия в сфере обеспечения безопасности информационных технологий в наших государствах.

Мы осознаем, что современные информационно-коммуникационные технологии являются серьезным инструментом укрепления мира, безопасности, стабильности в государстве и организации эффективного взаимодействия на национальном и международном уровне. Информационные технологии существенно расширяют возможности повышения эффективности государственного управления, создают новое измерение качества жизни человека.

В то же время всех нас объединяет понимание того, что для продолжения интенсивного развития информационной сферы наших стран необходимо обеспечить эффективное противодействие угрозам использования современных информационных технологий в целях нарушения международного мира и национальной безопасности, совершения различных преступлений (и не только компьютерных), распространения социально опасной информации (террористической и криминальной направленности) в сетях общего пользования.

Мы понимаем, что добиться решительного перелома в противодействии данным угрозам еще не удалось, хотя определенные позитивные тенденции в этой области имеются. И в этой связи данная научная конференция может выступать еще одним элементом в общем фундаменте международной и национальной информационной безопасности.

Желаю вам, дорогие участники конференции, успехов в решении поставленных задач, успешной и результативной работы в достижении целей обеспечения безопасности информации.

Заместитель министра
внутренних дел Республики Беларусь
А.А. Кобрусев

Уважаемые участники и гости конференции!

От имени профессорско-преподавательского состава Академии Министерства внутренних дел Республики Беларусь, а также от себя лично сердечно приветствую вас на белорусской земле в городе Минске.

Международная научно-практическая конференция по проблемам информационной безопасности проводится в Беларуси уже третий раз. В ней принимают участие лучшие представители науки и практики в области защиты информации из Российской Федерации, Украины, Республики Казахстан и Беларуси, работники предприятий и организаций известные в нашей стране и за ее пределами. На данной научной площадке обмениваются опытом использования современных технических и организационных средств защиты информации и борьбы с компьютерной преступностью, создания и внедрения систем обеспечения безопасности критически важных объектов информатизации. Участники форума эффективно анализируют инновационные подходы в подготовке специалистов в сфере защиты информации, исследуют актуальные вопросы информационной безопасности в деятельности учреждений уголовно-исполнительной системы. Анализ перспективных методологических подходов к проблеме информационной безопасности и выработка адекватных средств по ее решению позволили обеспечить качественное повышение квалификации сотрудников правоохранительных органов, изучить практические наработки в области создания и внедрения систем защиты информации в информационных системах и распространить передовой опыт, обменяться мнениями о ситуации в области международно-правового регулирования в сфере защиты информации и борьбы с уголовно наказуемыми деяниями против информационной безопасности.

В настоящее время информационные технологии активно внедряются во все сферы жизни, что приводит к значительному расширению спектра как внешних, так и внутренних угроз безопасности информации. Плодотворный научный анализ этих проблем позволит выработать соответствующие практические рекомендации и послужит динамичному развитию информационных технологий в наших странах, укреплению сотрудничества и оказанию помощи друг другу в решении проблем, имеющихся в области защиты информации. В этой связи сегодняшняя конференция является важным этапом в развитии сотрудничества в области обеспечения информационной безопасности.

Выражаю уверенность, что материалы Международной научно-практической конференции «Теоретические и прикладные аспекты информационной безопасности» станут важным ресурсом для государственных органов Республики Беларусь и стран СНГ при подготовке предложений по реализации ими своих полномочий в области обеспечения безопасности в информационной сфере.

Желаю всем участникам конференции успехов и продуктивной работы!

Начальник Академии МВД Республики Беларусь
кандидат юридических наук, доцент
В.В. Бачила

Уважаемые участники конференции!

На современном этапе развития нашего социума информационная сфера превращается в системообразующий фактор жизни людей, обществ и государств. Усиливается роль и влияние средств массовой информации и глобальных коммуникационных механизмов на экономическую, политическую и социальную ситуацию. Информационные технологии нашли широкое применение в управлении важнейшими объектами жизнеобеспечения, которые становятся более уязвимыми перед случайными и преднамеренными воздействиями. Происходит эволюция информационного противоборства как новой самостоятельной стратегической формы глобальной конкуренции. Распространяется практика целенаправленного информационного давления, наносящего существенный ущерб национальным интересам. Таким образом, значение защиты информации в обеспечении национальной безопасности государства и его успешного социально-экономического развития непрерывно возрастает.

Следует констатировать, что эффективное противодействие преступлениям против информационной безопасности невозможно без широкой международной координации политики в данной области. Универсальный подход к анализу задач защиты информации, нацеленность на рассмотрение вопросов, имеющих высокую практическую значимость, способствуют утверждению репутации конференции «Теоретические и прикладные аспекты информационной безопасности» как важной инициативы по обеспечению безопасности Республики Беларусь и стран СНГ.

Состав участников форума в текущем году подтверждает это. В ходе пленарных заседаний и «круглых столов» конференции планируется представить более 100 докладов по широкому перечню проблем обеспечения безопасности в информационной сфере. Представители Следственного комитета Республики Беларусь поделятся опытом следственной работы в обозначенной сфере и предложениями относительно перспектив данной деятельности. Надеемся, что усиление нашего сотрудничества в области использования потенциала современных информационных и коммуникационных технологий пойдет на благо человека, на повышение эффективности противодействия общим угрозам безопасности информационной сферы. Думается, что опыт участников конференции поможет выработать рекомендации для совершенствования совместной деятельности в информационной сфере и в целях обеспечения безопасности информационного пространства наших стран.

Удачной вам работы!

Заместитель председателя
Следственного комитета Республики Беларусь
В.А. Гайдученок

Уважаемые коллеги!

Приветствуем вас от имени Секретариата Совета Межпарламентской ассамблеи государств – участников СНГ и Секретариата Парламентской ассамблеи Организации Договора о коллективной безопасности.

Многие годы наши ассамблеи осуществляют сотрудничество высших законодательных органов государств СНГ и ОДКБ и разработку региональных стандартов регулирования отношений по обеспечению безопасности стремительно развивающейся информационной сферы.

Высоко ценим вклад и усилия в этом процессе специалистов Академии МВД Республики Беларусь, которые совместно с учеными Института государства и права РАН, Санкт-Петербургского института информатики и автоматизации РАН и Института национальной безопасности Республики Беларусь находят ответы на сложнейшие вопросы.

Искренне верим в то, что установившаяся тесная кооперация законодателей Содружества, представителей компетентных органов и учреждений науки позволит и впредь успешно решать встающие общие задачи.

Желаем организаторам и участникам конференции успехов в достижении поставленных целей и задач.

Генеральный секретарь
Совета Межпарламентской ассамблеи
государств – участников СНГ
А.И. Сергеев

Ответственный секретарь Парламентской ассамблеи
Организации Договора о коллективной безопасности
П.П. Рябухин

Уважаемые коллеги!

Приветствую организаторов, участников и гостей Международной научно-практической конференции «Теоретические и прикладные аспекты информационной безопасности» в столице республики Беларусь городе-герое Минске накануне памятной для наших народов даты – начала Великой Отечественной войны.

События последних месяцев наглядно показали исключительную роль, которую приобрели информация, информационно-коммуникационные технологии в мировой политике, став, по сути, инструментом ведения боевых действий. Обеспечение информационной безопасности, уже очевидно, нельзя сводить лишь к технологической защите информационных ресурсов, оно на различных уровнях и в разных аспектах приобретает черты противоборства и должно стать непрерывным процессом.

Желаю всем участникам плодотворной работы и уверен, что конференция будет способствовать новому пониманию проблем информационной безопасности, внесет существенный вклад в достижение информационного суверенитета и укрепление национальной безопасности наших государств, способствуя дальнейшему развитию интеграционных процессов на евразийском пространстве.

Директор Санкт-Петербургского института
информатики и автоматизации
Российской академии наук
член-корреспондент РАН
Р.М. Юсупов

Уважаемые участники конференции!

Разрешите мне от ученого совета, руководства Академии ФСИН России, всего личного состава и себя лично поздравить вас с началом работы международной научно-практической конференции «Теоретические и прикладные аспекты информационной безопасности».

Информационные технологии, безусловно, играют сегодня очень важную роль в современном обществе, но наряду с большим количеством положительных моментов возникает ряд проблем, связанных с информационной безопасностью. Все последние мировые события, развитие общества показывают, что информационные технологии, стоящие сегодня на вооружении различных правоохранительных органов и в целом государств, постоянно развиваются. И оставлять без внимания такие проблемы, как информационная безопасность нельзя. Федеральная служба исполнения наказаний Российской Федерации уделяет большое внимание проблемам информационной безопасности. В Академии ФСИН России также информационная безопасность является предметом различных научных исследований, научно-практических семинаров и конференций. Мы уверены, что наша совместная работа и сегодняшняя международная конференция будут построены в форме открытого диалога, будут обозначены проблемы и найдены пути решения актуальных вопросов. А рекомендации, принятые по итогам конференции, станут основой для последующих исследований и принятия практических рекомендаций, подготовки различных учебных пособий, монографий, которые будут использованы в практической деятельности и в образовательном процессе как Беларуси, так и Российской Федерации. Желаем всем участникам конференции плодотворной работы и новых результатов и свершений.

Начальник Академии ФСИН России
генерал-майор внутренней службы
кандидат юридических наук, доцент
А.А. Крымов

РАЗДЕЛ 1

АКТУАЛЬНЫЕ ПРАВОВЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И БОРЬБЫ С КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТЬЮ

УДК 34:004.056

И.Л. Бачило

ПРОЕКТ МОДЕЛЬНОГО ЗАКОНА «ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

По плану работ Секретариата Межпарламентской ассамблеи государств – участников СНГ (далее – МПА СНГ) в области совершенствования правового обеспечения информационной безопасности предусмотрена работа по изменению и дополнению модельного закона 2005 г. «Об информатизации, информации и защите информации». К настоящему времени эта работа близка к завершению. Доклад предусматривает сообщение о ходе выполнения этого задания, включая обзор учитываемых факторов за время действия названного закона; необходимые требования к его совершенствованию; пояснения структуры, содержания и названия предлагаемого проекта закона и вывод по завершении данного этапа работы.

1. В процессе выполнения задания учитывались следующие обстоятельства: опыт развития информационного общества за последние 10 лет; состояние национального законодательства государств – участников СНГ и влияние его на безопасность общества, государства, человека; рост вала законов и других НПА за это время; вызовы общества к регулированию информационного взаимодействия всех видов субъектов в новых условиях; возрастание значения открытой информации, обострение проблем защиты результатов интеллектуального творчества (защита патентов, национального программного обеспечения в национальных ИКТ) и др.

2. Опыт информационного законодательства по вопросам информационной безопасности.

Особо следует отметить опыт законодательства в области информатизации Республики Казахстан и Республики Беларусь. Необходимо учитывать и перенастройку российского базового закона «Об информации, информационных технологиях и о защите информации» 2006 г.,

в результате которой были утрачены позиции по регулированию информационных ресурсов, процессу информатизации, ориентация на количественный учет результатов использования ИТ в социальной сфере жизни общества.

3. Что изменилось на последние 10 лет ?

Наиболее актуальными за этот период становятся вопросы качества функционирования института «Электронного правительства» и его роли в информатизации всей системы деятельности органов государственной власти органов местного самоуправления и управления. В этой связи необходимо обратить внимание на состояние инфраструктуры ИКТ и ее управляемость со стороны органов исполнительной власти – министерств информации, министерств информационных технологий, министерств связи и массовых коммуникаций и структур с другими названиями и соответственно с определенными функциями.

Необходимо отметить, что эти структуры за обозреваемый период превратились в полноценную отрасль экономики государства и, естественно, живут по законам рынка. Создается объективно обусловленный разрыв между инфраструктурой ИКТ и функциональной информационной инфраструктурой системы органов исполнительной власти. Функциональная информационная инфраструктура системы органов исполнительной власти не может быть ограничена работой по устройству ИС, специально организованными департаментами, управлениями и т. п. Информатизация – это постоянная и непрерывная деятельность всех администраций и ее подразделений на основе использования потенциала ИКТ. В этих условиях стоит вопрос об уточнении направлений деятельности «Электронного правительства» и координации функций министерств ИКТ и функций всего аппарата исполнительной власти. Эта область не может ограничиваться только функциями предоставления информации о деятельности органов государственной власти местного управления, функциями предоставления публичных услуг.

В этой связи важно обратить внимание на состав прав субъектов в информационной сфере (для России п. 4 ст. 29 Конституции и аналогичных законов других государств – участников СНГ), где в системе прав и обязанностей вопросу использования информации пока не уделено должного внимания. А это основной источник в процессе умышленного и неумышленного наращивания конфликтов, угроз и снижения уровня информационной безопасности. На встрече Президента Российской Федерации с крупными интернет-компаниями в июне 2014 г. как раз и подчеркнуто значение связи борьбы с нарушениями использования ИКТ (борьбы с «пиратами») и основной целью информатизации. Снижать роль государства при этом нельзя!

4. В этих условиях роль базовых национальных законов и базового модельного закона СНГ значительно взрастает.

А) С позиций формирования, обновления и ответственности за использование информационного ресурса следует отметить два вопроса. Первый касается проблемы юридического оформления режима информационных ресурсов государства и всех иных субъектов. В этой связи надо обратить внимание на широкое использование термина «обладатель» в национальных законах. Обладателями информационного ресурса являются буквально все виды субъектов информационных и любых иных отношений. Но важно определение юридического основания обладания. К сожалению, действующие законы не уделяют этому внимания. Возникают неясности и конфликты между собственником информационного ресурса и его обработчиками при определении прав на использование этого ресурса. Практика работы «одного окна», многофункциональных центров, облачных технологий требует более внимательного оформления оснований для взаимодействия органов власти, граждан и собственниками ИТ-систем. Это касается и проблем обработки персональных данных и проблем работы со служебной и деловой информацией.

Б) Важнейшей проблемой при упорядочении законодательства является обеспечение информационной безопасности – безопасности самого ИКТ-ресурса и безопасности его применения в решении социальных, экономических, политических, культурных процессов в содружестве государств – участников СНГ как одного из видов международного регионального взаимодействия государств. Безусловно, определяющим моментом настоящего времени являются проблемы единого экономического пространства. Но нельзя забывать, что это основа решения всех социальных проблем.

Здесь важна ориентация на понимание природы и сути информационного общества. В течение 15 лет Институт государства и права РАН использует концепцию информационного общества как общества: гражданского, социального, демократического, правового. Это основные векторы развития информационного обществ и они должны поддерживаться в балансе и безопасности системно и комплексно. Это непременное условие развития и функционирования сильного государства.

В) Проблемы информационной безопасности не ограничиваются созданием условий для безопасности информационного и технологического ресурса. Сегодня эта проблема касается безопасности использования информации и сетевых коммуникаций в процессе взаимодействия всех категорий пользователей интернет-средой. Меняются методы работы в области обеспечения информационной безопасности. Совершается поворот от методов консервации путем «защиты» ИР и ИС от внешнего воздействия к более широкому фронту обеспечения безопасности в процессе использования этих ресурсов в обществе и в системе государственного управления. На первый план выходят вопросы борьбы с использование вредной информации для человека и институтов общества, влияния на сознание человека и всех форм его жизнеобеспечения, включая и систему государственной власти.

В этой связи обращаю внимание на понимание гражданского общества. ИГП РАН разработал и применяет модель, в которой определяющей силой является человек, индивид, семья, народ. На основе их правосознания и социальной активности создаются институты государственной власти и все институты общества, которые как институты гражданского общества с учетом уровня гражданственности мышления и поведения различных структур и институтов (законности, выборов, семьи, НКО, церкви и т. д.). Эти вопросы детально разработаны и показывают недостаток узкого понимания гражданского общества как взаимодействие в треугольнике государство – бизнес – гражданское общество, представленное исключительно НКО и правозащитными организациями, что ведет к противостоянию и конфронтации. Практика применения более широкого понимания гражданского общества все более находит реализацию не только в сознании масс, но и в деятельности управленческих структур каждого государства.

Г) Методы и средства обеспечения информационной безопасности должны соответствовать вызовам современного общества. Не допустить развития таких форм опасности и угроз, как информационные войны. Социологи и политологи считают, что уже идет новая информационная война. В любом случае для права и государства, для сообществ государств важно обеспечить пресечение такого широкого состояния самоуничтожения социума в целом. В повестку дня ставится вопрос о методах не только защиты, но и поиска форм отказа, воздержания, запрета от вредного для общества и человека использования информации в качестве современного оружия.

В свете сказанного встает вопрос о понимании сильного государства и роли права в гуманитарном аспекте, о поиске решений проблем обеспечения суверенитета каждого государства и более четких границ и правил реализации государственной национальной и международной юрисдикции в рассматриваемой области жизни общества. Считаю не очень удачной формулу «информационного суверенитета». Суверенитет является институтом в системе взаимодействия государств в международных отношениях и должен быть единым, не распыляться по отдельным направлениям. Задача информационной безопасности –

обеспечивать незыблемость государственного суверенитета в международных контактах с другими государствами, в том числе по вопросам информационной безопасности и борьбы с киберпреступлениями.

5. Об условиях обеспечения качества модельного закона сегодня.

Вызовы информационного общества к состоянию правового обеспечения информационных процессов и отношений субъектов в этих условиях ставят новые задачи в обеспечении эффективности действующего законодательства. А это, в свою очередь, повышает требования к модельным законам и их роли в гармонизации национального законодательства. Тот вариант модельного закона, который был принят в 2005 г., сегодня не соответствует таким требованиям. Нужен базовый закон, который отвечает на вопросы: кто, что делает, для чего и каким образом, чтобы упорядочить взаимодействие всех участников содружества независимых государств (СНГ) и, в известной степени, членов ОДКБ в формировании информационного общества и решении задач создания единого экономического пространства в Евроазиатском сотрудничестве государств.

Кроме выше упомянутых проблем на процесс выработки проекта нового базового закона МПА СНГ влияет нерешенность ряда методологически важных вопросов.

К таким вопросам относятся следующие:

1. Унификация терминов и их определений, используемых в информационном законодательстве, выделение из них правовых дефиниций, которыми могут руководствоваться законодатели всех участников СНГ. Это касается в первую очередь определений терминов: «информация», «информационные ресурсы», «правовой режим информационных ресурсов или основных требований при организации этого ресурса; однообразное понимание термина «информатизация». На очереди стоят вопросы обобщения опыта работы в этой области, отказ от закрепления терминов по каждому отдельному закону. Большой задел по этой проблеме создан специалистами.

2. Правовой режим информационных ресурсов, а также информационных технологий нуждается в установлении единых или сходных правил документирования информации; правил установления прав собственности на эти объекты и объекты интеллектуальной собственности (интеллектуального творчества); систематизацию ИР по доступу и использованию (включая ресурсы служебной, деловой информации, персональных данных); способы защиты ИР, ИТ, социальных сетей и их безопасного использования, способы противодействия распространению и использованию вредной для общества и человека информации.

3. Рассматривать процесс информатизации как процесс формирования информационного общества на основе сбалансированных моделей

информационного взаимодействия органов государственной власти и органов местного управления и самоуправления между собой, с гражданами и организациями, со всеми институтами гражданского общества и как процесс формирования и использования интегрированных ИС для участников СНГ.

4. Безопасность процессов информатизации рассматривать как противостояние монополизации в использовании ИТ и коммуникаций, как работу по созданию безопасного национального программного обеспечения, соответствующего целям и интересам государств – участников содружества и каждого человека.

5. Организацию работы по определению индикаторов оценки хода и результатов информатизации, отказ только от скалярных методов (оценки по числу используемых ИТ-средств и получаемых доходов) и усиление учета результатов и оценки качества преобразуемых методов работы в области управления делами государства, общества и населения. Заслуживает внимания опыт систематизации информационного законодательства и подготовка к его кодификации на основе согласованных методик. Первые шаги в этом направлении сделаны в концепции кодификации информационного законодательства Российской Федерации, подготовленной в ИГП РАН и обсужденной на международной конференции по этой проблеме в 2014 г. Проблемы информационной безопасности по этой концепции выделяются как «Суперинститут обеспечения информационной безопасности», включающий ряд институтов и субинститутов.

6. Все требования к изменению базового закона МПА СНГ 2005 г. сформулированы разработчиками с учетом выше изложенных проблем.

В настоящее время проект нового закона состоит из четырех глав («Общие положения», «Информация, информационные ресурсы, основы правового режима ИР», «Информатизация, информационные системы и информационные технологии», «Правовое регулирование обеспечения безопасности и ответственности») и 22 статей. Если потребуется, можно представить содержание проекта в развернутом варианте.

7. В итоге можно сформулировать выводы по выполняемой проблеме обновления модельного закона МПА СНГ 2005 г. «Об информатизации, информации и защите информации». Они сводятся к следующему:

1. Изменить название закона и представить его как модельный закон «Об информации, информатизации и обеспечении информационной безопасности» в новой редакции.

2. Для завершения работы по проекту закона ускорить выполнение части плана работ по унификации терминов и их определений для данного закона.

3. Обеспечить завершение работы по проекту с ориентацией на ясность определения объема и форм работы по предмету регулируемых отношений на уровне интегрируемых задач для содружества и по гармонизации национальных решений с учетом общих задач для СНГ и ОДКБ.

УДК 004.056:34

М.С. Бекбаева

НЕКОТОРЫЕ АСПЕКТЫ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕСПУБЛИКЕ КАЗАХСТАН

В условиях формируемого глобального информационного пространства информация приобретает свойства ценнейшего элемента как национального, так и общечеловеческого достояния. Можно сказать, что в современном мире информация стала одним из главных инструментов продвижения не только влияния, но и достижения его. Кардинальные изменения, порождаемые этим процессом, подталкивают к серьезным сдвигам во всех отраслях жизни социума, в том числе и информационной. В настоящее время обеспечение безопасности является одним из важнейших функций современного государства.

Безопасность – это состояние, при котором отсутствует опасность либо имеются в наличии эффективные меры по устранению потенциальных опасностей и угроз. Одной из важных тенденций современного этапа развития человечества является информационная революция. Стремительные изменения, вызываемые этим процессом, приводят к серьезным сдвигам во всех сферах общественной жизни. Наиболее важной сферой, переживающей в настоящее время значительную трансформацию, является информационная. В этой связи сегодня одной из актуальных проблем любого государства становится информационная безопасность. В настоящее время проблематика рассмотрения основных аспектов рассмотрения информационной безопасности характеризуется недостаточной изученностью и отсутствием четко выраженных дефиниций. Сложность решения проблемы также состоит в необходимости сочетания, с одной стороны, максимальной открытости, гарантированной Конституцией Республики Казахстан, доступа к необходимой информации, с другой стороны, ограничения доступа к ней в интересах национальной безопасности.

В то же время можно говорить о том, что мировое сообщество и отдельно взятые государства осознают сопутствующую угрозу, вызванную бурным развитием информационных технологий и необходимостью обеспечения информационной безопасности. Защита собственного информационного пространства является основной для современного общества, развитие которого обусловлено в первую очередь информационными технологиями. Однако противостоять негативной информации достаточно сложно, поскольку динамичное развитие информационных технологий каждый день формирует новые угрозы для устоявшихся в обществе стандартов и норм. Исследование, оценка и выработка действий, направленных на устранение потенциальных угроз, – вот основные задачи в сфере информационной безопасности конкретно-исторического общества и государства. Все большее влияние на общественные отношения оказывает информация, поскольку все больший ее объем проникает в сознание индивида, оказывая свое влияние на его мысли и поступки.

Информационная безопасность сегодня стала стратегической категорией, состоящей из таких комплексных понятий, как «международная безопасность» и «национальная безопасность». Она может рассматриваться в аспекте социально-экономического развития как политика, проводимая в целях сохранения и защиты технической и языковой информации, влияния информационных потоков на массовое и индивидуальное сознание, мониторинга и классификации компьютерных и сетевых угроз и предупреждения информационных войн. Понимание и исследование этих явлений, выработка мер противодействия – основные задачи, на решение которых направлена вся система обеспечения национальной безопасности.

Актуальность проблемы обеспечения информационной безопасности обусловлена прежде всего тем, что в современном мире информация стала стратегическим национальным ресурсом. За последние годы в Республике Казахстан реализован ряд мер по совершенствованию системы обеспечения информационной безопасности государства. В соответствии со Стратегией национальной безопасности Республики Казахстан была разработана и принята Концепция информационной безопасности, предусматривающая реализацию комплекса правовых, организационных и научно-технических мероприятий, направленных на прогнозирование, выявление, предупреждение и пресечение угроз в сфере информационной безопасности. Технический прогресс в областях микроэлектроники, аппаратных и программных средств, вычислительной техники ускоряет развитие информационных технологий и влияет на их совершенствование. Тенденции, связанные с информатизацией всех аспектов государственной и общественной жизни, объективно свидетельствуют, что существование современного независимого государства неразрывно связано с обеспечением информационной

безопасности всех звеньев его государственных структур. Анализ мирового опыта показывает, что именно в последние несколько лет произошел качественный скачок в процессе управления на всех уровнях: от межгосударственных образований до отдельных фирм и банков. В то же время параллельно развивалась и усиливалась опасность несанкционированного вмешательства в работу информационных систем с целью получения информации и нарушения их функционирования. Такая опасность совершенно очевидна, так как разрушение и дезорганизация информационной инфраструктуры государства по силе воздействия соизмерима с последствиями реальных боевых действий.

Так, например, информационное противоборство между государствами присутствовало практически всегда. С появлением новых информационных технологий и организацией международного информационного обмена информационная составляющая в стратегии обеспечения национальной безопасности вышла на новый уровень. Приобретение средств информационной борьбы в США за последние 15 лет увеличилось в четыре раза, Пентагон выделяет ежегодно более 90 млн долларов для проведения экспериментальных исследований в данной области, в том числе по созданию новых технологий распознавания образов, автоматическому поиску, сбору, обработке информации с помощью спутников. Во всех видах Вооруженных сил США созданы специализированные центры по ведению информационных войн, проводятся учения и штабные игры по данной проблематике.

Адекватными должны быть и меры по предотвращению таких последствий. Эффективно противостоять информационным угрозам в современных условиях может лишь хорошо организованная государственная система обеспечения информационной безопасности, которая должна осуществляться при полном взаимодействии всех государственных органов, негосударственных структур и граждан Республики Казахстан.

Подобные положения содержит и Доктрина информационной безопасности Российской Федерации, в которой отмечается, что современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

Страны, давно вступившие в информационную эру, уже имеют развитую систему защиты и ее правовую основу. США имеют более 500 законодательных актов (Россия – более 50), достаточно полно регулирующих отношения в информационной сфере, к сожалению, Казахстан и иные страны ближнего зарубежья уступают им в данном ас-

пекте. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности. Национальная безопасность существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать. Следовательно, на наш взгляд, необходимо обратить внимание на необходимость усовершенствования нормативно-методической базы и государственного запрета на распространение и использование не сертифицированной продукции в информационной сфере. Применение импортных средств защиты информации, прозрачных для их разработчиков и изготовителей, часто нецелесообразно и малоэффективно. Одной из особенностей проблемы защиты информации является абсолютный характер требования полноты всех информационных угроз, потенциально возможных в современной информационной системе. Даже один неучтенный, дестабилизирующий фактор может в значительной мере снизить эффективность защиты.

На наш взгляд, на современном этапе в Казахстане имеется определенный уровень угрозы информационной безопасности. В частности, наблюдается зависимость от импорта готовой информационной продукции, которая может повлечь за собой дестабилизацию внутриполитической ситуации. Практически не сформировано собственное мощное информационное пространство, в котором были бы задействованы самостоятельные средства массовой информации, способные конкурировать с зарубежными информационными агентствами в производстве новой информационной продукции.

В связи со сказанным представляется, что главной проблемой в обеспечении информационной безопасности в Казахстане является отсутствие единой скоординированной политики взаимодействия государственных органов с частным сектором и средствами массовой информации. Например, наша страна производит ничтожное количество компьютерной техники, программного обеспечения, новейших средств связи. А это увеличивает технологическую отсталость и информационную зависимость Казахстана от других государств, т. е. тем самым ущемляется информационная безопасность нашего государства.

Вместе с тем стремление спрятаться от новых веяний современной эпохи может способствовать развитию технологической отсталости Казахстана. В теории человеческого капитала уже давно было показано, что открытость новой информации является одной из основ качественного развития творческих способностей и возможностей человека. Речь идет о том, что политика гласности и открытости Казахстана дает широкие возможности для модернизации всех отраслей социума,

включая глобальные масштабы – взаимообмен знаниями в области экономической и политической рыночной теории, а также частные случаи каждого отдельного человека, его индивидуального сознания.

Однако данное обстоятельство – открытость – не может оцениваться только лишь как позитивный, объективный и саморегулируемый процесс. Здесь, на наш взгляд, нельзя исключать и деструктивный элемент в неконтролируемом информационном потоке, значительную часть которого могут заполнять различного рода радикальные и экстремистские идеи.

Известно, что достижение абсолютной информационной безопасности невозможно. Поэтому следует классифицировать все возможные методы и средства сопротивления информационным угрозам, комплекс специальных защитных методов и средств состоит:

1) из правовой базы (в Казахстане правовая составляющая защиты информации находится на стадии развития);

2) методов и средств информационной защиты (организационная и инженерно-техническая защита)

3) программно-аппаратной защиты.

Таким образом, следует констатировать, что основные подходы к обеспечению информационной безопасности, осознание угроз в этой сфере сближают государства в своих стремлениях обеспечить национальную безопасность в целом. Это обусловлено идентичностью основных подходов к национальной безопасности и принципов ее осуществления в Казахстане и странах ближнего зарубежья. Объединение в Таможенный союз все больше сближает страны, ставя на пути их развития новые угрозы, устранить которые возможно только посредством межгосударственного сотрудничества. Только в развитом информационном пространстве возможно совершенствование экономической и политической систем.

УДК 004.056:34

Ж.Б. Ботаханов

НЕКОТОРЫЕ АСПЕКТЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕСПУБЛИКЕ КАЗАХСТАН

Современное развитие любого государства и общества сопровождается возникновением новых форматов угроз и вызовов для национальной безопасности, обусловленных воздействием различных факторов и условий.

Неслучайно в своем ежегодном послании народу Казахстана «Казахстанский путь – 2050: Единая цель, единые интересы, единое будущее» глава государства Н. Назарбаев отметил, что одной из главных ценностей, которые объединяют всех казахстанцев и составляют фундамент будущего страны, является национальная безопасность и глобальное участие страны в решении общемировых и региональных проблем. Учитывая то, что одной из глобальных тенденций современного этапа развития человечества является информационная революция, вызывающая стремительные изменения во всех сферах общественной жизни, особую актуальность приобретают проблемы, связанные с обеспечением информационной безопасности.

Указанное обстоятельство формирует новые угрозы для информационной безопасности, являющейся составной частью национальной безопасности, и обусловливает необходимость адекватного реагирования со стороны государства и прежде всего в области правового регулирования информационной безопасности.

Говоря о правовом регулировании информационной безопасности, следует отметить, что Казахстан, являясь активным членом региональных и международных организаций, в сфере законодательной деятельности придерживается принципов и норм международного права. РК были ратифицированы «Концепция сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности», подписанная в Бишкеке 10 октября 2008 г., «Соглашения между правительствами государств – членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности», заключенное в Екатеринбурге 16 июня 2009 г.

Активно ведется законодательная работа и на национальном уровне. За последние годы в РК реализован комплекс мер по совершенствованию системы правового регулирования обеспечения информационной безопасности государства.

Так, ст. 18 Конституции РК определено, что каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и достоинства. Государственные органы, общественные объединения, должностные лица и средства массовой информации обязаны обеспечить каждому гражданину возможность ознакомиться с затрагивающими его права и интересы документами, решениями и источниками информации. В рамках реализации указанной нормы Конституции были приняты ряд законодательных актов Республики Казахстан.

В частности, закон РК «О государственных секретах» от 15 марта 1999 г. № 349-I устанавливает правовые основы и единую систему защиты государственных секретов в интересах обеспечения национальной

ной безопасности; регулирует общественные отношения, возникающие в связи с отнесением сведений к государственным секретам, их засекречиванием, распоряжением, защитой и рассекречиванием; определяет компетенции и полномочия государственных органов и организаций, в том числе и в области разработки систем правовых, административных, экономических, технических, программных и криптографических мер по защите государственных секретов.

В законе РК «О средствах массовой информации» от 23 июля 1999 г. № 451-I определены порядок получения и распространения информации, полномочия и компетенции соответствующих государственных органов в рамках государственного регулирования в области средств массовой информации.

Регулирование отношений, возникающих при создании и использовании электронных документов, удостоверенных посредством электронных цифровых подписей, предусматривающих установление, изменение или прекращение правоотношений, а также прав и обязанностей участников правоотношений, возникающих в сфере обращения электронных документов, предписано законом РК «Об электронном документе и электронной цифровой подписи» от 7 января 2003 г. № 370-II.

Закон РК от 5 июля 2004 г. № 567-II «О связи» определяет назначение связи как неотъемлемой части экономической и социальной инфраструктуры страны, предназначенной в том числе и для обеспечения потребности безопасности, обороны, охраны правопорядка, государственных органов в услугах связи. Данным законом установлены основные принципы и задачи государственного регулирования и контроля за деятельностью в области связи, в том числе компетенции соответствующих государственных органов, а также обязанности организации и учреждений, предоставляющих услуги связи.

Закон РК от 9 ноября 2004 г. № 603-II «О техническом регулировании» регламентирует правовые основы государственной системы технического регулирования, направленного на обеспечение безопасности продукции, услуг и процессов в качестве одной из основных целей технического регулирования определяет обеспечение национальной безопасности.

Правовые основы информатизации, а также регулирование общественных отношений, возникающих при создании, использовании и защите электронных информационных ресурсов и информационных систем, отражены в законе РК от 11 января 2007 г. № 217-III «Об информатизации». В частности, определены государственное регулирование и контроль в сфере информатизации, электронные информационные ресурсы, порядок их формирования и использования, технологии и средства обеспечения информационных систем, учет, регистрация

электронных информационных ресурсов, информационных систем и их аудит, права физических и юридических лиц на доступ к электронным информационным ресурсам и порядок их предоставления, а также защита электронных информационных ресурсов и информационных систем. В свою очередь, порядок лицензирования деятельности в сфере обеспечения информационной безопасности определен нормами закона РК от 11 января 2007 г. № 214-III «О лицензировании».

Важным этапом в правовом регулировании информационной безопасности стало принятие «Концепции информационной безопасности Республики Казахстан до 2016 года», утвержденной указом Президента РК от 14 ноября 2011 г. № 174. Концепция определяет задачи, приоритеты, направления и ожидаемые результаты в области обеспечения информационной безопасности личности, общества и государства. Являясь основой для взаимодействия органов государственной власти, бизнеса и общественных объединений для защиты национальных интересов РК в информационной сфере, концепция призвана обеспечить единство подходов к формированию и реализации государственной политики обеспечения информационной безопасности. Данным нормативным документом предусмотрена реализация комплекса правовых, организационных и научно-технических мероприятий, направленных, прежде всего на прогнозирование, выявление, предупреждение и пресечение угроз в сфере информационной безопасности.

В законе РК от 6 января 2012 г. № 527-IV «О национальной безопасности Республики Казахстан», принимая во внимание степень влияния информационных технологий на состояние социально-экономической и культурной жизни общества и государства, обусловливающую необходимость предъявления повышенных требований к решению вопросов информационной безопасности, в качестве одного из видов национальной безопасности выделена информационная безопасность.

Так, согласно нормам данного закона информационная безопасность обеспечивается решениями и действиями государственных органов, организаций и должностных лиц, направленными на недопущение информационной зависимости и изоляции, информационного воздействия на общественное и индивидуальное сознание, предотвращение информационной экспансии и блокады, обеспечение бесперебойной и устойчивой эксплуатации сетей связи, выявление, предупреждение и пресечение утечки и утраты сведений, составляющих государственные секреты и иную защищаемую законом тайну, обнаружение и дезорганизацию механизмов скрытого информационного влияния, поддержание и развитие эффективной системы защиты информационных ресурсов, информационных систем и инфраструктуры связи, в которых циркулируют сведения, составляющие государственную тайну.

Принятие указанных законодательных актов свидетельствует о том, что в настоящее время обеспечение информационной безопасности является неотъемлемой частью обеспечения национальной безопасности государства.

Для сравнения в Российской Федерации, учитывая возрастающую роль информационной сферы, еще в начале нового тысячелетия была принята «Доктрина информационной безопасности Российской Федерации», утвержденная приказом Президента РФ от 9 сентября 2000 г. № 1895, направленная на развитие Концепции национальной безопасности РФ применительно к информационной сфере. В данном документе, представляющем собой совокупность официальных взглядов на цели, задачи, принципы и направления обеспечения информационной безопасности, выделены основные составляющие национальных интересов РФ в информационной сфере, виды и источники угроз информационной безопасности, основные задачи по ее обеспечению.

Отдельные аспекты обеспечения информационной безопасности нашли отражение и в «Стратегии развития информационного общества в Российской Федерации», утвержденной Президентом РФ 7 февраля 2008 г. приказом № 212. Так, обеспечение национальной безопасности в информационной сфере определено в числе основных задач, требующих решения для достижения вышеуказанной цели, а также основных направлений реализации вышеуказанной стратегии.

Сравнительный анализ законодательных актов в сфере обеспечения информационной безопасности позволяет констатировать наличие общих подходов к обеспечению информационной безопасности, обусловленную, на наш взгляд, идентичностью основных подходов к национальной безопасности и принципов ее осуществления в России и Казахстане.

Таким образом, следует отметить, что правовое регулирование информационной безопасности в РК осуществляется в соответствии с принципами и нормами международного права и направлено на обеспечение защиты прав и интересов человека и гражданина, общества и государства в информационной сфере от реальных и потенциальных угроз. В условиях необходимости обеспечения устойчивого развития и информационной независимости государства правовое обеспечение состояния защищенности и деятельности по противодействию и предотвращению угроз информационной безопасности является основным фактором устойчивого развития современного независимого государства.

В свою очередь, создание эффективного механизма противодействия угрозам информационной безопасности прежде всего должно происходить в рамках постоянного совершенствования национального законодательства, что, предусматривает углубленное изучение международно-правовых аспектов данной проблемы.

УДК 34:001.32

М.А. Вус, М.М. Кучерявый,
О.С. Макаров, Г.И. Перекопский

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОДКБ

I. Общей стратегической целью государств – членов Организации Договора о коллективной безопасности (ОДКБ) является формирование многофункциональной системы коллективной безопасности. Важнейшим ее элементом является создание системы обеспечения информационной безопасности.

Информационная сфера влияет на все сферы национальной безопасности, при этом проецируются новые угрозы и риски, возрастают опасности.

В качестве основной угрозы для государств – членов ОДКБ в области международной информационной безопасности рассматривается возможное деструктивное использование информационных и коммуникационных технологий.

В формате ОДКБ существует согласие относительно того, что под информационной безопасностью понимается состояние защищенности личности, общества, государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве. Под системой информационной безопасности в политических и правовых документах ОДКБ понимается комплекс мер правового, политического, организационного, кадрового, финансового, научно-технического и социального характера, нацеленных на обеспечение информационной безопасности государств-членов. На первом месте позиционируются меры правового характера. От единого понимания правовых подходов к формированию системы информационной безопасности сегодня зависит развитие всей системы обеспечения международной и коллективной безопасности [1].

В современных геополитических условиях для достижения общих целей государствам – членам ОДКБ требуется коллективность и скоординированность действий. Решением Совета коллективной безопасности ОДКБ в 2008 г. была утверждена Программа совместных действий по формированию системы информационной безопасности, а в 2010 г. обеспечение информационной безопасности было закреплено как важное направление сотрудничества в уставе организации. В том же году было утверждено Положение о сотрудничестве государств – членов ОДКБ в сфере обеспечения информационной безопасности, в котором выделены два направления: информационная политика и ин-

формационная безопасность. Годом позже были утверждены план первоочередных мероприятий по формированию основ скоординированной информационной политики и перечень мероприятий, направленных на формирование системы обеспечения информационной безопасности в интересах ОДКБ.

II. Комплексным планом мероприятий Программы деятельности Парламентской ассамблеи ОДКБ по сближению и гармонизации национального законодательства государств – членов ОДКБ на 2011–2015 гг. предусмотрена разработка Рекомендаций по совершенствованию и гармонизации национального законодательства государств – членов ОДКБ в сфере обеспечения информационно-коммуникационной безопасности (далее – Рекомендации). Проект этого документа представлялся и рассматривался в апреле 2014 г. на заседании Экспертно-консультативного совета при Парламентской ассамблее ОДКБ, получил одобрение и направлен в парламенты государств – членов ОДКБ для получения экспертных заключений.

Сферой применения (направленности) указанных Рекомендаций в документах ОДКБ определена «информационно-коммуникационная безопасность». В международно-правовом поле встречается понятие «информационная и коммуникационная безопасность» в трактовке: «состояние защищенности личности, общества, государства и их интересов от существующих и потенциальных угроз в сфере информационных и коммуникационных средств и технологий, включая меры, направленные на обеспечение доступности, целостности, конфиденциальности и подлинности информации» [2]. Это понятие шире англоязычного термина «Network and Information Security», введенного в сообщении комиссии Евросоюза «Сетевая и информационная безопасность: предложения для подхода европейской политики». Это понятие трактуется как «способность сети или информационной системы противостоять при заданном уровне надежности случайным угрозам или умышленным вредоносным действиям, которые подвергают риску доступность, подлинность, целостность и конфиденциальность хранимых или передаваемых данных и связанных с ними служб, доступ к которым осуществляется с помощью таких сетей или систем».

Концептуальные подходы к разработке Рекомендаций выработаны на основе анализа действующих нормативных актов, концептуально-доктринальных документов и документов стратегического планирования ОДКБ и государств ее членов в сферах обеспечения информационной и коммуникационной безопасности, включая вопросы защиты государственных секретов, противодействия преступлениям против информационной безопасности, вопросы развития информационной инфраструктуры, деятельности средств массовой информации в условиях развития

информационного общества. В основу положены результаты анализа национального законодательства государств – членов ОДКБ, модельного законодательства Межпарламентской ассамблеи СНГ, межгосударственные документы и соглашения ШОС, БРИКС, ЕврАзЭс, ООН и др. в сфере обеспечения информационной безопасности [3].

III. Вопросы формирования активной согласованной информационной политики государств – членов ОДКБ и создание потенциала совместного противодействия угрозам и вызовам в современных условиях приобретают особую актуальность. Рекомендации направлены на установление общих подходов государств – членов ОДКБ к правовому обеспечению информационно-коммуникационной безопасности жизнедеятельности общества. Сбалансированность системы обеспечения информационно-коммуникационной безопасности будет стимулировать информационное развитие и международный информационный обмен, обеспечение информационных условий экономического и таможенного, научно-технического и культурного сотрудничества, в итоге – повышение эффективности обеспечения национальной безопасности всех государств – членов ОДКБ.

Проблематика информационной безопасности связана с категориями суверенитета и юрисдикции государств. Вследствие этого существует настоятельная необходимость всесторонней углубленной научной проработки принципиальных целей, задач и направлений развития сотрудничества государств – членов ОДКБ по противодействию современным угрозам в информационной сфере. Необходима также разработка системы показателей и характеристик информационно-коммуникационной безопасности в ОДКБ.

На практике сегодня на постсоветском пространстве отсутствует единое понимание понятийно-категориального аппарата и не выстроена иерархичная система субъектов (сил) обеспечения информационно-коммуникационной безопасности. Это порождает аморфность механизма выработки единых решений, а нередко и сужает проблему, нормативное регулирование оказывается направлено преимущественно на стандартизацию технологических процессов. Предлагаемый в Рекомендациях алгоритм сближения законодательства предусматривает определение основных направлений обустройства единого безопасного информационного пространства как объединенного сегмента информационных пространств государств – членов ОДКБ.

К числу основных направлений сближения законодательства государств – членов ОДКБ в Рекомендациях отнесены:

общие вопросы организации обеспечения информационной безопасности;

защита единого информационного пространства;

защита информационных ресурсов;

противодействие преступлениям в информационной сфере (в том числе информационному терроризму);

обеспечение безопасности информационно-коммуникационной инфраструктуры (включая критически важные объекты);

информационное обеспечение реализации государственной политики.

Сближение и гармонизация законодательства государств – членов ОДКБ по каждому из перечисленных выше направлений должны включать:

проработку понятийного аппарата;

определение основных угроз информационной безопасности;

выработку концептуальных мер правового обеспечения информационной безопасности по каждому направлению (такими решениями, в частности, представляются лицензирование деятельности, регистрация и стандартизация работ и услуг, сертификация товаров в области обеспечения информационной безопасности);

разработку системы организационных мер обеспечения информационной безопасности по каждому направлению;

совершенствование правового обеспечения информационной безопасности на национальном уровне;

гармонизацию системы мер правового обеспечения информационной безопасности на международном (региональном) уровне.

Для реализации перечисленных неординарных задач требуется эффективный механизм совершенствования нормативно-правовой базы и устранение пробелов в национальном законодательстве. В практическом плане разработчикам Рекомендаций видится полезной также подготовка Соглашения о сотрудничестве государств – членов ОДКБ по организации межгосударственного обмена информацией в сфере обеспечения информационной безопасности.

1. Законодательство государств – членов ОДКБ в сфере обеспечения информационной безопасности: опыт, проблемы и перспективы гармонизации : материалы Междунар. науч.-практ. конф. СПб. : Секретариат МПА СНГ, 2014. 88 с.

2. Соглашение между Правительствами Российской Федерации и Правительством Федеративной Республики Бразилии о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности (2010 г.) / Международные правовые акты и документы в области международной информационной безопасности. М., 2012. С. 80–87.

3. О совершенствовании и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности / И.Л. Бачило [и др.] // Информац. право, 2013, № 1(32). С. 24–27.

УДК 004:34

А.П. Жалов, А.В. Калиберов

ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТАМОЖЕННЫХ ОРГАНОВ

Информационно-коммуникационные технологии и услуги в настоящее время являются ключевым фактором в развитии почти всех областей социально-экономической сферы и представляют собой один из активно развивающихся секторов экономики Республики Беларусь. На протяжении последних 15 лет в результате выполнения государственных программ разработан ряд общегосударственных и ведомственных информационных систем, создана национальная система формирования и регистрации информационных ресурсов. Начиная с 2011 г. осуществляется поэтапный переход на использование общегосударственной автоматизированной информационной системы для оказания электронных услуг и реализации государственных функций в электронном виде.

Государственный таможенный комитет Республики Беларусь, решая задачи, стоящие перед государственными органами в процессе построения электронного правительства, последовательно реализует мероприятия по таким направлениям:

формирование стандартов и рекомендаций в сфере использования информационных и коммуникационных технологий в таможенных органах;

обеспечение эффективного международного и межведомственного информационного взаимодействия на основе информационных и коммуникационных технологий и интеграция информационных систем таможенных органов Таможенного союза;

обеспечение эффективности взаимодействия таможенных органов с населением и организациями на основе информационных и коммуникационных технологий;

создание типовых программно-технических решений поддержки деятельности таможенных органов.

В условиях широкого внедрения информационно-телекоммуникационных технологий во все сферы деятельности таможенных органов решение вопросов обеспечения информационной безопасности является одним из приоритетных, что предопределяет динамичные процессы совершенствования правовой базы в данной области.

Таможенное законодательство в части использования современных информационных технологий и обеспечения информационной безопасности базируется на ряде международных правовых актах и прежде всего на Международной конвенции об упрощении и гармонизации таможенных процедур, заключенной в Киото 18 мая 1973 г.

Киотская конвенция является универсальным кодифицированным международно-правовым актом в области таможенного дела, регулирующим практически все. Согласно Киотской конвенции новые или измененные нормы национального таможенного законодательства должны предусматривать:

электронные способы обмена информацией в качестве альтернативы требованию предоставления документов на бумажных носителях;

сочетания электронных и документарных методов удостоверения подлинности и идентичности;

право таможенной службы оставлять у себя информацию для использования в таможенных целях в случае необходимости, для обмена информацией с другими таможенными службами и со всеми иными пользователями, если это допускается законом.

Также стандарт 9.6 данной конвенции предусматривает, что при предоставлении информации таможенные органы обеспечивают неразглашение подробностей частного или конфиденциального характера, за исключением случаев, когда такое разглашение предписано или санкционировано национальным законодательством.

Данные положения нашли свое отражение в актах таможенного законодательства Республики Беларусь. Закон от 10 января 2014 г. № 129-З «О таможенном регулировании в Республике Беларусь» закрепил:

1) информационные системы и информационные технологии используются таможенными органами в целях обеспечения выполнения возложенных на них функций, в том числе обмена информацией с государственными органами, оказания государственных услуг населению, участникам внешнеэкономической деятельности по предоставлению информации в электронном виде;

2) порядок формирования, использования информационных ресурсов таможенных органов, требования к документированию информации и сведений, в том числе предоставляемых электронным способом, устанавливаются Государственным таможенным комитетом Республики Беларусь;

3) защита информации, распространение и (или) представление которой ограничено, в таможенных органах обеспечивается в соответствии с законодательством Республики Беларусь.

В структуре законодательства, регулирующего вопросы обеспечения информационной безопасности, особое значение имеют концептуальные политические документы, в Республики Беларусь к важнейшим из которых надо отнести Концепцию национальной безопасности Республики Беларусь (утверждена указом Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь»).

В деятельности таможенных органов Республики Беларусь таким правовым актом является Концепция информационной безопасности таможенных органов Республики Беларусь, утвержденная в 2006 г. решением Коллегии Государственного таможенного комитета Республики Беларусь.

Концепция определила систему взглядов на проблему обеспечения информационной безопасности прежде всего в автоматизированных информационных системах, составляющих Единую автоматизированную информационную систему таможенных органов Республики Беларусь, а также в таможенных органах в целом.

Однако 6 июля 2010 г. вступили в силу Договор о Таможенном кодексе Таможенного союза, подписанный в Минске 27 ноября 2009 г., и Протокол о внесении изменений и дополнений в Договор о Таможенном кодексе Таможенного союза от 27 ноября 2009 г., подписанный в Москве 16 апреля 2010 г. 10 ноября 2008 г. принят закон Республики Беларусь № 455-З «Об информации, информатизации и защите информации». Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575 утверждена Концепция национальной безопасности Республики Беларусь.

В связи с этим положения Концепции информационной безопасности таможенных органов Республики Беларусь должны быть переработаны с учетом изменений национального законодательства, положений Таможенного кодекса Таможенного союза, а также с учетом соглашений, договоров, протоколов, заключенных в рамках Таможенного союза, решений Межгосударственного Совета Евразийского экономического сообщества, решений Комиссии Таможенного союза.

Концепция должна стать методологической основой для формирования и проведения единой политики в области обеспечения безопасности таможенных органов в современных условиях; разработки практических мер по воплощению политики безопасности информации и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации.

УДК 004.056.52

П.С. Ивличев, Н.А. Ивличева

ЭФФЕКТИВНОСТЬ ДЕЙСТВИЯ РЕЕСТРА ДОМЕННЫХ ИМЕН, УКАЗАТЕЛЕЙ СТРАНИЦ САЙТОВ В СЕТИ ИНТЕРНЕТ И СЕТЕВЫХ АДРЕСОВ, ПОЗВОЛЯЮЩИХ ИДЕНТИФИЦИРОВАТЬ САЙТЫ, СОДЕРЖАЩИЕ ИНФОРМАЦИЮ, РАСПРОСТРАНЕНИЕ КОТОРОЙ В РОССИЙСКОЙ ФЕДЕРАЦИИ ЗАПРЕЩЕНО

Понятие Единого реестра доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено, введено в российское законодательство федеральным законом от 28 июля 2012 г. № 139-ФЗ.

Указанный закон дополняет основной документ, регулирующий оборот информации (федеральный закон «Об информации, информационных технологиях и защите информации») ст. 15.1, которая предусматривает порядок ограничения распространения информации посредством сети Интернет.

Принятие этого закона вызвало в Российской Федерации значительный общественный резонанс и носило в основном негативную оценку. Были высказывания, касающиеся нарушения прав добросовестных распространителей информации, нарушения прав свободы слова. В настоящее время волнения относительно этого закона практически утихли. Причем причина такого затишья заключается далеко не в том, что положения законодательства были приняты участниками информационного обмена целиком и полностью.

Механизм блокировки затрагивает два существенных звена информационного обмена в сети Интернет: провайдера хостинга и провайдера услуг связи.

Провайдер хостинга обязан принять превентивные меры, предупредив владельца сайта о необходимости удаления информации, распространение которой запрещено. В случае непринятия мер к провайдеру хостинга как к информационному посреднику могут быть применены меры гражданской ответственности, предусмотренные Гражданским кодексом Российской Федерации.

Однако на деле эта норма остается недействующей. Провайдер хостинга – юридическое лицо, основу дохода которого составляют средства, полученные от владельцев сайта. Терять клиентов предприниматели не желают, поэтому в последние полгода наблюдается активный отток хостинг-бизнеса за пределы Российской Федерации. Используются как международные зоны (.org, .net), так и национальные домены стран с низким уровнем информационной культуры (например, Королевства Тонга).

Таким образом, несмотря на имеющуюся норму права, у владельцев сайтов всегда есть механизм ее несоблюдения.

Второе звено в цепи блокировок – это провайдер услуг связи. На первый взгляд блокировка на этом уровне может показаться эффективной, поскольку доступ к сайтам сети Интернет осуществляется именно через серверы провайдера, которые расположены на территории Российской Федерации и к которым возможно применение санкций, однако механизмы навигации в сети Интернет делают и эту защиту во многом формальной.

Если зайти на сайт любой поисковой системы и сделать поиск способов обхода блокировок, то без особого труда будет найден десяток «рецептов», использование которых не требует наличия специальных навыков в области информационных технологий. Популярные торрент-трекеры даже завели отдельные форумы на своих сайтах, посвященные обходу ограничений по доступу к информации.

Суть всех методов, по существу, сводится к переадресации запросов. Методика этой переадресации может быть различной: анонимайзеры, анонимные прокси-серверы, альтернативные DNS-серверы, плагины к браузерам, анонимные сети.

В частности, популярный браузер Google Chrome имеет плагин Frigate, который переадресует все запросы через прокси-серверы, расположенные в Германии и Нидерландах. Ни один из этих прокси-серверов не относится к запрещенным сайтам, поэтому провайдер не может блокировать такие запросы. Прокси-сервер же, от имени пользователя, делает запрос к заблокированному сайту. Таким образом, дискомфорт для пользователя минимален, владелец хостинга получает арендную плату от владельца сайта, владелец сайта продолжает получать рекламные отчисления.

По состоянию на 18 апреля 2014 г., только плагином Frigate пользуются 239 000 пользователей, что составляет 2–3 % пользователей Google Chrome в России.

Таким образом, в российском обществе сформировалась очередная ситуация законодательного формализма. Это, в конечном итоге, влияет на развитие информационной культуры, уважение к законам и авторитет государства.

Очевидно, что методы борьбы с распространением запрещенной информации в сети Интернет нуждаются в существенной коррекции. Анализ мирового опыта может подсказать несколько направлений для развития российского законодательства в этой сфере:

1. Фильтрация информации в национальных масштабах на государственном уровне. Примером такого решения может служить «Великий китайский файрвол», использование которого позволило сократить даже использование анонимной сети Tor.

2. Разработка международных соглашений в сфере распространения информации. Этот метод менее эффективен, поскольку нормы международного права носят необязательный характер. Сложность соблюдения границ в глобальных сетях признается многими странами, что создает предпосылки к распаду интернета на национальные сегменты.

3. Введение ответственности конечных пользователей. Примером может служить законодательство Германии и Франции. В Российской Федерации ответственность пользователя наступает только при совершении уголовного преступления.

4. Пересмотр порядка доступа к ресурсам сети Интернет. Использование систем ограничения и контроля доступа, мониторинга просматриваемой информации.

Разумеется, все эти меры будут непопулярными, однако если в национальные интересы входит развитие информационной политики, то принимаемые ограничения должны реально работать.

УДК 343.985

Ю.Ф. Каменецкий

ПРИМЕНЕНИЕ СЛЕДОВАТЕЛЕМ ЗНАНИЙ О СИСТЕМЕ «КЛИЕНТ-БАНК» В РАССЛЕДОВАНИИ ХИЩЕНИЙ ПУТЕМ ЗЛОУПОТРЕБЛЕНИЯ СЛУЖЕБНЫМИ ПОЛНОМОЧИЯМИ

В последние годы модернизация экономики и развитие финансовой сферы Беларуси потребовали значительного сокращения времени для совершения оборота безналичных расчетов и платежей. С этой целью для дистанционного управления денежными средствами клиента на большинстве предприятий внедрены системы дистанционного банковского обслуживания, использующие в качестве удаленного рабочего места электронные устройства: персональный компьютер, ноутбук, нетбук, планшетный компьютер и т. д. Наибольшее распространение получили система «Клиент-банк» и интернет-банкинг. Поэтому набравшая темпы информатизация общества не только способствовала стремительному росту компьютерных преступлений, но и видоизменила способ совершения значительной части экономических преступлений, в том числе и хищений путем злоупотребления служебными полномочиями.

В свою очередь, с помощью систем дистанционного банковского обслуживания способ совершения хищений путем злоупотребления служебными полномочиями предопределяет специфику следообразования, поскольку действия преступника неизбежно связаны с совершением безналичных расчетов и платежей. В силу сказанного для установления способа совершения преступления, выдвижения версии и отыскания следов хищения огромную роль играет криминалистически значимая информация о первичных учетных документах, отражающих преступные действия и указывающих на лиц, их совершивших. Однако в настоящее время научно обоснованные рекомендации по получению такой информации из системы «Клиент-банк» в ходе расследования хищений путем злоупотребления служебными полномочиями отсутствуют.

Личный опыт автора и анализ судебно-следственной практики указывают, что эффективное расследование таких уголовных дел напрямую зависит от уровня знания следователями порядка функционирования системы «Клиент-банк». Например, с использованием знаний о работе этой системы следствию удалось своевременно получить сведения о способе преступления и собрать достаточные доказательства для привлечения директора предприятия Х. и главного бухгалтера М. к уголовной ответственности по ч. 4 ст. 210 УК. В частности, Х. и М. с целью хищения безосновательно перечислили с предприятия Б. на подконтрольное им предприятие Ф. деньги с назначением платежа «по договору безвозмездного займа». В действительности договор безвозмездного займа не оформлялся и не мог быть оформлен, поскольку данное право отнесено к исключительной компетенции учредительного собрания. С целью сокрытия своих преступных действий от аудиторской проверки М. и Х. внесли заведомо ложные сведения в бухгалтерский учет предприятия, изменив в платежном поручении запись о назначении платежа: «за поставку техники». В ходе предварительного следствия М. и Х. свою причастность к совершению преступления категорически исключали.

Анализ исходной информации о хищении поставил перед следователем ряд задач по сбору доказательств, связанных с отысканием первичного учетного документа, послужившего основанием незаконного платежа, установлением в составе данного платежного документа корректности, целостности и авторства электронной подписи, а также установлению обстоятельств составления поддельного платежного поручения и помещения его в бухгалтерский учет предприятия. В основе решения данных задач лежала организация следователем различных технических мероприятий, направленных на предотвращение сокрытия следов, уничтожение информации. Для этого были задействованы используемые в

банке средства и методы защиты информации, ее хранения в неизменном виде. С помощью специалиста в сфере высоких технологий информация о реквизитах платежного поручения была зафиксирована и осмотрена в базе данных систем дистанционного банковского обслуживания и базе данных автоматизированной банковской системы.

Более того, следователем из банка затребована информация о движении платежного поручения, его авторстве, дате, времени, способе его создания, а также системах обнаружения вторжения и антивирусной защиты и т. п. Установление исходной информации о первичном учетном документе, с помощью которого совершено преступление, позволило выдвинуть версию о способе совершения Х. и М. хищения и собрать неопровержимые доказательства их вины.

Как показывает практика, расследования уголовных дел, способ сокрытия хищения путем злоупотребления служебными полномочиями может включать не только действия по изменению в бухгалтерском учете сведений о назначении платежа, но и осложняться отражением в таком учете ряда вымышленных операций. Выявить данные фиктивные операции в бухгалтерском учете можно путем анализ платежей в системе дистанционного банковского обслуживания и последующего сопоставления результатов такого анализа с данными бухгалтерского учета.

Например, такой анализ платежей в системе «Клиент-банк» послужил отправной точкой в расследовании уголовного дела по ч. 4 ст. 210 УК в отношении бухгалтера П. предприятия М., которая с целью хищения денежных средств предприятия на основании платежных поручений через систему «Клиент-банк» перечислила денежные средства на предприятия А., Б. и В. за продукцию, которой завладела совместно со своим подельником Е. Для сокрытия совершенного преступления в бухгалтерской программе «1С. Бухгалтерия» в карточках счета платежного поручения контрагентов П. указала вместо фактических получателей иные предприятия Г., Д., Е., с которыми предприятием М. ежедневно осуществлялись различные сделки.

Для получения доказательств о способе преступления следователем произведены осмотры систем «Клиент-банк» и «1С. Бухгалтерия», что позволило зафиксировать информацию о содержании внесенных в бухгалтерский учет недостоверных сведений и должностном лице, осуществившем эти преступные действия с целью сокрытия хищения.

Таким образом, успешное расследование данного уголовного дела опиралось на своевременное получение информации о платежах, производстве следственных действий для закрепления следов преступления в системе дистанционного банковского обслуживания, использующего электронные устройства клиента банка.

Подводя итог, следует подчеркнуть, что компьютерные технологии, принятые на вооружение в финансовой сфере страны, значительно видоизменяют способ совершения хищений путем злоупотребления служебных полномочий, а следовательно, и следовой картины в системе «Клиент-банк».

Сегодня отправной точкой в расследовании этих преступлений является уровень знаний следователем возможностей систем дистанционного банковского обслуживания и особенностей отражения в ней следов хищений данного вида. В настоящее время одним из способов улучшения качества и оперативности расследования может стать систематическая работа по повышению профессионального уровня следователей, специализирующихся на расследовании данных хищений.

УДК 343.985

А.Г. Кулага

ТЕОРЕТИЧЕСКИЕ И ПРИКЛАДНЫЕ ВОПРОСЫ КВАЛИФИКАЦИИ ХИЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНОЙ ТЕХНИКИ

Возможности, предоставляемые международным технологическим прогрессом, телекоммуникационными инновационными системами, внедрением компьютерной техники, заключают в себя не только положительное влияние на общество и государство, но и угрозы безопасности.

В процессе обмена информацией, использования инновационного высокотехнологичного оборудования во всех сферах жизнедеятельности государств между пользователями телекоммуникационных платежных международных систем возникает множество различных вопросов в сложившейся ситуации.

Развитие компьютерных технологий, их внедрение в деловую сферу во всех направлениях общественной жизни привело к возникновению преступлений, в результате которых преступники для завладения чужим имуществом используют высокотехнологическое оборудование. Это заставило правоохранительные органы более активно включиться в борьбу с новыми способами хищений с использованием компьютерной техники. В связи с этим при расследовании преступлений против информационной безопасности, хищений с использованием компьютерной техники в даче правовой оценки возникают проблемные вопросы в выявлении преступлений с использованием компьютерной техники, во взаимодействии специалистов правоохранительных органов, в

техническом обеспечении и подготовке квалифицированных экспертов, а также квалификации преступлений.

Сегодня используются методические рекомендации квалификации хищений, предусмотренных ст. 212, 205 УК, а нужно разрешать вопросы и ст. 209, 350 УК и др.

Хищение, предусмотренное ст. 212 УК, отличается от других форм хищения способом нарушения отношений собственности. В законе сказано о хищении путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сети передачи данных, либо путем введения в компьютерную систему ложной информации.

Хищение путем использования компьютерной техники возможно лишь посредством компьютерных манипуляций, заключающихся в обмане потерпевшего или лица, которому имущество вверено или под охраной которого оно находится, с использованием системы обработки информации. Данное хищение может быть совершено как путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, так и путем введения в компьютерную систему ложной информации.

Хищение путем использования компьютерной техники имеет материальную конструкцию состава преступления. Юридически оконченным оно признается с момента наступления двух последствий: собственнику причиняется реальный вред; лицо противоправно, безвозмездно завладевает имуществом и получает реальную возможность пользоваться или распоряжаться похищенным. Для оконченного преступления не требуется, чтобы виновный реально распорядился имуществом. В подобной ситуации достаточно установить, что у лица объективно появилась такая возможность и это обстоятельство осознается им.

Например, лицо, изменившее информацию, обрабатываемую в компьютерной системе, и переведшее со счета потерпевшего на банковский счет виновного определенную сумму денег, должно нести ответственность за оконченное хищение не со времени реального получения им определенной суммы похищенных денег, а с момента их перевода и получения виновным возможности пользоваться или распоряжаться ими.

Если лицо использует компьютерную технику для изготовления заведомо фиктивного документа с целью последующего противоправного безвозмездного завладения имуществом путем обманного использования документа, все совершенное квалифицируется только как мошенничество (ст. 209 УК).

В ч. 2 ст. 212 предусматривается ответственность за хищение путем использования компьютерной техники, совершенное повторно либо

группой лиц по предварительному сговору или сопряженное с несанкционированным доступом к компьютерной информации. В ч. 3 – за действия, предусмотренные ч. 1 или ч. 2, совершенные в крупном размере. В ч. 4 – за действия, предусмотренные ч. 1, 2 или ч. 3, совершенные организованной группой либо в особо крупном размере.

Перечисленные признаки, за исключением одного, по своему содержанию совпадают с одноименными квалифицирующими обстоятельствами других форм хищения.

Особенность представляет собой такой квалифицирующий признак, как хищение путем использования компьютерной техники, сопряженное с несанкционированным доступом к компьютерной информации. Доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, является несанкционированным, если он сопровождался нарушением системы защиты.

Отграничение от иных, сходных преступлений. Преступление, предусмотренное ст. 212, следует отграничивать от модификации компьютерной информации (ст. 350 УК) по таким признакам преступления, как объект преступления, предмет преступления, объективная сторона и субъективная сторона.

Хищение путем использования компьютерной техники необходимо отграничивать от мошенничества (ст. 209 УК) по следующим признакам: при мошенничестве потерпевший либо иное лицо, в ведении или под охраной которого находится имущество, сам добровольно передает имущество или право на имущество виновному под влиянием обмана или злоупотребления доверием; при хищении путем модификации компьютерной информации изъятие и завладение имуществом происходят посредством использования компьютерной техники (например, похититель путем модификации компьютерной информации переводит со счета потерпевшего через посреднический банк на свой счет похищенную сумму денег).

В условиях глобализации мира, увеличения международных компьютерных телекоммуникаций, несомненно, повышается рост преступлений, связанных с хищениями имущества путем использования компьютерной техники. Первые преступления, предусмотренные ст. 212 УК и гл. 31 «Преступления против информационной безопасности» были зарегистрированы в 2001 г. в связи с принятием новой редакции Уголовного кодекса Республики Беларусь, ежегодно просматривалась тенденция роста. В частности, уже за первое полугодие текущего года зарегистрировано 755 преступлений данного вида, что почти соответствует количеству преступлений, зарегистрированных за весь 2013 г. (855). Преступления в XXI в. все больше совершаются «интеллектуалами». Мировая тенденция предрасположена к тому, что основная доля ущер-

ба будет причиняться с использованием глобальных компьютерных систем. Вместе с тем наши возможности в выявлении и раскрытии данного вида преступлений не в полной мере соответствуют требованиям времени. С внедрением международных компьютерных систем преступность становится интернациональной, не признающей границ. В связи с этим необходимо инициировать проведение совместных международных встреч правоохранительных органов по подготовке специалистов в области раскрытия и расследования компьютерных преступлений, обмену имеющимся опытом в этой области для получения научных разработок и методических рекомендаций.

С учетом возникающих проблем выявления и расследования преступлений с использованием компьютерной техники в целях повышения эффективности получения и использования информации правоохранительными органами при расследовании преступлений против информационной безопасности необходимо:

1) внести предложение по разработке нормативных правовых актов, регламентирующих международное сотрудничество правоохранительных органов стран СНГ при расследовании преступлений против информационной безопасности и иных преступлений с целью увеличения эффективности такого взаимодействия;

2) включать в состав следственно-оперативных групп по расследованию конкретных резонансных преступлений сотрудника, отвечающего за анализ информации и осуществить подготовку квалифицированных сотрудников по техническим вопросам, производить обмен полученными данными специалистов по проведению компьютерно-технических экспертиз в области криминалистического исследования высокотехнологического оборудования, программного обеспечения;

3) использовать лицензионное профильное техническое обеспечение, позволяющее проводить процессуальные действия в минимальные сроки, исключающие уничтожение и модификацию информации;

4) разработать методические рекомендации по своевременной профилактике преступлений, в которых фигурирует компьютерная техника, телекоммуникационные сети и программное обеспечение.

Использование нового технического потенциала, лицензионного технического обеспечения, методических рекомендаций, применение значимой информации, качественных компьютерно-технических экспертиз в установленные сроки, предоставят дополнительные возможности по улучшению доказательственной базы расследуемых уголовных дел, усовершенствуют возможности профилактических мероприятий по пресечению хищений путем использования компьютерной техники и выявлению преступлений против информационной безопасности.

УДК 004.9

В.В. Лавренов

НЕКОТОРЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Успешное выполнение правоохранительных задач в условиях формирования новой социально-экономической и политической ситуации в стране неразрывно связано с обеспечением эффективности управления органами внутренних дел, способствует созданию нормальных условий для функционирования всей инфраструктуры общества. Стабильный правопорядок в стране образует соответствующие общественные предпосылки для социально-экономического и научно-технического прогресса, духовного и нравственного развития.

Эффективность функционирования системы напрямую зависит от информационных процессов, составляющих основу управления, так как любой управленческий цикл осуществляется на основе поступающей в систему информации. Совершенствование системы управления в современных условиях невозможно без использования современных информационных технологий, поскольку именно вопросы обработки информации являются критическими.

Повышение роли информационного обеспечения управленческой деятельности органов внутренних дел обусловлено сложностью выполняемых задач, резкими изменениями оперативной обстановки. Все это вызывает необходимость обработки большого объема информации в короткие сроки.

От полноты и объективности информации, получаемой органами внутренних дел, зависит правильность принимаемых управленческих решений, что, в свою очередь, непосредственно связано с вопросами усиления борьбы с преступностью. Результативность работы органов внутренних дел по предупреждению, раскрытию, расследованию преступлений невозможна без своевременного, достаточного и качественного обеспечения информацией.

Масштабы применения и приложения информационных технологий в органах внутренних дел таковы, что наряду с проблемами производительности, надежности и устойчивости функционирования информационных систем остро встает вопрос о защите циркулирующей в системах информации от несанкционированного доступа. Мировая статистика фактов несанкционированного доступа к информации показывает, что большинство современных информационных систем достаточ-

но уязвимы с точки зрения безопасности, информационные системы органов внутренних дел не исключение.

При рассмотрении безопасности информационных систем обычно выделяют две группы проблем: сетевая безопасность и безопасность компьютера. Под сетевой безопасностью понимают все вопросы, связанные с взаимодействием устройств в сети, это, прежде всего, защита данных в момент их передачи по линиям связи и защита от несанкционированного удаленного доступа в сеть. К безопасности компьютера относят все проблемы защиты данных, хранящихся и обрабатывающихся компьютером, которая рассматривается как автономная система. Эти проблемы решаются средствами операционных систем и приложений таких, как базы данных, а также встроенными аппаратными средствами компьютера.

На практике сегодня существует два подхода к обеспечению безопасности компьютера:

1) использование только встроенных в операционную систему (ОС) и приложения средств защиты;

2) применение, наряду со встроенными, дополнительных механизмов защиты. Этот подход заключается в использовании так называемых технических средств добавочной защиты – программных, либо программно-аппаратных комплексов, устанавливаемых на защищаемые объекты.

С учетом существующей статистики угроз можно утверждать, что встроенных в ОС и приложения механизмов защиты недостаточно. По оценкам специалистов в современных универсальных ОС не выполняются в полном объеме требования к защите информации в автоматизированных системах. Это значит, что они не могут без использования технических средств добавочной защиты применяться для защиты информации. При этом следует отметить, что основные проблемы защиты здесь вызваны не невыполнимостью ОС требований к отдельным механизмам защиты, а принципиальными причинами, обусловленными реализуемой в ОС концепцией защиты. Концепция эта основана на реализации распределенной схемы администрирования механизмов защиты, что само по себе является невыполнением формализованных требований к основным механизмам защиты.

Таким образом, наиболее эффективным способом безопасности компьютера является подход применения дополнительных механизмов защиты.

К этим механизмам можно отнести программы управления доступом (рассматривая весь класс таких программ). Механизмы управления доступом являются основой защиты ресурсов, обеспечивая решение задачи разграничения доступа субъектов к защищаемым информационным и техническим ресурсам. Однако при применении только программных механизмов защиты в общем случае невозможно осуществлять контроль активности одной программы над другой, запущенной на том же компьютере, что может привести к несанкционированному доступу к информации. Поэтому данная функция должна возлагаться на аппаратную компоненту системы защиты – плату, устанавливаемую в свободный слот защищаемого компьютера.

С учетом сказанного можем сделать вывод, что преимуществом реализации технологии защиты информации является программно-аппаратный подход. Этот подход оказывает противодействие всей совокупности угроз информационной безопасности, причем противодействие осуществляется вне зависимости от того, какой способ доступа использован злоумышленником, т. е. задача защиты решается в общем виде.

Отдельно следует отметить необходимость повышения квалификации сотрудников, эксплуатирующих средства защиты. При этом необходимо понимать, что процесс защиты информации непрерывен, равно как непрерывен процесс изменения угроз информационной безопасности.

Таким образом, одним из важнейших условием защищенности компьютерной информации является квалификация администраторов безопасности и сотрудников эксплуатирующих служб, которая, по крайней мере, не должна уступать квалификации злоумышленников. В противном случае не помогут никакие средства защиты.

УДК 343.985

А.Н. Лепёхин

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМ В БОРЬБЕ С КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТЬЮ

Проблемы борьбы с современной преступностью, и в том числе компьютерной, являются достаточно актуальными и предполагают решения ряда первостепенных задач и в первую очередь информационного обеспечения управленческой деятельности посредством использования компьютерных технологий обработки и анализа различных данных. Одним из эффективных средств решения подобной научно-практической задачи является использование программно-технических средств информационно-аналитической работы. Объективно, что задачами любой современной информационно-аналитической системы являются эффективное хранение, обработка и анализ данных.

Следует отметить, что в настоящее время накоплен определенный опыт в этой области.

Эффективное хранение информации достигается наличием в составе информационно-аналитической системы целого ряда источников данных. Обработка и объединение информации достигается применением инструментов извлечения, преобразования и загрузки данных. Анализ данных осуществляется при помощи современных инструментов анализа данных.

Проблема анализа исходной информации для принятия управленческих решений оказалась настолько серьезной, что появилось отдельное направление или вид информационных систем – информационно-аналитические системы (ИАС), под которыми понимают комплекс аппаратных, программных средств, информационных ресурсов, методик, которые используются для обеспечения автоматизации аналитических работ в целях обоснования принятия управленческих решений и других возможных применений [1, с. 38].

Разнообразие источников данных и необходимость их использования в каждом конкретном случае объясняется потребностью поразному хранить информацию в зависимости от стоящих перед правоохранительными органами задач. Классифицируя источники данных по типам и назначению, каждый из них можно условно отнести к одной из трех групп: транзакционные источники данных, хранилища данных, витрины данных.

Данные в ИАС могут заноситься как вручную, так и автоматически. На этапе первоначальной фиксации данные поступают через системы сбора и обработки информации в так называемые транзакционные базы данных или операционные базы данных (БД).

Поскольку транзакционные источники данных, как правило, не согласованы друг с другом, то для анализа таких данных требуется их объединение и преобразование. Поэтому на следующем этапе решается задача консолидации данных, их преобразования и очистки, в результате чего данные поступают в аналитические базы данных. Аналитические базы данных, например хранилища данных или витрины данных, и есть те основные источники, из которых аналитик получает информацию, используя соответствующие инструменты информационного анализа.

Наряду с общими функциональными требованиями информационно-аналитическая система структурного подразделения правоохранительных органов должна обеспечивать пользователям доступ к аналитической информации, защищенной от несанкционированного использования. Таким образом, классическая архитектура информационно-аналитической системы насчитывает следующие уровни: сбор и первичная обработка данных; извлечение, преобразование и загрузка данных;

хранение данных; представление данных в витринах данных; анализ данных; Web-портал (для правоохранительных органов – защищенный).

Следует отметить, что в настоящее время на рынке информационных технологий представлен широкий спектр инструментальных средств, предназначенных для быстрой реализации компонентов архитектуры ИАС. Использование таких инструментов позволяет не разрабатывать аналитические приложения заново, а воспользоваться готовыми современными технологиями и, следовательно, сократить время и затраты на их создание [2, с. 12–17].

Таким образом, решение задачи информационно-аналитического обеспечения борьбы с преступностью определяется правильным подбором инструментов информационного анализа, а также средств поддержки процессов извлечения, преобразования, загрузки и хранения данных. При этом в ходе реализации ИАС правоохранительных органов могут быть использованы программные решения как разных производителей (смешанные), так и одного производителя (платформенно-базированные) для разрешения практических задач информационного обеспечения принятия управленческих решений.

1. Белов В.С. Информационно-аналитические системы. Основы проектирования и применения : учеб. пособие / Моск. гос. ун-т экономики, статистики и информатики. М., 2005.

2. Волков И.В., Галахов И.Ю. Архитектура современной информационно-аналитической системы // Директор информ. службы. М., 2002. № 3.

УДК 681.3

А.Л. Осипенко

НАУЧНОЕ ОБЕСПЕЧЕНИЕ ПРОТИВОДЕЙСТВИЯ СЕТЕВОЙ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

Среди приоритетных направлений деятельности полиции в последние годы руководством МВД России особо выделяется противодействие преступности в сфере информационных технологий, что вполне оправдано с учетом очевидных тенденций повышения ее социальной опасности. Число преступлений, связанных с использованием сети Интернет, неуклонно растет, все чаще они приобретают «резонансный» характер. Преступность активно осваивает преимущества, предлагаемые сетью Интернет. Выступая в прошлом году на 22-й сессии Комиссии ООН по предупреждению преступности и уголовному правосудию в Вене, представитель России А. Змеевский отметил, что за год жерт-

вами преступлений в сети Интернет стали около 556 млн пользователей, а прямой ущерб превысил 110 млрд долларов США.

Совершение сетевых компьютерных преступлений становится менее опасным и более выгодным по сравнению с «традиционными» способами криминального обогащения. Среди наиболее «доходных» преступлений – онлайн мошенничество, хищения с банковских счетов, рассылка спама и организация DDoS-атак. Однако социальная опасность сетевой компьютерной преступности не измеряется лишь причиняемым экономическим ущербом. Особую озабоченность вызывает деятельность в сети экстремистских групп, распространение детской порнографии и иные деяния, оказывающие разрушающее воздействие на общественные устои.

Координация противоправной деятельности с помощью всемирной сети осуществляется на любых расстояниях с высочайшей скоростью. На этой основе сетевая преступность обретает более организованные формы, получая ярко выраженный транснациональный характер. Расширяются сферы преступного влияния, открываются перспективы как для распространения «традиционной» противоправной деятельности на новые регионы мира, так и для использования новых видов незаконного получения доходов. Отсутствие препятствий для трансграничных действий приводит к тому, что многие преступники сознательно идут на совершение преступления в отношении сетевых объектов, расположенных на территории других государств, рассчитывая на то, что раскрытие преступлений существенно затруднится несовершенством взаимодействия правоохранительных органов разных стран.

Стоит отметить и значительное усиление адаптивности криминальных структур, действующих в глобальной сети, не только к изменениям в среде их существования, но и к противодействию со стороны правоохранительных органов: преступники активно изучают методы оперативной работы и учитывают их при подготовке и реализации преступного замысла. Изощренные способы достижения противоправных целей предполагают применение конспирации, тщательную проработку способов сокрытия следов преступлений.

Можно констатировать, что проблема слабой защищенности пользователей интернета от преступных проявлений носит комплексный характер и имеет много составляющих (организационную, техническую, правовую, экономическую, социальную и др.), затрагивает не только международные, общие для всех стран, но и национальные интересы отдельных государств. В этой связи зарубежными учеными уже активно ведется исследование влияния технологических достижений на общественные процессы, на развитие права и трансформацию преступности. Понятно, что вопросы противодействия преступности в

сфере информационных технологий приобретают особую актуальность и для наших стран. Поиск ответов на них, несомненно, является одной из важнейших задач науки и в первую очередь наук криминального цикла, включая и теорию оперативно-розыскной деятельности.

С позиций последней перечисленные особенности проявления сетевой компьютерной преступности подтверждают, что эффективное противодействие невозможно без применения оперативно-розыскных сил, средств и методов. Выявление и раскрытие сетевых компьютерных преступлений стало одной из важных задач полиции, решение которой должно быть основано на осуществлении оперативно-розыскной деятельности непосредственно в сети Интернет.

Многочисленные практические примеры из опыта специализированных подразделений говорят о том, что установление обстоятельств совершения указанных преступлений в большинстве случаев возможно только благодаря использованию оперативно-розыскных приемов, а ставка в их раскрытии исключительно на технические методы, как правило, не дает нужного результата. Более того, использование ресурсов сети Интернет при добывании оперативно значимой информации стало важным для всех оперативных подразделений полиции, поскольку в последние годы очевидно массовое перемещение такой информации в сетевое информационное пространство. Разумеется, это побуждает с позиций оперативно-розыскной науки изучать закономерности отражения в сетевых ресурсах оперативно значимой информации, особенности ее обнаружения, получения, проверки и фиксации.

Проведенные исследования подтверждают, что потенциал применения оперативно-розыскных сил, средств и методов в добывании оперативно значимой информации достаточно высок. Однако опыт их применения должен не просто переноситься на сетевые криминальные явления, но творчески адаптироваться к условиям, возникающим в киберпространстве. Важную роль в этом должны играть научные исследования, обеспечивающие понимание сложных сетевых криминогенных процессов.

С каких же позиций предлагается подходить к организации ОРД в сети? Для ответа на этот вопрос уточним, что до сих пор в оперативно-розыскной науке компьютерные сети преимущественно рассматриваются в качестве: а) инструмента обмена информацией; б) информационного хранилища. Такой подход вполне справедлив, но он позволяет применять для добывания оперативно значимой информации лишь отдельные оперативно-технические мероприятия. Однако сеть выступает сегодня не только средством коммуникации и обработки информации. Интернет можно считать новой специфической средой осуще-

ствления различных видов деятельности с уникальными социальными и пространственными характеристиками.

С учетом результатов изучения социальных процессов, связанных с использованием интернета, можно предложить следующую модель. Вокруг информационной инфраструктуры сплотилось сообщество пользователей сети, образовавшее особую социальную среду. Взаимодействие этого сообщества с сетевой инфраструктурой породило сетевое информационное пространство, в котором люди во все большей степени проявляют социальную активность (работают, получают образование, совершают финансовые операции и покупки, получают разнообразные услуги, общаются, проводят досуг). В этом пространстве формируются сообщества и осуществляется совместная деятельность в самых разных сферах. Здесь активно развиваются инструменты не только обратной связи общества с государством, но и информационно-психологического воздействия. Наконец, здесь совершаются преступления, на которые полиции необходимо реагировать.

С обозначенных позиций становится ясным, что интернет является не просто инструментом коммуникации, но особой средой реализации различных видов деятельности, в том числе и противоправной. В этой среде формируются криминальные сообщества, на постоянной основе совершающие преступления, здесь возникают новые виды противоправной активности, множатся способы и формы совершения противоправных деяний.

Все это приводит нас к выводу о том, что интернет может рассматриваться в качестве особой среды осуществления ОРД, задающей специфические условия применения оперативно-розыскных методов.

Осознание социальной природы глобальных сетей, использование понятий сетевой социальной среды и сетевого информационного пространства, признание этого пространства в качестве особого места осуществления ОРД позволяют с научных позиций познавать суть явлений, на которые направлено применение оперативно-розыскных методов в интернете. Этот подход помогает определять эффективные способы получения информации, например, на таких сетевых объектах, как социальные сети, специализированные тематические форумы и блоги лиц, представляющих оперативный интерес.

Познание уникальных свойств интернета обеспечивает выявление закономерностей образования оперативно значимой информации и отражения ее в окружающей среде. На этой основе могут быть систематизированы места ее преимущественной концентрации и источники получения:

1. В технологической инфраструктуре глобальных сетей: а) сетевое оборудование, через которое осуществляются коммуникационные акты

разрабатываемых лиц; б) средства вычислительной техники и программное обеспечение, используемые в криминальной деятельности либо подвергшиеся преступным воздействиям.

2. В сетевой социальной среде: а) криминогенная среда, связанная с деятельностью сетевых сообществ негативной социальной направленности, в которых участвуют лица со схожими криминальными интересами, занятиями и условиями существования; б) технические специалисты, осведомленные по роду деятельности о компьютерных преступлениях и обстоятельствах их совершения; в) лица, потерпевшие от сетевых компьютерных преступлений.

3. В сетевом информационном пространстве: а) сетевые объекты, на которых совершаются компьютерные преступления и имеются условия их повторения; б) информационные ресурсы, содержащие сведения о совершении преступлений и лицах, их совершающих; в) места сетевого общения криминально настроенных лиц.

Вероятно, этим круг потенциальных информационных источников не ограничивается. Тем не менее он демонстрирует возможности добывания оперативно-розыскной информации и способствует определению требований к его организации и тактике непосредственно в интернете.

Изучение показывает, что оперативный поиск возможен по трем направлениям: на сетевых криминогенных объектах; в сетевой криминогенной среде; сетевых информационных ресурсах.

Основными местами сосредоточения оперативно значимой информации в сетевом пространстве являются криминогенные объекты, на которых могут проводиться мероприятия по ее обнаружению. Важные для выявления преступлений сведения концентрируются на сетевых криминогенных объектах в виде: а) следов противоправной деятельности; б) ссылок на материалы, запрещенные к распространению; в) сообщений лиц, осведомленных об обстоятельствах подготовки и совершения преступлений.

Сетевые криминогенные объекты целесообразно разделить на три основные типа:

1. Объекты, на которых фиксируются повторяющиеся попытки преступных посягательств и (или) наличие условий для их совершения (сетевые объекты, обрабатывающие конфиденциальную информацию; сайты банковских структур; интернет-магазины, интернет-аукционы; сайты социальных сетей и т. п.). Здесь происходит выявление признаков совершенных преступлений и установление лиц, их совершивших.

2. Информационные ресурсы, содержащие оперативно значимые сведения (сайты, через которые распространяется социально опасная информация, реализуются предметы, запрещенные к обороту, ведется пропаганда криминального образа жизни, вовлекаются в противоправную

деятельность новые участники и т. п.). Сбор информации на таких объектах связан с изучением их информационного наполнения в целях выявления фактов распространения определенных предметов (наркотических средств, оружия, детской порнографии и др.) и социально опасной информации (например, материалов экстремистской направленности).

3. Места сетевого общения криминально настроенных лиц (форумы криминальной направленности, блоги, чаты и др.). В подобных местах осуществляется активный информационный обмен между лицами, причастными к преступной деятельности. Постоянное наблюдение за такими объектами создает продуктивные каналы поступления оперативно значимой информации.

Получение оперативно значимой информации в сетевой криминогенной среде в основном осуществляется с применением адаптированных к сетевой социальной среде оперативно-розыскных методов работы, которая может осуществляться в том числе в закрытых сетевых форумах. В подобных местах регулярно появляются индикаторы, сигнализирующие о криминальной активности конкретных субъектов: сообщения о подборе соучастников противоправной деятельности (наводчиков, сбытчиков, скупщиков, сообщников), объявления о поиске поставщиков средств достижения противоправных целей (вредоносного программного обеспечения, бот-сетей, реквизитов кредитных карт и т. п.) и др. Непосредственное наблюдение за закрытыми для общего доступа местами сетевого общения криминальной направленности обеспечивает возможность получать сведения о намерениях участников преступных сообществ, устанавливать их связи между собой, узнавать детали замышляемых деяний, выявлять признанных лидеров, следить за их перемещениями, вести подбор лиц для привлечения к сотрудничеству и т. д. Можно контролировать интернет-адреса тех, кто часто посещает эти сайты, изучать характер их активности в сетевом общении, сведения о конкретных фактах преступной деятельности.

Особое место среди направлений сбора информации в интернете занимает поиск в его информационных ресурсах. Преимущественно он должен реализовываться через комплексную систему мероприятий, объединяемых понятием «оперативно-розыскной мониторинг сетевых информационных ресурсов».

Обобщение алгоритмов поиска позволило выделить два основных направления оперативно-розыскного мониторинга, которые способны обеспечить высокую интенсивность поступления оперативно значимой информации:

1. Автоматизированный поиск сетевых информационных ресурсов, содержащих запрещенную к распространению информацию и оперативно значимые сведения. Наиболее просто реализуется с использованием

поисковых систем (таких, как Google, Яндекс и т. п.), которые могут применяться для получения дополнительной информации о пользователе или группе пользователей сети. В сетевом информационном пространстве существуют и обширные закрытые зоны. По некоторым данным, почти 20–30 % сетевого пространства недоступно для обычных пользователей: эти ресурсы не индексируются поисковыми серверами, а доступ к ним возможен только для «посвященных» лиц, знающих сетевые адреса ресурсов. Преодолеть указанные затруднения возможно за счет применения специального программного обеспечения, осуществляющего более «глубокий» анализ информационных ресурсов.

2. Контент-анализ выявленных сетевых информационных ресурсов, связанных с деятельностью разрабатываемых лиц и преступных сообществ. Это формализованный аналитический метод исследования содержания документов в целях выявления и измерения характеристик социальных явлений, получивших в них отражение. При осуществлении контент-анализа в тексте или массивах текстов устанавливается присутствие ключевых слов, фиксируются смысловые единицы содержания, частота их употребления, соотношение различных элементов текста.

В последние годы активно разрабатываются и внедряются системы противодействия киберпреступности с элементами искусственного интеллекта, которые, в частности, формируют базы данных, содержащие «досье» на потенциальных преступников: идентификационные данные, преступная специализация, регулярность участия в форумах и публикационная активность, тематика сообщений, упоминания о нем в сообщениях других участников, позволяющие установить личность, связи в социальных сетях. В результате анализа совпадений данных, указываемых при регистрации, выявляется соответствие псевдонимов, под которыми разрабатываемый участвует в разных форумах.

Дальнейшая обработка данных проявляет связи между указанными сведениями, полученными в ходе проведенных ранее расследований, между конкретными событиями криминального характера, о которых стало известно от заявителей, и сообщениями на «просканированных» форумах. Все это позволяет выявлять группировки криминальной направленности, их специализацию, характер неочевидных связей между фигурантами и их причастность к тем или иным событиям в сети.

Подобные группы, сформировавшиеся на основе сетевого принципа организации, крайне сложно изучать с применением традиционных методов. На слайде представлены их основные характеристики, которые, несомненно, заслуживают глубокого научного анализа с позиций наук криминального цикла. Для них характерны отсутствие иерархии участников, децентрализация, наличие межнациональных и трансграничных связей, маневренность и динамичность, адаптивность, гиб-

кость реагирования на изменения внешних условий, повышенная сопротивляемость оперативно-розыскным воздействиям. В таких группах нередко отсутствуют непосредственные контакты между участниками, а координация действий осуществляется с использованием сетевых коммуникационных каналов. Группы могут быстро формироваться, а после достижения преступных целей столь же быстро распадаться. Важно, что указанные особенности снижают эффективность применения общепринятых подходов к выявлению преступных групп, требуют пересмотра стратегии и тактики оперативных подразделений и в первую очередь повышения их структурно-функциональной гибкости.

Безусловно, специфика интернета не может не отражаться на правовом регулировании оперативно-розыскной деятельности в сети. Здесь остро стоит целый ряд вопросов, связанных в первую очередь с обеспечением прав граждан при осуществлении оперативно-розыскных мероприятий, определением пределов полномочий оперативно-розыскных органов в наднациональном сетевом пространстве, регламентацией взаимодействия операторов связи с органами, осуществляющими ОРД. Разумеется, законодательная деятельность должна подкрепляться серьезными научными исследованиями.

Особый блок составляют проблемы, связанные с соблюдением прав граждан. Не вызывает сомнений, что с развитием интернета проблемы защиты прав личности на неприкосновенность частной жизни усугубляются. Попадая в сеть, сведения о частной жизни лица выходят из-под контроля субъекта распространения, могут массово дублироваться на многочисленных информационных ресурсах и храниться там неограниченно долго. В результате у полиции появляется возможность выполнять в киберпространстве мониторинг персональных данных граждан, следить за электронной перепиской разрабатываемых лиц, автоматизированно собирать и анализировать разрозненные сведения об их поведении, связях, интересах, финансовых операциях, местонахождении и перемещениях.

Естественно, расширение возможных форм «электронного» контроля за гражданами со стороны правоохранительных органов обостряет задачу поиска оптимального соотношения между интересами личности и общества. Отметим, что в последнее время во многих государствах отмечается тенденция изменения баланса приоритетов в пользу защиты общественных, государственных интересов.

Согласно докладу о мониторинге социальных сетей, представленному Агентством по национальной безопасности США, использование в правоохранительной деятельности сведений, которые пользователи социальных сетей добровольно выставляют в открытый доступ, признается допустимым. В Великобритании законодателем рассматривается законопроект, предоставляющий полиции самые широкие полномочия по доступу к электронной почте, контактам через Skype и сообщениям в Facebook.

Попытки устранить определенные пробелы в отечественном законодательстве, на основе которого осуществляется борьба с преступностью в сфере информационных технологий, должны находить соответствующую теоретическую проработку.

В наиболее заметной степени права граждан ограничиваются при проведении в интернете оперативно-розыскных мероприятий, направленных на сбор, поиск, изъятие информационных объектов, а также на обследование компьютерных средств, в которых возможно их обнаружение. Осуществление соответствующих мероприятий из-за их новизны нередко сопряжено с возникновением неоднозначных ситуаций. Так, в различных регионах страны сформировалась разная практика выбора ОРМ при осуществлении одних и тех же действий для документирования фактов противоправной деятельности в сети.

Например, отмечается различие в подходах оперативных подразделений к получению данных о пользователях сети. Такая информация по запросу уполномоченных оперативных подразделений передается им оператором связи (провайдером сети Интернет) при исполнении закрепленной федеральным законом «О связи» обязанности предоставлять субъектам ОРД информацию о пользователях услугами связи и об оказанных им услугах связи, а также иную информацию, необходимую для выполнения задач, возложенных на оперативно-розыскные органы. Заметную остроту имеет проблема недостаточной определенности правового статуса служебных сведений о состоявшихся сеансах связи, а также правовой регламентации процедуры их предоставления субъектам ОРД.

Следует отметить, что в 2010 г. вопрос о необходимости судебного решения для получения информации о соединениях между абонентами частично разрешен в результате внесения изменений в уголовно-процессуальное законодательство. Так, в п. 24.1 ст. 5 УПК РФ введено понятие «информации о соединениях между абонентами и (или) абонентскими устройствами». К такой информации отнесены сведения о дате, времени, продолжительности соединений между абонентами и (или) абонентскими устройствами (пользовательским оборудованием), о номерах абонентов, о других данных, позволяющих идентифицировать абонентов, а также сведения о номерах и месте расположения приемопередающих базовых станций. Важно, что ст. 186.1 УПК РФ устанавливает, что получение следователем указанной информации допускается на основании судебного решения. И хотя речь в данном случае идет о порядке получения информации при производстве соответствующего следственного действия, очевидно, что аналогичный подход должен быть сохранен при осуществлении оперативно-розыскных мero-

приятий, связанных с получением служебных сведений о сетевых соединениях в сеансах связи, реализованных в сети Интернет.

На наш взгляд, необходимо внесение в законодательство изменений, уточняющих правовое регулирование исполнения операторами связи запросов оперативно-розыскных органов, и разработка межведомственного нормативного правового акта, регламентирующего процедуры представления оператором связи информации об абоненте, идентификационных данных пользовательского оборудования, сведений о состоявшихся сетевых соединениях.

Значительная часть сетевых компьютерных преступлений имеет трансграничный характер, при их раскрытии нередко в сферу осуществления ОРД попадают иностранные граждане и складываются ситуации столкновения различных интересов и правовых систем. Такое положение дел требует регламентации в соответствующих международных актах вопросов ограничения прав граждан при раскрытии трансграничных компьютерных преступлений. Стоит отметить, что согласование международных правовых средств в изучаемой сфере затрудняется не только существенными различиями в правовых системах государств, но и спецификой объекта правового регулирования. Одной из проблем, становящейся основным «камнем преткновения» в организации борьбы с трансграничными сетевыми преступлениями, является определение юрисдикции государства при их раскрытии. Для ОРД актуальность данной проблемы состоит в первую очередь в том, что от вариантов ее решения напрямую зависят пределы полномочий национальных оперативно-розыскных органов в сетевом информационном пространстве, а следовательно, и допустимость осуществления ими отдельных трансграничных действий в сетевом пространстве с учетом наднациональной природы последнего. На наш взгляд, есть необходимость в дополнении федерального закона «Об оперативно-розыскной деятельности» статьей, определяющей особенности проведения оперативно-розыскных мероприятий с использованием информационно-телекоммуникационных сетей международного информационного обмена

Нельзя забывать еще об одном важном направлении исследований. К сожалению, в специальной литературе весьма слабо отражаются актуальные вопросы предупреждения противоправного поведения в сетевой социальной среде, проблемы искоренения причин и условий киберпреступности. И это при том, что подходы к профилактике здесь должны быть особыми, учитывающими роль технических методов, важность консолидации усилий международных организаций, государственных органов, представителей бизнеса, гражданского общества и сетевой общественности. Решая указанные проблемы необходимо рассматривать интернет и связанные с его использованием криминальные

явления в широком контексте социальных, политических, культурных и экономических трансформаций современного общества.

Безусловно, изложенное не исчерпывает всей совокупности проблем теоретической проработки вопросов организации и правового регулирования ОРД в сети Интернет. Подводя итог, отмечу, что сегодня важным ресурсом повышения эффективности оперативно-служебной деятельности органов внутренних дел становится ведомственная наука. Перед ней стоят серьезные и ответственные задачи, связанные с внедрением инновационных методов и средств противодействия преступности. Более того, на ведомственные учебные заведения руководство МВД возлагает особые надежды, связанные с подготовкой личного состава и формированием нового облика полиции.

Наш институт на протяжении многих лет готовит для МВД России специалистов технического профиля в области радиотехники, связи, защиты информации, а с 2010 г. осуществляет подготовку специалистов по эксплуатации и администрированию программно-технических комплексов органов внутренних дел. В вузе на кафедрах технического и юридического профилей трудятся 31 доктор и свыше 150 кандидатов наук. Их совместная работа позволяет определять точки соприкосновения для проведения междисциплинарных исследований по наиболее актуальным темам в обсуждаемой сегодня сфере. Ведь не секрет, что среди довольно многочисленных публикаций, посвященных таким темам, не так уж много работ, в которых проблемы освещались бы одинаково корректно как с технической, так и с правовой точки зрения. И здесь у нашего научного коллектива имеется особое преимущество – есть солидный научный потенциал, который включает ученых по научным специальностям и юридических, и технических наук и позволяет успешно решать указанные задачи. Ежегодно нашими учеными выполняется свыше 70 научно-исследовательских работ. Мы стремимся сосредоточить усилия наших ученых в первую очередь на решении наукоемких, комплексных задач, актуальных для органов внутренних дел. Среди таких задач в последнее время особое место занимает решение проблем раскрытия и расследования преступлений в сфере информационных технологий.

Завершая, подчеркну, что эффективная научная работа невозможна без постоянного обмена мнениями и идеями между учеными и практическими работниками. Для обеспечения такого обмена в институте ежегодно проводится большое количество различных научно-представительских мероприятий с привлечением специалистов из других образовательных и научных организаций МВД России и стран ближнего зарубежья, правоохранительных органов. Для нас очень важно участие в таких мероприятиях специалистов-практиков. Это дает возможность «сверить часы», понять, какие темы научно-исследовательской работы наиболее востребованы сегодня.

УДК 346.34

А.А. Пуп

АКТУАЛЬНЫЕ ПРАВОВЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ЗАКЛЮЧЕНИИ, ИСПОЛНЕНИИ И ПРЕКРАЩЕНИИ ДОГОВОРА ФРАНЧАЙЗИНГА

Современное развитие общественно-политических и экономических отношений привело к созданию информационного общества. Возникновение частной собственности и частного сектора в экономике, дальнейшее развитие частного бизнеса и информационных технологий предопределило появление конфиденциальной информации, а также стало предпосылкой зарождения недобросовестных форм и методов ведения информационной борьбы и, как следствие, реальной угрозы нарушения режима информационной безопасности предпринимательской деятельности.

В данный момент успешное развитие бизнеса зависит от информационной безопасности, а информация часто становится товаром, от наличия и сохранности которого зависит благополучие граждан, организаций и общества в целом.

Одной из наиболее прогрессивных форм ведения предпринимательской деятельности является франчайзинг, известный также в современной правовой теории как франшизинг или франчайз.

В соответствии с белорусским законодательством (п. 1 ст. 910 ГК Республики Беларусь) под *договором франчайзинга* (иначе именуемым в праве Республики Беларусь договором комплексной предпринимательской лицензии), понимается договор, в котором одна сторона (правообладатель) обязуется предоставить другой стороне (пользователю) за вознаграждение на определенный в договоре франчайзинга срок либо без указания срока комплекс исключительных прав (лицензионный комплекс), включающий право использования фирменного наименования правообладателя и нераскрытой информации, в том числе секретов производства (ноу-хау), а также других объектов интеллектуальной собственности (товарного знака, знака обслуживания и т. п.), предусмотренных договором франчайзинга, для использования в предпринимательской деятельности пользователя.

Таким образом, все составляющие элементы договора франчайзинга подлежат правовой охране в Республике Беларусь как объекты права интеллектуальной собственности.

Наибольшую ценность для сторон договора франчайзинга представляет правовая охрана такой нераскрытой информации, как секреты производства или ноу-хау.

Право на защиту секрета производства (ноу-хау) от незаконного использования установлено гл. 66 ГК. При этом сведения, составляющие секрет производства (ноу-хау), в силу п. 2 ст. 1010 и п. 2. ст. 140 ГК охраняются в режиме коммерческой тайны в случае, если они соответствуют следующим требованиям: не являются общеизвестными или легкодоступными третьим лицам в тех кругах, которые обычно имеют дело с подобного рода сведениями; имеют коммерческую ценность для их обладателя в силу неизвестности третьим лицам; не являются объектами исключительных прав на результаты интеллектуальной деятельности и не отнесены в установленном порядке к государственным секретам. Режим коммерческой тайны считается установленным после определения состава сведений, подлежащих охране в режиме коммерческой тайны, и принятия лицом, правомерно обладающим такими сведениями, совокупности мер, необходимых для обеспечения их конфиденциальности.

Право на защиту таких сведений возникает независимо от выполнения в отношении этих сведений каких-либо формальностей (регистрации, получения свидетельства и т. п.).

Основной проблемой информационной безопасности при заключении, исполнении и прекращении договора франчайзинга является «человеческий фактор». Часто основную опасность для организации представляют случайные или преднамеренные действия персонала по раскрытию секретов производства (ноу-хау).

По результатам многочисленных исследований утечки информации в отечественных и зарубежных компаниях представляется возможным установить ряд конкретных причин, приводящих к разглашению коммерческой тайны и, как следствие, утрате значимости секретов производства, как при заключении, так и при исполнении договора франчайзинга. Такими причинами являются: недопонимание руководителями компаний прямой зависимости успеха бизнеса от информационной безопасности; недостаточная компетентность персонала, ответственного за информационную безопасность; неудовлетворительное отношение руководства и сотрудников компании к обучению информационной безопасности; отсутствие представления о реальной стоимости информации и деловой репутации.

Угрозы сохранности коммерческой тайны могут быть внешними и внутренними. Внешние угрозы возникают вследствие непосредственной деятельности недобросовестных конкурентов, преступных элементов, из-за неумелой постановки взаимоотношений фирмы с представителями государственных структур, общественных организаций,

средств массовой информации, а внутренние – инициируются персоналом предприятия.

Действия извне могут быть направлены на пассивные носители информации и выражаться, например, в попытках похищения документов или снятия копий с документов; снятии информации, возникающей в тракте передачи в процессе коммуникаций; уничтожении информации или повреждении ее носителей; случайном или преднамеренном доведении до сведения конкурентов документов или материалов, содержащих коммерческую тайну.

Действия извне могут быть также направлены на персонал компании и выражаться в форме угроз, подкупа, шантажа, выведывания информации, составляющей коммерческую тайну, или предполагать переманивание ведущих специалистов в конкурирующую фирму.

Миграция специалистов, особенно имевших дело с конфиденциальной информацией, – основной и трудно контролируемый канал утечки информации. Вторым по значимости каналом являются всевозможные монографии сотрудников, публикации в печати. Как отмечают эксперты, так называемый традиционный обмен опытом между работниками организаций также является одним из значимых факторов, способствующих утечке информации.

Обеспечение сохранения конфиденциальной коммерческой информации требует соблюдения предприятиями следующих условий: определение (выявление) сведений, составляющих коммерческую тайну предприятия; разработка порядка их охраны; обеспечение соблюдения этого порядка.

В Республике Беларусь отношения, возникающие в связи с установлением, изменением и отменой режима коммерческой тайны, а также в связи с правовой охраной коммерческой тайны регулирует закон Республики Беларусь от 5 января 2013 г. № 16-З «О коммерческой тайне».

Разглашение сведений, содержащих коммерческую тайну организации, и сведений конфиденциального характера влечет гражданско-правовую, уголовную, административную и дисциплинарную ответственность в соответствии с законодательством Республики Беларусь.

Таким образом, несмотря на то, что практика заключения договоров как национального, так и международного франчайзинга в Республике Беларусь немногочисленна, имеет место динамика развития данных отношений, в связи с чем возникают актуальные вопросы защиты прав и обеспечения информационной безопасности по данному виду правоотношений.

В настоящее время стороны договора франчайзинга при обеспечении информационной безопасности уделяют особое внимание использованию различных технологических решений на программном и аппаратном уровнях. Вместе с тем результаты анализа сложившейся ситуации убедительно доказывают, что при заключении, исполнении и прекращении договора франчайзинга технологические решения позволяют обеспечить защиту лишь от некоторых опасностей. При охране секретов производства (ноу-хау) многое зависит от человеческого фактора, участия конкретных сотрудников компаний в процессах обмена информацией, использования ресурсов информационных систем.

В данный момент в Республике Беларусь на законодательном уровне созданы все предпосылки для защиты прав и законных интересов обладателей нераскрытой информации (ноу-хау), передаваемой по договору франчайзинга, однако немногие организации уделяют внимание обучению своих сотрудников с целью повышения их знаний в области информационной безопасности и недопущению разглашения коммерческой тайны.

Для обеспечения конфиденциальности информации, составляющей коммерческую тайну, в организациях, осуществляющих сотрудничество по договорам франчайзинга, должен быть введен режим коммерческой тайны или режим конфиденциальной информации.

Несмотря на то, что договор франчайзинга в настоящее время получил распространение и признан самостоятельным объектом правового регулирования более чем в 80 странах мира, законодательная база, регулирующая франчайзинговые отношения, разработана лишь в некоторых из этих стран, что в достаточной степени осложняет возможности защиты прав, в том числе международных, и обеспечения информационной безопасности при исполнении данного вида договоров.

Все это свидетельствует о необходимости развития и гармонизации подходов к охране информации на международном уровне, выработки единых методов и механизмов правового регулирования режима информационной безопасности с целью недопущения незаконного использования конфиденциальной информации и сохранения участниками гражданского оборота заинтересованности в конкурентном сотрудничестве, ведущем к развитию как национальной, так и мировой экономики.

УДК 004.056:34

А.А. Султанов

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ КАЗАХСТАН

В Концепции правовой политики Республики Казахстан на период с 2010 по 2020 годы определена важная задача национального права –

это определение основ государственной системы защиты информации и основных угроз в данной сфере. Как следствие актуальным становится разработка механизмов реализации единой государственной политики в сфере информационной безопасности. В этой связи в Республике Казахстан уделяется повышенное внимание вопросам реализации мер, направленных на противодействие реальным и потенциальным угрозам в данной сфере.

Следует отметить, что указом Президента Республики Казахстан от 14 ноября 2011 г. № 174 была утверждена «Концепция информационной безопасности Республики Казахстан до 2016 года». Информационная безопасность страны в данном документе рассматривается с двух взаимосвязанных аспектов: технического и социально-политического.

Технический аспект подразумевает обеспечение защиты национальных информационных ресурсов, информационных систем, информационно-телекоммуникационной инфраструктуры от неавторизованного доступа, использования, раскрытия, нарушения, изменения, прочтения, проверки, записи или уничтожения для обеспечения целостности, конфиденциальности и доступности информации.

Социально-политический аспект заключается в защите национального информационного пространства и систем распространения массовой информации от целенаправленного негативного информационного и организационного воздействия, могущего причинить ущерб национальным интересам Республики Казахстан.

Государственная техническая политика информационной безопасности – составная часть внутренней и внешней политики Республики Казахстан, совокупность взглядов, правил и практических методов, регулирующих обработку, передачу, хранение и защиту информации в киберпространстве; разработку, использование, защиту программно-аппаратных комплексов.

В нынешних условиях в Республике Казахстан, по сути, выстроена система обеспечения информационной безопасности, подчиненная общей цели обеспечения национальных информационных интересов Казахстана и гарантирующая реальное участие государственных органов, общественных и иных организаций и объединений, граждан в создании условий для информационной безопасности в соответствии с законом, а также приняты концептуальные и нормативные правовые акты, регламентирующие отношения в сфере безопасности. При этом предпринимаемые государством меры ориентированы, прежде всего, на своевременное предупреждение негативных последствий посягательства на информационную безопасность.

На сегодняшний день основными направлениями государственной деятельности в области обеспечения информационной безопасности являются:

установление ответственности за сохранность, засекречивание и рассекречивание информации;

формирование специальной нормативной правовой базы, регламентирующей права, обязанности и ответственность всех субъектов, действующих в информационной сфере;

определение ответственности перед законом юридических и физических лиц, собирающих, накапливающих и обрабатывающих персональные данные и конфиденциальную информацию, за их сохранность и использование;

обеспечение защиты общества от ложной, искаженной и недостоверной информации, поступающей через СМИ;

осуществление контроля над созданием и использованием средств защиты информации путем их обязательной сертификации и лицензирования деятельности в области защиты информации;

проведение протекционистской политики, поддерживающей деятельность отечественных производителей средств информатизации и защиты информации, и осуществление мер по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;

предоставление гражданам доступа к мировым информационным ресурсам, глобальным информационным сетям;

стремление к отказу от зарубежных информационных технологий для информатизации органов государственной власти и управления по мере создания конкурентоспособных отечественных информационных технологий и средств информатизации;

формирование программы информационной безопасности, объединяющей усилия государственных организаций и коммерческих структур в создании единой системы информационной безопасности;

поддержка интернационализации глобальных информационных сетей и систем.

Государство в лице его органов как основной институт политической системы занимает главное место в обеспечении национальной безопасности, в том числе информационной составляющей. Эту функцию оно осуществляет через институты президентства, законодательной, исполнительной и судебной власти, институт государственного контроля. Каждая из перечисленных структур имеет свою «нишу» в системе обеспечения национальной безопасности и выполняет возложенную на них роль в соответствии с положениями Конституции Республики Казахстан и закона «О национальной безопасности Республики Казахстан».

Проблемы обеспечения информационной безопасности органами законодательной и исполнительной власти Республики Казахстан, политическим руководством страны, учеными и практиками воспринимаются как одни из наиболее актуальных и жизненно важных для современного состояния и перспектив развития казахстанской государственности, демократии, гарантий защиты интересов общества и личности. Социально-политическая рефлексия данных проблем в значительной степени определяется динамикой современных политических процессов, связанных с формированием нового мирового порядка в условиях глобализации, объективными процессами изменения места и роли Казахстана на мировой политической арене, происходящими на фоне кризисных явлений в мировой экономике.

Система обеспечения информационной безопасности включает в себя широкий круг государственных органов, возглавляемых Президентом Республики Казахстан.

К основной функции Президента Казахстана в области информационной безопасности и соответственно национальной безопасности следует отнести его консолидирующую роль и идейные начала.

Существенные полномочия в области обеспечения информационной безопасности принадлежат парламенту и правительству Республики Казахстан.

Так, парламентом страны принят целый ряд законов, регулирующих отдельные аспекты обеспечения информационной безопасности личности, общества и государства, а также юридическая ответственность за нарушение информационных интересов, в частности законы «О государственных секретах» от 15 марта 1999 г. № 349-I; «О средствах массовой информации» от 23 июля 1999 г. № 451-I; «Об электронном документе и электронной цифровой подписи» от 7 января 2003 г. № 370-II; «О связи» от 5 июля 2004 г. № 567-II; «О техническом регулировании» от 9 ноября 2004 г. № 603-II; «Об информатизации» от 11 января 2007 г. № 217-III.

На правительство Казахстана как высший исполнительный орган власти возложены реализация государственной политики по развитию науки и техники, внедрению новых технологий, а также целый комплекс функций в области обеспечения национальной безопасности, в том числе и его информационной составляющей.

Помимо органов национальной безопасности, обеспечивающих защиту жизненно важных национальных интересов от противодействий иностранных государств, разведывательных служб, международных и иных организаций, обеспечением внутренних аспектов информационной безопасности занимается целый ряд государственных органов.

Ключевые позиции в данном аспекте занимают и центральные исполнительные органы власти Казахстана, на которые возложен ряд

специальных контрольно-надзорных и разрешительных функции по вопросам информирования и информатизации.

Технические аспекты информатизации и защиты информации возложены на Министерство транспорта и коммуникаций Республики Казахстан, являющееся центральным исполнительным органом, осуществляющим государственное регулирование в сфере информатизации и в области связи.

Таким образом, информационная безопасность является одной из ключевых составных национальной безопасности и заключается в обеспечении стабильного состояния защищенности национальных интересов страны, представляющей собой сбалансированную систему интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз. Данный вид безопасности приобретает особую значимость и актуальность в настоящее время – период перехода на новую ступень общественного развития и вхождения Республики Казахстан в мировое информационное пространство.

УДК 343.985

А.Е. Сушко

ЦЕНТР ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ КАК ЭЛЕМЕНТ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Защита граждан, их прав и свобод, интересов общества и государства входит в перечень основных задач, стоящих перед правоохранительными органами Республики Беларусь.

В условиях формирования глобальной информационной среды особую роль играет возможность эффективного противодействия преступлениям против информационной безопасности, мишенью которых становятся информационные ресурсы, принадлежащие банковскому сообществу, государственным органам и коммерческим организациям, а также конфиденциальная информация и персональные данные граждан.

Концепция национальной безопасности Республики Беларусь, утвержденная указом Президента Республики Беларусь от 9 ноября 2010 г. № 575, определяет информационную безопасность как состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере, выделяя ее в самостоятельную составляющую национальной безопасности.

К таким угрозам относятся и преступления против информационной безопасности, впервые нашедшие юридическое закрепление в Уголовном кодексе Республики Беларусь 1999 г.

Статистика уголовных дел данной категории в общем количестве преступлений такова: в 2011 г. – 1,6 %, 2012 г. – 2 %, 2013 г. – 2,6 %, среди которых несанкционированный доступ к компьютерной информации, заведомое использование вредоносных программ, компьютерный саботаж, хищение с использованием компьютерной техники и др.).

Таким образом, статистика свидетельствует об увеличении количества преступлений, выявленных в этой сфере. Тенденция роста таких преступлений присуща всем странам СНГ, Европы и иных государств, что объясняется высокими темпами развития информационных технологий.

Киберпреступность является международной проблемой, так как подобные преступления совершаются, как правило, транснациональными организованными преступными группами, члены которых используют возможности сети Интернет, легко пересекают виртуальные границы между государствами и используют несовершенство законодательств различных государств.

Таким образом, только адекватный этим вызовам уровень сотрудничества может помочь правоохранительным органам нашего государства в противодействии киберпреступности. Следует отметить, что сотрудничество должно осуществляться как на международном, так и на национальном уровне.

В Республике Беларусь в целом выстроена система противодействия киберпреступлениям.

Так, в 2012 г. в структуре центрального аппарата Следственного комитета Республики Беларусь создано управление по расследованию преступлений против информационной безопасности и интеллектуальной собственности. На сегодняшний день в областных управлениях Следственного комитета закреплены по два следователя, специализирующихся на расследовании уголовных дел указанной категории.

Раскрытием преступлений указанной категории занимаются сотрудники управления по раскрытию преступлений в сфере высоких технологий МВД, ОРПСВТ УВД и управления безопасности в сфере информационных технологий КГБ.

Изучение ряда уголовных дел показало, что в республике отсутствует единая практика расследования уголовных дел против информационной безопасности в разных территориальных подразделениях (в настоящее время в одном органе уголовное дело направляется прокурору для передачи в суд, а в другом органе при наличии, по сути, одних и тех же доказательств предварительное расследование прекращается).

Существующие в настоящее время проблемы правоприменительной практики связаны также и со сложностями квалификации действий

виновных лиц, что требует от участников процесса определенных знаний в области компьютерной техники, владения специальной лексикой, а также опыта в расследовании дел данной категории.

Не меньшую сложность представляют вопросы квалификации действий обвиняемых, что связано с отсутствием обобщенной судебной практики и официального толкования Верховного суда о применении норм УК, предусматривающих ответственность за преступления против информационной безопасности.

Анализ правоприменительной практики показывает, что в нашей стране принимаются меры, в том числе и организационного характера, по противодействию киберпреступности со стороны правоохранительных органов, однако они недостаточны ввиду быстрого развития технологий, видоизменения преступлений против информационной безопасности, отсутствия детального исследования киберпреступлений, их состояния и тенденций развития, что может сказаться на уровне защиты граждан и государства от преступных посягательств в этой сфере.

Очевидно, что в настоящее время наблюдается активное воздействие информационных технологий на так называемые традиционные составы преступлений. При совершении различных преступлений могут применяться мобильные телефоны, компьютерная техника, интернет, специальные системы и устройства, программные средства, что требует определенных навыков и знаний у оперативных сотрудников и следователей.

Обучение либо специализация при раскрытии и расследовании преступлений позволит овладеть общими положениями и техническими особенностями функционирования компьютерных систем, интернетом, тактикой проведения отдельных оперативно-розыскных мероприятий и следственных действий, в том числе осмотров различных носителей информации и интернета, установления принадлежности IP-адресов, получения движения средств по счетам различных электронных платежных систем (Easypay, Webmoney и др.), сведений об использовании банковских платежных карточек, установления «облачных» хранилищ и иных технологических сервисов, которые могут использовать преступники при совершении преступлений.

В настоящее время, на наш взгляд, необходимо создать Центр противодействия киберпреступности (далее – Центр) на базе одного из учреждений образования, в состав которого войдут представители профессорско-преподавательского состава учреждений высшего образования, сотрудники правоохранительных органов. На базе Центра как государственного правоохранительного органа целесообразно осуществлять практическое противодействие киберпреступлениям в виде выявления и расследования преступлений, исследовать уголовное пра-

во, уголовный процесс, криминалистику, проводить регулярные встречи ученых, представителей правоохранительных органов и частного сектора для обмена опытом и решения проблем, выработки стратегических подходов в борьбе с киберпреступностью, создания учебных и образовательных программ по данной тематике, проведения переподготовки и повышения квалификации следователей, оперативных сотрудников, судей, прокуроров и экспертов, в том числе осуществляющих свою деятельность не только в сфере противодействия преступлениям против информационной безопасности.

Создание и эффективное функционирование Центра позволит повысить качество расследования не только уголовных дел о преступлениях против информационной безопасности, но и иных категорий преступлений, принять дополнительные меры обеспечения защиты собственности и прав граждан, повысить уровень обеспечения информационной и национальной безопасности Республики Беларусь.

Центр должен стать платформой для сотрудничества и координации действий относительно теоретических и практических вопросов борьбы с киберпреступлениями в Беларуси, объединить экспертные знания правоохранителей, ученых, представителей частного сектора, которые смогут внести финансовый вклад в создание и деятельность организации.

В ходе первоначальных мероприятий Центра по совершенствованию действующего законодательства целесообразно с участием заинтересованных ведомств завершить разработку инициированной в 2012 г. Следственным комитетом Стратегии информационной безопасности Республики Беларусь, в которой могут быть определены угрозы в области информационной безопасности и основные мероприятия, направленные на защиту объектов критической инфраструктуры, прав граждан и государства в киберпространстве, предложены пути решения возникающих проблем, совершенствования национального законодательства в области информационной безопасности.

Оценивая опыт создания специализированных подразделений в составе различных международных правоохранительных организаций, в том числе в рамках Интерпола и Европола, занимающихся вопросами расследования киберпреступлений, необходимо рассмотреть вопрос участия белорусских правоохранительных органов, включая сотрудников Центра противодействия киберпреступности, в деятельности таких подразделений, в том числе путем подписания международных соглашений.

УДК 004:34

Т.Г. Чудиловская

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ

Развитие аппаратного обеспечения и технологий виртуализации способствуют тому, что технологии облачных вычислений (cloud computing) приобретают все большую популярность.

По определению Национального института стандартов и технологий США (NIST), официально принятому правительством США, облачные вычисления – это модель предоставления возможности удобного, осуществляемого по запросу пользователя сетевого доступа к общему фонду настраиваемых вычислительных ресурсов (таких, как сети, сервера, хранилища данных, программные приложения и услуги), которые могут быть быстро предоставлены и выделены с минимальными управленческими усилиями или взаимодействием с провайдером услуг.

Суть концепции облачных вычислений заключается в удаленном предоставлении конечным пользователям удаленного динамического доступа к услугам, вычислительным ресурсам и приложениям (включая операционные системы и инфраструктуру) через локальную сеть или интернет.

К наиболее востребованным видам облачных вычислений относятся:

SaaS (Software as a service) – программное обеспечение как сервис, т. е. клиенту предоставляется доступ к необходимому программному обеспечению как услуга.

IaaS (Infrastructure as a Service) – инфраструктура ИТ как сервис, т. е. клиенту предоставляется ИТ инфраструктура в соответствии с потребностями пользователей клиента.

PaaS (Platform as a Service) – платформа как сервис, который предназначен для разработки облачных приложений, прежде всего ориентирован на производителей программного обеспечения.

В настоящее время в передовых странах активно обсуждается и продвигается возможность использования потенциала «облачных вычислений» для решения задач в области государственного управления. Облачные вычисления открывают большие возможности использования «облачных сервисов» государственными органами, способствуют внедрению «облачных технологий» на основе стандартов, позволяют консолидировать информационные ресурсы, повышают качество предоставления государственных услуг и одновременно обеспечивают снижение затрат на ИТ.

Для перевода государственных функций в «облако» многими государствами предпринимаются конкретные действия по дальнейшему системному развитию облачных вычислений в соответствии с современным развитием технологий, разрабатываются стратегические планы развития собственных cloud-систем. В Республике Беларусь в соответствии с указом Президента Республики Беларусь от 23 января 2014 г. № 46 «Об использовании государственными органами и иными государственными организациями телекоммуникационных технологий» создается республиканская платформа на основе технологий облачных вычислений, на которой будут размещены программно-технические средства, информационные ресурсы и информационные системы всех государственных органов и иных государственных организаций. Республиканская платформа создается и размещается на базе республиканского центра обработки данных и единой республиканской сети передачи данных (ЕРСПД) и представляет собой программно-технический комплекс для распределенной обработки данных, реализующий технологии облачных вычислений и обеспечивающий взаимодействие с внешней средой. Оператором республиканской платформы является СООО «Белорусские облачные технологии». Порядок использования государственными органами и организациями республиканской платформы, действующей на основе технологий облачных вычислений, утвержден приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 28 марта 2014 г. № 26.

Одним из сдерживающих факторов при работе с облачными ресурсами являются вопросы безопасности – отсутствие контроля над серверами, вычислительными процессами, возможность утечки критично важной информации и пр.

Проблема организации защищенной среды облачных сервисов обусловлена отсутствием принятого большей частью рынка стандарта обеспечения безопасности облачных вычислений. Несмотря на существование разных сертификационных процедур, базирующихся на критериях и требованиях безопасности, единого подхода и методики для обеспечения защищенности облачных вычислений пока нет, нет и единой методики проверки адекватности защиты провайдера подобных сервисов.

Эффективное обеспечение безопасности облачных сервисов возможно при соблюдении баланса между мерами обеспечения информационной безопасности, ответственность за которые несет поставщик услуг, и средствами защиты, применяемыми клиентом. При этом необходимо учитывать требования законов, подзаконных актов и внутриведомственных нормативных документов; определить политику контроля и доступа к хранимым данным в зависимости от их типа; обеспечить конфиденциальность с целью защиты против случайного или злонамеренного доступа к информации; организовать оптимальное управление

данными (поставщики облачных услуг должны предоставлять адекватные средства обеспечения безопасности и контроля).

В набор средств защиты, обеспечивающих безопасность при использовании облачных сервисов, входят:

безопасная регистрация получателя услуги в «облаке»;

аутентификация получателя услуги в «облаке». Для обеспечения более высокой надежности часто прибегают к таким средствам, как токены и сертификаты;

защита обмена информацией между получателем услуги и «облаком». Провайдер, предоставляющий доступ к данным должен шифровать информацию клиента, хранящуюся в центре обработки данных, а также в случае отсутствия необходимости безвозвратно удалять;

электронная подпись данных;

защита от атак, связанных с подменой «облака» («фишинг», «спуфинг» и т. п.);

обеспечение доверенной среды (операционная система, в которой работает получатель услуги, должна быть свободной от вирусов, программ-шпионов и иного вредоносного софта).

УДК 351.74

В.В. Чумак

ЗАКОНОДАТЕЛЬНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАТИЗАЦИИ МИЛИЦИИ УКРАИНЫ

Последние 20 лет нормативно-правовое обеспечение информатизации милиции Украины вынуждено было развиваться в новых для страны рамках демократии и гласности и, кроме этого, в условиях стремительного производства новейших технологий. Очевидно, в связи с этим некоторые сферы информатизации милиции остаются не до конца урегулированными, что, безусловно, требует проведения анализа содержания нормативно-правовой базы.

Некоторые вопросы относительно указанной проблемы рассматривались в работах А.М. Бандурки, М.В. Ковалева, Ю.Ф. Кравченко, А.Ф. Скакун, А.Г. Фроловой т. п. Однако необходимость дальнейшего научного поиска обосновывается наличием пробелов в нормативном обеспечении, организационных и даже программно-технических недостатков в комплексе мероприятий, направленных на развитие действенной системы информационного обеспечения украинской милиции. Именно данная проблема заставляет определить целью доклада анализ нормативно-правового обеспечения информатизации милиции Украины, ко-

торый непосредственно связан с необходимостью совершенствования организации системы управления информатизацией деятельности органов внутренних дел Украины.

Нормативное регулирование информационного обеспечения управления органами внутренних дел предусматривает создание предпосылок для комплексного решения задач, стоящих перед органами внутренних дел, предоставления субъектами управления ОВД научно обоснованной информации для эффективного выполнения управленческих функций.

Надо признать, что в системе МВД Украины нормативно-правовое регулирование предполагает использование трех групп нормативно-правовых документов: законы Украины, указы Президента Украины, постановления Кабинета министров Украины; приказы и распоряжения министра внутренних дел, решения коллегии министерства; приказы руководства ГУМВД, УМВД, УМВСТ.

Современный этап развития общества характеризуется значительным ростом роли информатизации, усложнением и расширением ее задач во всех сферах человеческой деятельности, которые с успехом решаются на основе нового информационно-коммуникационного обеспечения.

Согласно закону Украины «Об основных принципах развития информационного общества в Украине» развитие информационного общества в Украине и внедрение новейших информационно-коммуникационных технологий во все сферы общественной жизни в деятельности органов государственной власти и органов местного самоуправления определяется одним из приоритетных направлений государственной политики. Однако статистические показатели неутешительны и свидетельствуют, что уровень информатизации некоторых государственных органов низкий. В связи с этим внедрению и развитию информационно-коммуникационных технологий в правоохранительных органах посвящен ряд специальных нормативно-правовых актов, в частности указ Президента Украины «О Единой компьютерной информационной системе правоохранительных органов по вопросам борьбы с преступностью».

Среди нормативных актов об информатизации милиции Украины заслуживает внимания Комплексная целевая программа борьбы с преступностью. Значительная роль в реализации данной программы принадлежит системе информационного обеспечения, которая осуществляет информационную поддержку в раскрытии, расследовании и предотвращении преступлений, установлении и розыске преступников, а также способствует раскрытию преступлений экономического характера, предоставляет многоцелевую статистическую, аналитическую и справочную информацию.

Правовое определение института информатизации ОВД Украины были конкретизированы в 1996 г. постановлением Кабинета министров Украины «О Концепции развития системы Министерства внутренних дел». Именно в указанной постановлении были определены основные принципы и положения формирования, функционирования информационных подсистем, программно-технического обеспечения, нормативно-правовой базы, защиты информации, организационно-кадрового, материально-технического и финансового обеспечения.

Также Концепция развития системы Министерства внутренних дел Украины определила, что основной целью системы информационного обеспечение ОВД Украины является всесторонняя информационная поддержка практической деятельности ОВД в борьбе с преступностью в Украине на основе комплекса организационных, нормативно-правовых, технических, программных и других подходов. Развитие данного вопроса нашло свое отражение в решении коллегии МВД Украины от 28 декабря 1999 г., на которой была принята Программа деятельности органов внутренних дел по улучшению правопорядка Украины в начале III тысячелетия и Программа информатизации органов внутренних дел Украины.

Стоит отметить, что согласно Программе информатизации органов внутренних дел Украины стремительное развитие средств компьютерной техники и информационных технологий в мировом пространстве привел к активному использованию в борьбе с преступностью компьютерных информационных систем. Именно указанной Программой информатизации органов внутренних дел Украины (далее – Программа) были установлены главные задачи по улучшению ситуации в сфере информационно-коммуникационного обеспечения милиции.

С целью разработки стратегии и основных направлений развития системы информационного обеспечения в МВД Украины был создан научно-технический совет по проблемам информатизации и современной сети связи правоохранительных органов с привлечением ведущих специалистов и ученых.

Программой предусматривалось также ежегодное финансирование информатизации органов внутренних дел Украины за счет бюджетного финансирования и внебюджетного финансирования через привлечение инвестиций, инновационных программ и пр.

Кроме того, на основании положений указанной Программы в целях развития средств компьютерного обмена информацией и распространения сети пользователей информационных подсистем разработан проект использования сети Интернет в органах внутренних дел Украины и проект компьютеризации адресных бюро и паспортных подразде-

лений в органах внутренних дел Украины. Определена также стратегия защиты информации в информационной сети ОВД Украины, которая предусматривает комплексную защиту информационной системы ОВД Украины. Как следствие, определены специальные требования к средствам компьютерной техники, передачи данных и криптографических средств, включая каналы связи для передачи конфиденциальной информации. Отметим, что в юридической литературе выделяют следующие основные способы информационной защиты: технические, программные, правовые. Интересно, что правовая защита информации характеризуется как комплекс административно-правовых и уголовно-правовых норм, которые устанавливают ответственность за несанкционированное использование данных или программных средств.

Кроме указанных направлений Программой предусмотрена интеграция информационных подсистем правоохранительных органов, согласно которой МВД Украины совместно со Службой безопасности Украины, прокуратурой, Министерством юстиции необходимо определить требования по использованию интегрированной информационно-аналитической системы правоохранительными органами Украины, создать межведомственный банк данных. В этом направлении предполагается наладить работу по обмену информацией с правоохранительными органами иностранных государств, ее накопление и использование в органах внутренних дел Украины.

Сегодня ведутся многочисленные дискуссии и имеются предложения о необходимости совершенствования нормативно-правового обеспечения информатизации милиции Украины. Учитывая же ориентиры нашей страны, одним из которых является построение демократического государства, мы не можем недооценивать реальный уровень способности государственных структур выполнять свои задачи в соответствии с действующим законодательством Украины, признавая нормативное регулирование информационно-правовых отношений неотъемлемым гарантом эффективности функционирования ОВД.

Таким образом, подводя итог всему вышесказанному, приходим к выводу, что процесс нормативного внедрения информационных технологий в органах внутренних дел только набирает силы. Однако те позитивные изменения, происходящие в последнее время, и определенные перспективные направления помогут преодолеть все препятствия в информационном обеспечении деятельности органов внутренних дел и повысить эффективность противодействия преступности и предотвращения административных правонарушений.

УДК 34:001.32

А.С. Чумакова

СОВРЕМЕННЫЕ ПОДХОДЫ К ПРОБЛЕМЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

Проблемы в сфере информационной безопасности актуальны с тех пор, как люди стали обмениваться информацией, накапливать ее и хранить. Во все времена возникала необходимость надежного сохранения наиболее важных достижений человечества с целью передачи их потомкам. В современном обществе проблемы информационной безопасности особенно актуальны, поскольку информация стала частью жизни.

Как считают многие исследователи, в настоящее время формируется и развивается информационное общество, которое характеризуется тем, что каждый гражданин может получить любую информацию в любое время и в любом месте. С массовым внедрением компьютеров во все сферы деятельности человека объем информации, хранимой в электронном виде, вырос в тысячи раз. С появлением компьютерных сетей даже отсутствие физического доступа к компьютеру перестало быть гарантией сохранности информации.

Несмотря на все возрастающие усилия по созданию технологий защиты данных, их уязвимость не только не уменьшается, но и постоянно возрастает. Поэтому актуальность проблем, связанных с защитой потоков данных и обеспечением информационной безопасности, их обработкой и передачей, все более усиливается.

В связи с эти следует раскрыть понятие «информационная безопасность». До настоящего времени ни в методологических документах, ни в нормативных правовых актах, ни среди специалистов не выработано единой формулировки. Доктрина информационной безопасности России гласит: «Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества, государства».

Практически аналогичная формулировка содержится в проекте Концепции информационной безопасности Беларуси. Под информационной безопасностью Республики Беларусь понимается состояние защищенности национальных интересов, определяющихся совокупностью сбалансированных интересов личности, общества, государства [1, с. 229].

В.И. Ярочкин определяет информационную безопасность как состояние защищенности информационной сферы общества, обеспечи-

вающее ее формирование, использование и развитие в интересах граждан, организаций, государств [2, с. 6].

В.А. Северин также близок к этому определению. Под информационной безопасностью он понимает состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз. Задачи защиты информационных ресурсов он видит в изучении форм, способов, методов выявления и предупреждения опасности в информационной сфере [3, с. 5].

Мы солидаризируемся с мнением авторов Концепции национальной безопасности Республики Беларусь, согласно которой под информационной безопасностью понимаю состояние защищенности жизненно важных интересов личности, общества и государства в сфере информационных отношений от внутренних и внешних угроз.

Республика Беларусь, являясь частью мирового сообщества, не избежала тенденции перехода к информационному обществу. В таких условиях возникают огромные проблемы в области информационной безопасности.

С.П. Алексеенко выделяет такую проблему, как информационная безопасность детей и подростков при использовании информационных технологий. Сущность данной проблемы заключается в том, что многие молодые люди находятся в информационной среде, без которой они не представляют себе жизнь. В связи с этим С.П. Алексеенко выделяет самые распространенные угрозы, с которыми сталкивается ребенок при доступе в интернет: вредоносное программное обеспечение, недостоверная информация, доступ к неприемлемому содержимому, неконтролируемые покупки и др. [4, с. 4].

Похожей проблеме уделил внимание Н.Н. Лапченко. Он рассмотрел проблемы информационной безопасности в молодежной среде [5, с. 140].

А.В. Казеев и Т.Г. Чудиловская выделили не только такую проблему, как защита национальных информационных ресурсов, но и защита от разрушающего воздействия информации, приобретающей международный масштаб и стратегический характер. Авторы уделили особое внимание подробному рассмотрению понятия «информационная война». А.В. Казеев и Т.Г. Чудиловская сделали вывод, что информационное пространство, в котором ведется информационная война, динамично и что достижение информационного доминирования требует огромных усилий [6, с. 18].

А.Г. Ляхов уделил внимание такой проблеме, как информационная безопасность социальных систем в Республике Беларусь на современном этапе. Он отмечает, что в настоящее время не существует факторов расстояния и национальных границ в рамках информационного пространства, что приводит к образованию «глобальной деревни» (по терминологии маршала Маклюэна) и актуализирует вопрос информационной безопасности за счет вовлечения в процессы в информационной сфере огромного количества участников со всего мира, действующих по собственным правилам и в своих собственных интересах [7, с. 27].

Исследованиями в данной сфере также занимался Н.Д. Микулич. Он обратил внимание на такую проблему, как степень взаимного доверия государств в сфере национальной информационной безопасности.

Н.Д. Микулич отметил, что в настоящее время в странах СНГ активно ведутся работы по созданию и развитию национальных систем электронного документооборота, имеется или создается законодательная база для обмена электронными документами с использованием технологии электронной цифровой подписи. Данные работы в каждой стране ведутся в рамках собственных планов в соответствии с выбранными технологическими и архитектурными решениями. Важнейшей задачей при создании систем электронного документооборота является обеспечение безопасности информации [8, с. 39].

В.Ф. Картель обратил внимание на такую проблему в области информационной безопасности, как защита инфраструктур и их критически важных объектов. Он отметил, что в настоящее время информация является таким же богатством страны, как производственные и людские ресурсы. От успешного решения вопросов безопасности и уровня защищенности информационной среды в сфере государственного управления, в различных отраслях промышленности, транспорта, в сфере торговли и на финансовом рынке во многом зависит конкурентоспособность белорусского государства и благополучие граждан [9, с. 85].

Таким образом, можно сделать вывод, что проблемы, связанные с повышением безопасности информационной сферы, являются сложными, многоплановыми и взаимосвязанными. Они требуют постоянного, неослабевающего внимания со стороны государства и общества. Развитие информационных технологий побуждает к постоянному приложению совместных усилий по совершенствованию методов и средств, позволяющих достоверно оценивать угрозы безопасности информационной сферы и адекватно реагировать на них.

1. Горохов А.С. О содержании понятий «информационная безопасность», «информационная война» и «информационное оружие» // Упр. защитой информ. 2004. № 2.

2. Ярочкин В.И. Информационная безопасность М. : Междунар. отношения, 2000.

3. Северин В.А. Правовое обеспечение информационной безопасности предприятия. М. : Городец, 2000.

4. Алексеенко С.П. Информационня безопасность детей и подростков при использовании современных информационных технологий // Теоретические и

прикладные проблемы информационной безопасности в Республике Беларусь : Междунар. науч.-практ. конф. (Минск, 31 марта 2010 г.) : сб. материалов. Минск, 2011.

5. Лапченко Н.Н. Проблемы информационной безопасности в молодежной среде // Социолог. исслед. 2009. № 8.

6. Казеев А.В. Об определении понятия «информационная война» А // Теоретические и прикладные проблемы информационной безопасности в Республике Беларусь : Междунар. науч.-практ. конф. (Минск, 31 марта 2010 г.) : сб. материалов. Минск, 2011.

7. Ляхов А.Г. Актуальные вопросы обеспечения информационной безопасности социальных систем в Республике Беларусь на современном этапе // Теоретические и прикладные проблемы информационной безопасности в Республике Беларусь : Междунар. науч.-практ. конф. (Минск, 31 марта 2010 г.) : сб. материалов. Минск, 2011.

8. Микулич Н.Д. Актуальные вопросы безопасности информации при трансграничном электронном взаимодействии // Теоретические и прикладные проблемы информационной безопасности в Республике Беларусь : Междунар. науч.-практ. конф. (Минск, 31 марта 2010 г.) : сб. материалов. Минск, 2011.

9. Картель В.Ф. Защита критически важных объектов информационно-телекоммуникационных инфраструктур как фактор повышения безопасности государства в информационной сфере // Теоретические и прикладные проблемы информационной безопасности в Республике Беларусь : Междунар. науч.-практ. конф. (Минск, 31 марта 2010 г.) : сб. материалов. Минск, 2011.

УДК 34:001.32

В.Б. Шабанов, Ю.И. Кашинский

СИСТЕМНЫЙ ПОДХОД К АНАЛИЗУ КРИМИНАЛИСТИЧЕСКИХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА ОСНОВЕ ТЕЗАУРУСА

Система – это совокупность взаимодействующих, относительно самостоятельных элементов, объединенных (целостность системы) выполнением некоторой общей функции, не сводимой к функциям ее компонентов. Понятие системы достаточно широко применяется в следующих отраслях знаний: криминалистика; стратегия и тактика; методология; криминалистическая техника; политика; доказательства (по уголовным, гражданским или арбитражным делам).

Термин «система» и методы системного анализа используются при исследовании правовой системы на всех ее иерархических уровнях. Системный подход лежит в основе большинства частных методов познания, является одним из способов обобщения эмпирических фактов.

Он позволяет сосредоточиться на выявлении интегративных качеств, возникающих в результате соединения элементов в целое.

Методология системного анализа закона включает в себя выявление всех системообразующих связей, факторов, конструкций, оптимизацию этих связей, т. е. улучшение качества и эффективности закона, выяснение роли и функции каждой связи в повышении целостности и эффективности закона.

Системно-компонентный аспект отражает изучение состава системы. При этом выделяются компоненты, взаимодействие которых обеспечивает целостность системы.

Системно-структурный аспект предусматривает изучение внутренних связей и взаимодействия элементов системы. Структура понимается как внутренняя форма системы.

Системно-функциональный аспект предусматривает изучение информационно-функциональных зависимостей: между компонентами данной системы; компонентами и системой в целом; системой в целом и другой системой, в состав которой она входит.

Системно-коммуникационный аспект отражает изучение системы во взаимодействии с окружающей средой, анализ возмущающих факторов.

Понятие системы может быть применено к такому важному нормативному правовому акту, как закон.

Закон – целостная совокупность взаимодействующих норм, принципов, правовых структур различного уровня и характера, выполняющих различные функции и обеспечивающих целостность и стабильность закона.

Системообразующие факторы – концепция, принципы, а также концепция управления, отражение методологии. В законе используются многие важные категории общей теории права: субъект права, механизм правового регулирования, социальные и юридические цели, общественные отношения, правоотношения и др.

Проблемы предъявляют свои требования к создаваемой ИПС, особенно к ее логической стороне, языковой основой которой является тезаурус (сокровищница знаний). Он состоит из следующих элементов:

1) тезаурус в узком смысле, в котором приводятся дескрипторы (и их синонимы) и связи между ними;

2) иерархические схемы дескрипторов, расставленные в алфавитном порядке по общим дескрипторам (по объему);

3) перечень встречающихся в тезаурусе отдельных слов со ссылками на соответствующий дескриптор.

Самый трудоемкий процесс – составление 1-й части тезауруса. При формировании 2-й и 3-й частей можно в значительной мере использовать ЭВМ.

С точки зрения поиска информации ключевым критерием подбора слов остается детальность запросов. В юридических учреждениях был проведен предварительный анализ характера возможных запросов, выявилось большое их разнообразие.

Одна из наиболее трудных задач при составлении тезауруса — раскрыть взаимные связи между понятиями. Для того чтобы при составлении большого по объему тезауруса облегчить нахождение связей между словами, их заносят на рабочие карточки со словами, с которыми они были связаны в тексте, так как очень часто в текстах родовые и видовые понятия, их антонимы и другие находятся поблизости друг от друга.

Составляются и «обратные» карточки на все понятия, являющиеся родовыми или видовыми по отношению к основному слову. В тезаурусе фиксируются следующие связи между ключевыми словами: 1) синонимия; 2) род – вид; 3) часть – целое; 4) отрицание; 5) функциональная связь; 6) подчиненность; 7) юридически существенная связь; 8) ассоциативная связь; 9) нулевая связь (фиксирует устойчивость сочетания).

Прежде всего может возникнуть вопрос, необходимо ли такое большое число связей между ключевыми словами? Как правило, тезаурусы ограничиваются двумя или тремя первыми связями из приведенного перечня. Следует отметить, что характер связей, с которыми целесообразно считаться при поиске документов, в значительной мере зависит от той предметной области, на которую рассчитана конкретная ИПС. Опыт показывает, что при поиске правовой информации нужно пользоваться всеми вышеназванными связями. Кроме того, целью создаваемой ИПС является не только поиск, но и логический анализ документов (правовых норм), для которого необходима подробная фиксация в тезаурусе логических связей между понятиями.

Рассмотрим отличительные черты отдельных связей. Синонимия в ИПС понимается в довольно широком смысле. Так, нередко к ней относят антонимы, связь между ключевыми словами, обозначающими производителя действия и само действие, а также такие случаи родовидовой связи, учет которых в рамках данной системы не представляет интереса. В тезаурусе при определении синонимов строго придерживаются логического критерия – тождественности понятия, выражаемого ключевыми словами. Связь синонимов имеет еще дополнительную функцию ввода в систему некоторых элементов грамматики. Фиксация этой связи особенно существенна в юридических текстах, поскольку модель «производитель действия – действие – результат действия» представляет типичную ситуацию. Следовательно, учитывать эту связь необходимо, особенно при логическом анализе.

Пользование связью подчиненности и юридически существенной связью обусловлено также особенностями юридических текстов.

Под связью подчиненности понимается прежде всего отношение подчиненности между учреждениями, а также между должностными лицами, если это возможно зафиксировать. Юридически существенная связь фиксируется в тех случаях, когда исходя из каких-либо юридических соображений, необходимо учесть существующую связь между понятиями, которую нельзя отнести к какой-либо из вышеуказанных связей.

Ассоциативная связь определена в ИПС отрицательно. Она фиксируется тогда, когда связь между понятиями нельзя выразить вышеназванными связями, но их учет при поиске документов может все-таки оказаться целесообразным.

Также следует отметить, что количество ассоциативных связей в тезаурусе сравнительно невелико, поскольку многие их типы, которые в других тезаурусах зафиксированы в качестве ассоциативных связей, в нашем случае выступают самостоятельными (часть-целое, функциональная связь, юридически существенная связь).

Наконец, в рубрике нулевая связь приводятся при соответствующем дескрипторе устойчивые стандартные многословные словосочетания с этим дескриптором, которые не причисляются к самостоятельным ключевым словам.

Правовой тезаурус – это лексико-семантическое собрание ключевых слов и дескрипторов, применяемых в качестве лингвистического обеспечения и использования АИПС правовой информации. Его задача состоит в том, чтобы упорядочить и привести в систему лексические средства, используемые в правотворческом процессе.

В информатике тезаурус выполняет следующие основные функции:

1) используется для организации информационного поиска (информационно-поисковый тезаурус);

2) используется как лингвистическое средство в процессе решения правотворческих задач;

3) используется как средство, измеряющее смысл сообщения;

4) выступает в качестве важнейшего средства поиска латентной информации.

Тезаурус включает ряд основных понятий.

Ключевые слова, которые наиболее полно описывают содержание правовых норм (актов) и их существенные черты. Не относятся к ключевым слова, не имеющие смысловой нагрузки, например вспомогательные, общеупотребительные, которые можно опустить без ущерба для смысла правовой нормы.

Понятие дескриптора. Дальнейшее обобщение понятий ключевого слова приводит к понятию дескриптора. Под дескриптором понимают лексическую единицу информационно-поискового языка, служащую для описания основного смыслового содержания правовой нормы или нормативною акта. Можно сказать, что дескриптор – это выделенное ключевое слово, которое представляет целую группу ключевых слов. Такие слова образуют так называемую дескрипторскую статью. В результате происходит «сжатие информации».

Таким образом, дескрипторская статья может иметь следующую структуру: заглавный дескриптор, ключевые слова из класса эквивалентности; слова, подчиненные заглавному слову; ключевые слова, ассоциированные с заглавным.

УДК 343.534

Н.А. Швед

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПОД ЗАЩИТОЙ УГОЛОВНОГО ЗАКОНА

Современный период развития общества характеризуется повсеместным практическим применением компьютерной техники во всех общественно-значимых сферах человеческой деятельности, созданием индустрии производства и обработки информации. В настоящее время информация вполне обоснованно считается стратегическим национальным ресурсом, одним из основных богатств страны, объектом и продуктом труда более половины работающих людей. Информация становится также важным объектом правоотношений, неправомерное использование которой может нанести ущерб различным субъектам. Сущность и характер общественных отношений, возникающих между различными субъектами в информационной сфере, во многом определяются особенностями и юридическими свойствами информации – основного объекта, по поводу которого и возникают эти отношения.

Основная причина необходимости поддержания информационной безопасности на должном уровне заключается в прогрессирующей информатизации общества, объективном росте социальной роли информации. Становится все более очевидным, что и общественный прогресс, и развитие каждого человека сопровождаются и даже определяются развитием окружающей информационной среды, нуждающейся в надежной защите, в том числе и уголовно-правовыми средствами.

Проблема информационной безопасности стала осознаваться учеными и практиками сравнительно недавно, прежде всего с расширением применения вычислительной техники и современных информационных технологий, позволивших относиться к информации как к ресурсу, использование или переработка которого и введение в оборот в виде информационной продукции дают существенные материальные выгоды. Ввиду широкого применения в различных сферах жизнедеятельности человеческого общества компьютерной информации и компьютерных систем, в которых или с помощью которых она обращается, в настоящее время весьма актуальна потребность в использовании мер уголовно-правового характера против общественно опасных деяний, причиняющих значительный вред безопасности компьютерной информации. Таким образом, защита информационной безопасности средствами уголовного законодательства является одной из форм правовой защиты.

Уголовный кодекс Республики Беларусь, введенный в действие с 1 января 2001 г., содержит гл. 31 «Преступления против информационной безопасности», объединяющую семь статей (ст. 349–355).

Исходя из названия главы 31 УК, просматривается родовой объект – информационная безопасность. В основе содержания понятия информационной безопасности лежит общее понятие безопасности. В словаре Д.Н. Ушакова безопасность толкуется как отсутствие опасности. В толковом словаре С.И. Ожегова и Н.Ю. Шведовой безопасность определяется как состояние, при котором не угрожает опасность, есть защита от опасности.

В юридической литературе можно встретить различные определения понятия информационной безопасности. Одни авторы рассматривают информационную безопасность через призму двойственности, т. е., с одной стороны, это невозможность причинения ущерба защищаемому объекту, с другой – это свойство самого объекта не наносить ущерба другому объекту в информационной сфере. Таким образом, например, определяют информационную безопасность Р.М. Юсупов и В.П. Заболотный, включая такие ее признаки, как состояние объекта, когда ему путем воздействия на его информационную сферу не может быть причинен существенный вред или ущерб; свойство объекта, характеризующее его способность не наносить существенного ущерба какому-либо объекту путем оказания воздействия на информационную сферу этого объекта.

С точки зрения других авторов (и их большинство), информационная безопасность – это состояние защищенности. Однако различаются подходы в определении защищаемых объектов. Например, Т.М. Аскеров и П.Л. Боровик под информационной безопасностью понимают

защищенность самой информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуре. В.А. Мазуров определяет информационную безопасность как состояние защищенности жизненно важных интересов личности, общества, государства в информационной сфере от внешних и внутренних угроз. Информационная же сфера образуется «совокупностью общественных отношений, связанных с информацией и информационной инфраструктурой как объекта интересов личности, общества и государства».

Таким образом, основное содержание понятия «информационная безопасность» сводится к состоянию защищенности жизненно важных интересов различных субъектов в информационной сфере на сбалансированной основе от внутренних и внешних угроз. Такое понимание устанавливает уголовную ответственность не только за преступления, предусмотренные в гл. 31 УК, но и в других главах УК.

Нами проведен анализ и классификация статей Особенной части УК, на основании чего выделены следующие группы преступлений, так или иначе посягающих на состояние защищенности интересов физических, юридических лиц и государства в информационной сфере. Так, в частности, в УК Республики Беларусь можно выделить группу норм (ст. 177–179, 356, 358, 373–375, 407, 408, 457, 458), предусматривающих ответственность за различные посягательства на тайну конфиденциальной информации в виде личной, семейной, врачебной, следственной, судебной, государственной и служебной тайн, тайны усыновления. В следующую группу можно объединить нарушения конституционных прав граждан в сфере обращения информации и реализации права на получение информации (ст. 203, 204, 308, 376 УК). В отдельную группу можно также выделить преступления, посягающие на информационную безопасность в экономической сфере (ст. 226^1, 227, 237, 249, 250, 254, 255 УК). Далее можно объединить преступления по принципу недостоверности информации, т. е. общественно опасные деяния, связанные с распространением (предоставлением) ложной информации (ст. 192, 340, 400, 401, 427 УК). И отдельно выделить преступления, посягающее на информацию, сосредоточенную в объектах авторских, смежных, изобретательских и патентных прав (ст. 201 УК).

Таким образом, вышеизложенное свидетельствует, что информационная безопасность может являться объектом посягательства не только преступлений, предусмотренных гл. 31 УК, но и других преступлений, круг которых весьма широк и которые можно найти в различных главах УК. Поэтому информационную безопасность как объект уголовно-правовой охраны, по нашему мнению, следует рассматривать в узком и

широком смысле слова. Информационная безопасность в широком смысле слова – это состояние защищенности интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз. Говоря об информационной безопасности в узком смысле слова, акцент, по нашему мнению, следует делать уже на защищенности самой информации. Таким образом, информационная безопасность в узком смысле, по сути, является видовым объектом преступлений, предусмотренных гл. 31 УК. Вместе с тем следует отметить нечеткость обозначения видового объекта этих преступлений законодателем, не сделавшим акцент на компьютерном характере охраняемой информационной безопасности, тогда как ученые, исходя из особенностей преступлений, предусмотренных гл. 31 УК и соответствующими главами УК других государств, называют их, как правило, компьютерными преступлениями, тем самым конкретизируя их родовой объект. Сказанное предполагает внесение корректировок в УК с целью уточнения наименования гл. 31 УК.

К сожалению, до настоящего времени в Республике Беларусь нет единых подходов к используемой в уголовном законодательстве терминологии, раскрывающей основные термины и понятия, такие, как, например, «информационная безопасность», «компьютерная безопасность», «компьютерная информация» и т. д. Такие определения, на наш взгляд, должны быть выработаны на законодательном уровне и в последующем помещены в примечании к гл. 31 УК по аналогии с некоторыми другими главами УК в целях единообразного их понимания.

УДК 34:001.32

Д.С. Якжик

ПАРАМЕТРЫ ПОРЯДКА КАК ОБЪЕКТ ПРАВОВОГО РЕГУЛИРОВАНИЯ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Посредством правового регулирования государство культивирует человеческий капитал, воспроизводимый национальной культурой. Эффективная правовая система, воздействуя на сознание членов общества, создает условия для свободного развития необходимых и подавления нежелательных для государства искусственных объектов (идеальных и материальных), создаваемых обществом в процессе освоения природы.

Источником конкурентных преимуществ являются индивидуальные уникальные, а не массовые возможности людей и организаций. Управ-

ление ими сопряжено с обработкой гигантских информационных потоков, многократно усиленных информационно-телекоммуникационными системами. При этом лавинообразно нарастает сложность объекта управления.

Сложность объекта управления определяется степенью разнообразия его структурных элементов. Разнообразие – источник нестабильности. Определенный уровень нестабильности, при котором сохраняется управляемость, необходим для эволюции. Чрезмерное разнообразие ведет к потере управляемости и разрушению системы. Управляемое разнообразие – маневренность системы.

Степень допустимого разнообразия элементов управляемой системы ограничена уровнем развития управляющей системы. Чем эффективнее управление, тем большее разнообразие допустимо, тем большей маневренностью обладает система и выше скорость ее эволюции.

В ходе эволюции системы возникают устойчивые связи между различными степенями свободы ее элементов, называемые синергиями.

Дефицит синергий в управляемой системе компенсируется непосредственным управлением и влечет гипертрофию управляющей системы. При этом возрастает доля ресурсов, потребляемых управляющей системой, что как следствие в условиях ограниченности ресурсов приводит к истощению управляемой системы.

Вместе с тем сложные системы характеризуются наличием ряда параметров, относительно слабое воздействие на которые влечет изменение состояния всей системы. Такие параметры называются параметрами порядка. Ключом к построению эффективной компактной системы управления является выявление параметров порядка и прогнозирование откликов системы на их изменения. При этом регулирование большинства иных параметров, не являющихся параметрами порядка, осуществляется посредством создания отрицательных обратных связей, ограничивающих разнообразие в управляемой системе. Наиболее распространенным методом ограничения разнообразия является стандартизация.

При работе с социальными системами важно иметь в виду то, что человек в состоянии учесть одновременно не более 5–7 факторов, влияющих на принятие решения. Он может непосредственно работать с 5–7 людьми (с остальными опосредованно).

Пример. Конструкторские бюро, в котором необходимо определить около 1500 параметров боевого самолета. Генеральный конструктор определяет 5–7 ключевых характеристик, по 5–7 заместители и т. д.

В качестве параметров порядка информационной безопасности возможно выделить следующие: используемое оборудование; используемое программное обеспечение; политика безопасности; топология

управляемой системы; уровень квалификации персонала; морально-психологическая устойчивость персонала.

Использование программно-аппаратных комплексов сторонних разработчиков подразумевает наличие недекларированных возможностей и практически исключает возможность построения полностью безопасной системы. Важно не допустить формирование иллюзии защищенности и осознавать степень зависимости и уязвимости. Основным инструментом снижения уровня рисков является система государственной сертификации, дублирование инфраструктуры управления и резервирование информационных ресурсов.

При разработке политики безопасности степень регламентации должна быть пропорциональна уровню важности информационного ресурса. Попытки предусмотреть все угрозы с низким уровнем вероятности для систем с невысоким уровнем важности приводит к созданию инструкций, соблюдение которых приводит к «итальянской забастовке». Наличие рисков не ведет к отказу от использования технологий, дающих конкурентные преимущества. Например, общая осведомленность о возможности прослушивания телефонных разговоров не влечет отказ правонарушителей от использования этого вида связи.

Топология сложной системы является основным фактором, определяющим ее реакцию на внешнее воздействие. В системе информационной безопасности важную роль играет социальная подсистема.

Математическое моделирование устойчивости социальных систем показывает, что наибольшей устойчивостью как к внешним, так и к внутренним дестабилизирующим воздействиям являются два варианта сочетаний трех компонентов: экономики, управления и идеологии.

Первое устойчивое сочетание – так называемая X-структура. Это сочетание регулируемой экономики с централизованным иерархическим управлением и приматом коллективизма в социально-психологической сфере.

Второе устойчивое сочетание – это либеральная рыночная экономика, адаптивная демократическая система управления и индивидуализм в социально-психологической сфере. Это Y-структура.

В цивилизации, к которой принадлежит наше общество, доминирует X-структура с централизованным иерархическим управлением. Принимая во внимание ограничение на количество факторов, которые может одновременно учитывать человек, получим иерархическую структуру с лидером и 3–6 подчиненными в одном коллективе. Лидер является членом коллектива. Коллектив образует кадровое ядро, обеспечивающее управление сегментом аппаратно-технических средств. Стратегическое планирование, оценка рисков, выявление угроз на ран-

них стадиях являются задачей подразделения верхнего уровня, укомплектованного экспертами.

Каждый иерархический уровень должен агрегировать информацию, выявлять наиболее важное и представлять следующему уровню только то, что необходимо, и то, чем он может управлять.

Требования к квалификации персонала определяются уровнем рисков, источником которых служит эксплуатируемая информационная система. Возможно введение процедуры дифференцированного по уровню квалификации допуска физических лиц с выдачей удостоверений единого образца (наподобие удостоверений на право выполнения работ с повышенным уровнем риска).

Морально-психологическая устойчивость членов коллектива формируется через осознание персональной ответственности и понимание методов информационного противоборства. Дополнительным сдерживающим фактором являются автоматизированные системы защиты инсайдерской информации.

Таким образом, правовое регулирование в сфере информационной безопасности должно учитывать потенциальную уязвимость программно-аппаратных комплексов (наличие недекларированных возможностей), вероятность реализации которых достигает максимума в периоды социальных потрясений. При регламентации деятельности в обычных условиях следует избегать таких мер, соблюдение которых требует от добросовестного сотрудника выполнения дополнительных формальных процедур, не создающих существенных препятствий для злоумышленника. Также следует избегать таких правовых норм, соблюдение которых повлечет «итальянскую забастовку».

Необходима регламентация деятельности в кризисных условиях. Изоляция критически важных объектов от внешних воздействий повлечет снижение оперативности управления (отсутствие удаленного доступа, сокращение количества пользователей), что потребует компенсирующих мер.

Для подразделений, обеспечивающих техническую защиту информации, предпочтительна иерархическая штатная структура с руководителем и 3–6 подчиненными, которая обладает низкой инерционностью и коротким временем реакции на угрозы. Централизованное управление имеет свойство сокращать разнообразие аппаратно-программных средств, что обеспечивает стабильную управляемость. Компактность подразделений создает условия руководителю контролировать лично реализацию управленческих решений и обеспечивает необходимый уровень обратной связи для анализа их эффективности. Более того, в компактном коллективе наиболее благоприятные условия для обеспечения персональной ответственности сотрудников за результаты своей деятельности. Каждый иерархический уровень должен агрегировать информацию, что позволяет исключить подготовку рутинных отчетов, данные из которых крайне редко используются при подготовке управленческих решений.

УДК 34:001.32

О.И. Яхнович

ОТВЕТСТВЕННОСТЬ ЗА ПОСЯГАТЕЛЬСТВА НА ПРАВОВОЙ ИНСТИТУТ СЛУЖЕБНОЙ ТАЙНЫ КАК ЭЛЕМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Одним из значимых вопросов правового регулирования феномена (объекта), а также важным структурным элементом его системы является вопрос ответственности. Именно периодичность применения ответственности является одним из показателей правовой культуры общества, его правовых идеалов. Юридическая ответственность в конечном счете лежит в основе механизмов достижения законности и правового порядка.

На сегодняшний день служебная тайна является одним из самых сложных правовых институтов для проведения научных исследований. Основная сложность обусловлена ее двойственной в соответствии с законодательством Республики Беларусь, правовой природой, а значит и вопросами применения определенных видов ответственности.

Общие положения, касающиеся ответственности в сфере служебной тайны как составляющей правовой категории «государственные секреты», содержатся в ст. 46 закона Республики Беларусь «О государственных секретах» и устанавливают, в частности, что ответственность за организацию защиты государственных секретов в государственных органах и иных организациях, осуществляющих деятельность с использованием государственных секретов, возлагается на их руководителей. В свою очередь, конкретизируют вопросы ответственности нормы Уголовного кодекса Республики Беларусь, Кодекса Республики Беларусь об административных правонарушениях, Гражданского кодекса Республики Беларусь, Трудового кодекса Республики Беларусь, Дисциплинарных уставов, некоторых иных нормативных актов.

Уголовная ответственность за преступления, направленные против правового порядка относительно информации, составляющей служебную тайну, предусмотрена нормами УК. Основной статьей, устанавли-

вающей данный вид ответственности в отношении рассматриваемого правового института, является ст. 375 УК «Умышленное разглашение служебной тайны». Диспозиция статьи указывает на содержание информации, составляющей служебную тайну (экономические, научно-технические и иные сведения), умышленное разглашение которой субъектом преступления (лицом, которому эти сведения были доверены по службе или работе) может повлечь применение адекватной меры уголовной ответственности, содержащейся в ее санкции.

Определенное отношение к уголовной ответственности в сфере служебной тайны имеют нормы ст. 178, 179, 356, 358 УК. Например, ст. 358 УК, употребляющей служебную тайну в качестве единой категории «государственные секреты», установлена ответственность за передачу, похищение, собирание или хранение с целью передачи иностранному государству, иностранной организации или их представителю сведений, составляющих государственные секреты, информации, составляющей государственные секреты других государств, переданных Республике Беларусь. При этом следует отметить, что употребление категории «государственные секреты» в отношении иных государств представляется спорным, так как в законодательстве некоторых стран такая категория отсутствует (например, в Российской Федерации, Федеративной Республике Германия).

Административный вид ответственности в отношении информации, составляющей служебную тайну, закреплен нормами КоАП. Совершение административного правонарушения должностным лицом в связи с исполнением служебных обязанностей признается согласно п. 10 ст. 7.3 обстоятельством, отягчающим административную ответственность.

В соответствии со ст. 22.13 «Разглашение коммерческой или иной тайны» умышленное разглашение коммерческой или иной охраняемой законом тайны без согласия ее владельца лицом, которому такая коммерческая или иная тайна известна в связи с его профессиональной или служебной деятельностью, если это деяние не влечет уголовной ответственности, влечет наложение штрафа в размере от 4 до 20 базовых величин. При этом указанное деяние (разглашение, в том числе служебной тайны) в соответствие с п. 9 ст. 4.5 влечет административную ответственность лишь по требования потерпевшего либо законного представителя.

Административная ответственность в отношении рассматриваемого вида тайн содержится в ст. 22.15 «Разглашение служебной тайны по неосторожности». Диспозиция данной статьи устанавливает, что разглашение служебной тайны либо утрата документов или компьютерной информации, содержащих информацию, составляющую такую

тайну, или предметов, информация о которых составляет такую тайну, совершенные по неосторожности лицом, имеющим или имевшим к ним доступ, если утрата явилась результатом нарушения установленных правил обращения с указанными документами, компьютерной информацией или предметами предусматривает применение меры административной ответственности, указанной в санкции статьи.

Как составляющая единой категории «государственные секреты», служебная тайна регулируется нормами ст. 22.7 и 22.8, устанавливающих меры административной ответственности за нарушение правил защиты, входящей в указанную категорию, информации (ст. 22.7), а также за незаконную деятельность в области защиты такой информации (ст. 22.8).

Правовая охрана служебной тайны в качестве категории «нераскрытая информация» (ст. 140 ГК) подразумевает возможность ее использования в гражданском обороте как предмет гражданско-правовых сделок и возникновение в случае их нарушения гражданско-правовой ответственности, что противоречит ее правовой сущности. Так, в соответствии с ч. 4 ст. 140 в случае незаконного ознакомления или незаконного использования, а также разглашения информации, которая составляет служебную или коммерческую тайну, физические и юридические лица, государственные органы и их должностные лица обязаны возместить ее обладателю причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки обязательству о неразглашении коммерческой тайны, трудовому договору (контракту), и на контрагентов, сделавших это вопреки гражданско-правовому договору. Очевидна спорность применения служебной тайны как объекта гражданских прав, так как указанный вид юридических тайн является исключительно объектом публичного права, тайной органов государственной власти и местного самоуправления и не может быть предметом регулирования частного права.

Нормами ТК предусмотрены дисциплинарная и материальная ответственность. Нормой ст. 12 «Основные права нанимателей» предусмотрено право нанимателя привлекать работников к данным видам ответственности. Так, согласно п. 10 ст. 53, одной из обязанностей работника устанавливается необходимость хранить служебную тайну. В случае нарушения данной обязанности, наниматель может привлечь работника к материальной ответственности, однако для этого он должен доказать факт причинения вреда, а также других условий материальной ответственности (ст. 400 ТК).

Общие положения, касающиеся дисциплинарной ответственности работников, содержатся в гл. 14 ТК. В частности, в соответствии со ст. 197,

за противоправное, виновное неисполнение или ненадлежащее исполнение работником своих трудовых обязанностей (дисциплинарный проступок) устанавливается дисциплинарная ответственность. При этом за совершение дисциплинарного проступка (например, выразившегося в нарушении обязанности хранить служебную тайну) могут устанавливаться меры дисциплинарного взыскания: замечание, выговор, увольнение (ст. 198).

Следует также отметить, что нормой ст. 204 ТК установлена возможность правовой регламентации особого порядка применения дисциплинарной ответственности в отношении работников транспорта, таможенной службы и других категорий работников с особым характером труда. В отношении работников таможенной службы, особенности дисциплинарной ответственности регламентированы указом Президента Республики Беларусь от 9 марта 2011 г. № 98 «Об утверждении Дисциплинарного устава таможенных органов Республики Беларусь».

Таким образом, в результате проведенного анализа можно сделать вывод, что неурегулированность института служебной тайны служит причиной возникновения терминологической путаницы (использование в отношении информации, составляющей служебную тайну термина «владелец» (ст. 22.13 КоАП) и термина «обладатель» (ст. 140 ГК)); категориального коллапса (использование в качестве самостоятельного термина «служебная тайна» (ст. 375 УК), категории «нераскрытая информация» (ст. 140 ГК), составляющего звена категории «государственные секреты» (ст. 358 УК); использование частноправовых методов регулирования публичных отношений.

РАЗДЕЛ 2

СОВРЕМЕННЫЕ ТЕХНИЧЕСКИЕ И ОРГАНИЗАЦИОННЫЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

УДК 621.397

В.М. Алефиренко, А.А. Борейко

ВЫБОР КОМПОНЕНТОВ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ

В настоящее время видеонаблюдение стало неотъемлемой частью комплексной системы безопасности объекта. Основными задачами систем видеонаблюдения являются: непрерывный оперативный контроль ситуации на объекте, автоматическое обнаружение несанкционированного доступа в контролируемое пространство, видеозапись тревожных событий. Современное оборудование видеонаблюдения позволяет программировать реакцию всей системы безопасности на возникающие тревожные события.

Для создания эффективной системы видеонаблюдения немаловажным фактором является выбор оборудования. Анализ представленных на рынке моделей технических средств систем безопасности показал, что они характеризуются различным числом определяющих параметров. При большом числе параметров, имеющих различные значения, представляется затруднительным выбор конкретных моделей технических средств, необходимых для построения оптимального состава системы видеонаблюдения. Для решения этой задачи может использоваться комплексный метод определения уровня качества изделий с использованием единичных показателей. В качестве единичных показателей могут использоваться значения параметров технических средств.

Для оценки комплексных показателей качества технических средств системы видеонаблюдения необходимо подготовить и преобразовать исходные данные. Для этого надо выполнить следующие операции: провести преобразование параметров, выраженных несколькими числовыми значениями, в параметры, выраженные одним значением; определить численные значения параметров, по которым информация отсутствует; выразить качественные значения параметров числом; выбрать оптимальные и критические значения параметров для нормирования; назначить параметрам коэффициенты значимости; провести нормирование коэффициентов значимости.

Параметры, выраженные несколькими значениями, можно преобразовать в отдельные параметры для каждого значения, что приведет к увеличению общего числа параметров, или провести соответствующие логические вычисления. Например, диапазон, выраженный минимальным и максимальным значениями, можно заменить диапазоном.

Для определения численных значений показателей моделей технических средств, по которым информация отсутствует, предлагается использовать среднее значение показателей по остальным моделям, по которым имеется информация и количество которых превышает число первых.

Для выражения качественных значений параметров числом можно использовать общее количество представленных данных по параметру или использовать двух-, трех- или многоуровневое назначение числовых значений от 0 до 1 для каждого данного.

Оптимальные и критические значения параметров могут быть выбраны следующим образом:

за оптимальное значение может быть взято значение на 5–10 % превышающее максимальное значение из всех значений рассматриваемого параметра, если увеличение параметра приводит к увеличению качества, или значение на 5–10 % меньше минимального значения из всех значений этого параметра, если уменьшение параметра приводит к увеличению качества;

за критическое значение может быть взято значение на 5–10 % превышающее максимальное значение из всех значений рассматриваемого параметра, если увеличение параметра приводит к уменьшению качества, или значение на 5–10 % меньше минимального значения из всех значений рассматриваемого параметра, если уменьшение параметра приводит к уменьшению качества.

Наиболее сложной операцией является назначение параметрам коэффициентов значимости, так как их числовые значения нигде не при- [illegible] группа включает параметры, характеризующие наиболее важные функциональные возможности технического средства, поэтому им присваивались коэффициенты значимости от 0,7 до 0,99 в зависимости

от важности. Вторая группа – параметры, характеризующие вспомогательные функциональные возможности технического средства, поэтому им присваивались значения от 0,4 до 0,69. Третья группа – параметры, являющиеся общепринятыми для всех технических средств (габариты, вес и т. п.) и не оказывающие существенного влияния на комплексный показатель качества технического средства, поэтому им присваивались значения от 0,01 до 0,39.

Нормирование полученных значений коэффициентов значимости может быть осуществлено путем деления каждого значения на сумму всех значений.

Предложенный подход для предварительной подготовки технических параметров компонентов системы видеонаблюдения поможет упростить получение численных значений исходных данных для расчета комплексных показателей качества, на основании которых можно выбрать конкретные модели технических средств.

Типовой состав любой системы видеонаблюдения представляет собой набор следующих основных компонентов: видеокамеры, видеорегистраторы и мониторы. В работе были проанализированы модели поворотных купольных ip-видеокамер (рис. 1), внутренних миниатюрных ip-видеокамер (рис. 2), ip-видеокамер типа Fisheye (рис. 3), 16-ти канальных ip-видеорегистраторов (рис.4), ЖК-мониторов с LED-подсветкой (рис. 5) ведущих производителей:

поворотные купольные ip-видеокамеры: № 1 3S Vision N5012; № 2 ACUMEN AiP-Y34H-03N2B; № 3 AVTECH AVM571; № 4 AXIS Q6035-E; № 5 Beward BD135; № 6 Brickcom OSD-200A; № 7 Etrovision EV8280U-MD; № 8 Everfocus EPN4220; № 9 Evidence Apix-18ZDome/M2 EXT; № 10 Hikvision DS-2DF5286-A; № 11 Rvi IPC52DN20; № 12 VIVOTEK SD8362E;

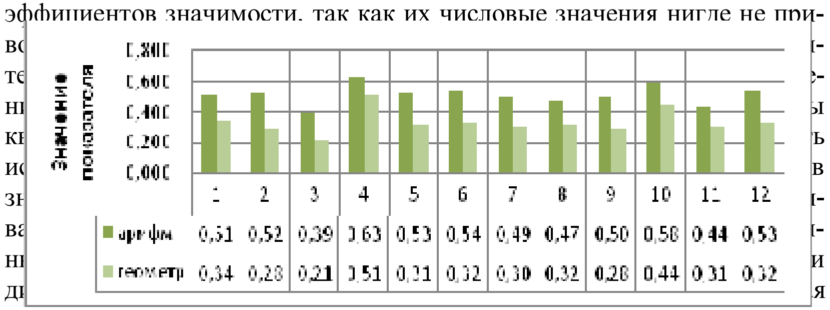


Рис. 1. Распределение показателей поворотных купольных ip-видеокамер

внутренние миниатюрные ip-видеокамеры: № 1 ACTi D11; № 2 AXIS M1054; № 3 Beward N500; № 4 HIKVISION DS-2CD8153F-E; № 5 Rvi IPC12; № 6 Sarmatt SR-IQ25F40; № 7 Tantos TSi-C211F; № 8 ViDigi S-1002f; № 9 VIVOTEK IP8133; № 10 ZAVIO F3210;

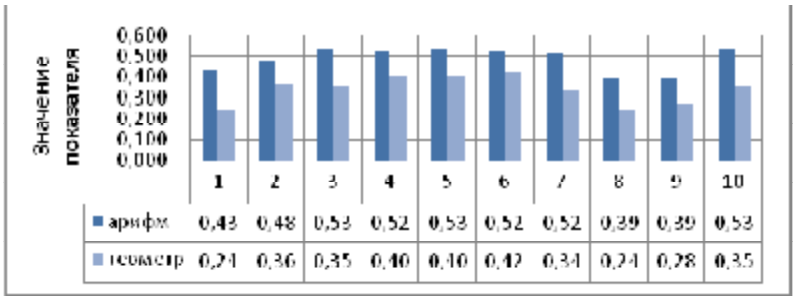


Рис. 2. Распределение показателей внутренних миниатюрных ip-видеокамер

ip-видеокамеры типа Fisheye: № 1 ACTiKCM-3911; № 2 ACUMENA iP-A54A-05Y2W; № 3 Aerica AI-501DOF; № 4 AXISM3007-PV; № 5 Etrovision N53F-F; № 6 Geovision GV-FE420; № 7 Hikvision DS-2CD783F-EP; № 8 Mobotix MX-Q24M-Sec-D11; № 9 Samsung SNF-7010P; № 10 VIVOTEK FE8172;

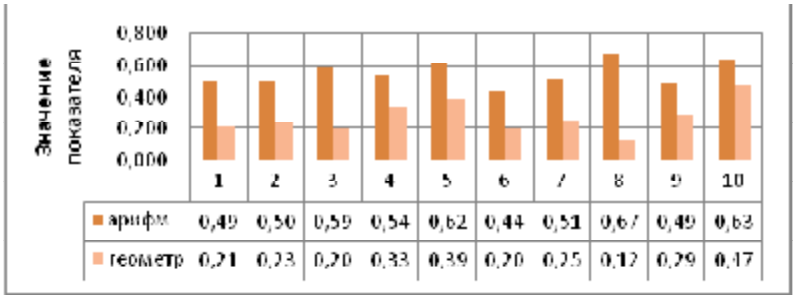


Рис. 3. Распределение показателей ip-видеокамер типа Fisheye

ip-видеорегистраторы: № 1 Brickcom NR-1604; № 2 Cyfron NV1116; № 3 EverFocus PARAGON 960; № 4 Hikvision DS-7716NI-ST; № 5 LiteView LVNR-3216C; № 6 MACROSCOPNVR-16 M; № 7 MicroDigital MDR-i016; № 8 Pinetron PNR-HD4004P; № 9 Polyvision PVDR-16NRS2; № 10 Rvi IPN16/2;

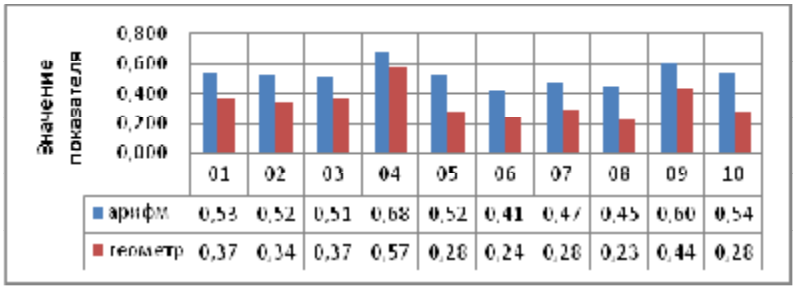


Рис. 4. Распределение показателей 16-канальных ip-видеорегистраторов

ЖК мониторы: № 1 Acer V246HLbd; №2 AOC E2495Sd; № 3 BenQ GL2460; №4 DELL S2440L; № 5 Hanns.G HL245DBB; № 6 Iiyama-ProLite E2472HD; № 7 Lenovo LS2323; № 8 LG 23EA53T-P; № 9 NEC E231W-BK; № 10 Philips 249C4QSB; № 11 Samsung S24C450B; № 12 ViewSonic VA2342-LED.

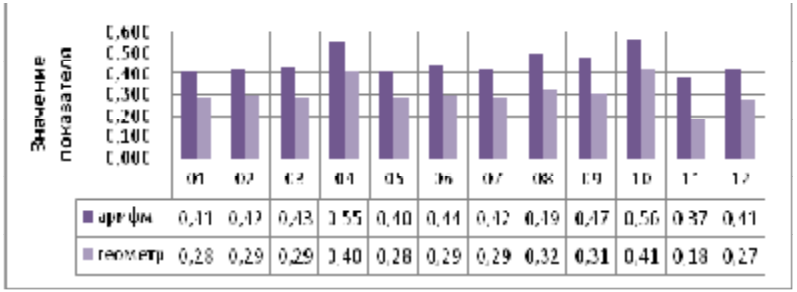


Рис. 5. Распределение показателей ЖК-мониторов с LED-подсветкой

Как видно по результатам расчетов наилучшими характеристиками по сумме показателей обладают: поворотная купольная ip-видеокамера № 4 AXIS Q6035-E, внутренняя миниатюрная ip-видеокамера № 6 Sarmatt SR-IQ25F40, ip-видеокамера типа Fisheye №10 VIVOTEKFE8172, ip-видеорегистратор № 4 Hikvision DS-7716NI-ST, ЖК-монитор № 10 Philips 249C4QSB. Предложенный метод позволяет провести выбор конкретных моделей технических средств для построения оптимальной структуры системы видеонаблюдения.

УДК 681.3

А.Н. Бабкин, А.В. Эсауленко

ОБЕСПЕЧЕНИЕ ПОМЕХОЗАЩИЩЕННОСТИ РАДИОСИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ

В настоящее время правоохранительные органы в своей деятельности активно используют различные радиосистемы передачи информации (РСПИ). Радиосистемы представляют собой совокупность базовых и абонентских радиостанций, функционирующих в условиях воздействия преднамеренных и непреднамеренных помех.

Защищенную РСПИ можно определить как систему, способную выполнять свою целевую функцию при наличии мешающих воздействий естественного происхождения и направленных действий противника.

Так как самым уязвимым элементом РСПИ является радиоканал, то основные мероприятия по защищенности системы необходимо проводить в отношении именно радиоканала.

Можно определить четыре основные требования, которым должна отвечать защищенная РСПИ:

1. Обеспечение конфиденциальности передаваемых сообщений.
2. Имитозащита радиоканала (защита от доступа к ним злоумышленников).
3. Обеспечение энергетической скрытности работы радиоканала.
4. Защита радиоканала РСПИ от радиоэлектронного подавления.

Для обеспечения конфиденциальности передаваемых сообщений в России установлен единый стандарт криптографического преобразования данных: ГОСТ 28147-89. В соответствии с этим стандартом режим шифрования, называемый режимом гаммирования, состоит в поразрядном сложении по модулю 2 передаваемых двоичных данных с двоичной шифрпоследовательностью (гаммой).

Имитозащита передаваемых данных осуществляется криптографическим методом.

Обеспечение энергетической скрытности работы радиоканала можно достичь пространственной помехозащитой, а также сигнальной помехозащитой, используя широкополосные методы модуляции.

Для количественной оценки скрытности специалисты предлагают использовать коэффициент:

$$K = \frac{R_{обн}}{R_{св}},$$

где $R_{обн}$ – радиус обнаружения работы РСПИ приемником противника; $R_{св}$ – радиус связи, определяемый окружность, в пределах которой обеспечивается требуемое отношение сигнал/шум.

В правильно спроектированной радиосети К<1. Для обеспечения этого условия необходимо применение широкополосных сигналов (ШПС) или организация передачи сообщений в спектре прикрывающих сигналов.

Как правило, применяемые в правоохранительной деятельности РСПИ работают в выделенном диапазоне частот и относятся к узкополосным системам с шириной канала связи 25к Гц или 12,5 кГц. Применить ШПС не представляется возможным.

Для наиболее ответственных РСПИ для обеспечения высоких скоростей передачи данных и помехозащиты возможно объединение нескольких каналов связи (на время передачи сообщений) в объединенный канал с шириной $\Delta F = n \times \Delta$с.ч. , где Δс.ч. – шаг сетки частот РСПИ, n – количество каналов связи с Δс.ч.

Рассмотрим энергетические характеристики и показатели помехозащищенности радиоканала РСПИ.

Для обеспечения помехозащищенности радиоканала необходимо обеспечить на выходе приемника максимальное отношение сигнала к шуму.

В качестве критерия эффективности функционирования радиоканала с точки зрения выполнения целевой функции при наличии мешающих воздействий естественного происхождения и направленных действий противника предлагается использовать отношение сигнал/шум по мощности на выходе приемника при выполнении требований по безопасности и достоверности:

$$\frac{P_c}{P_ш} \geq \left(\frac{P_c}{P_ш}\right)^{тр} \left| \begin{array}{lll} P_{ош} & \leq & P_{ош}^{тр} \\ P_{нсд} & \geq & P_{нсд}^{тр} \end{array} \right. \quad (1)$$

где $\frac{P_c}{P_ш}, \left(\frac{P_c}{P_ш}\right)^{тр}$ – соответственно отношение сигнал/шум на выходе приемника и отношение сигнал/шум требуемая, $P_{ош}$ $и P_{ош}^{тр}$ – соответственно вероятность ошибочного приема и вероятность ошибочного приема требуемая, $P_{нсд}$ и $P_{нсд}^{тр}$ – соответственно вероятность защиты от несанкционированного доступа в радиоканал и вероятность защиты от несанкционированного доступа требуемая.

При этом должно выполняться следующее соотношение:

$$\left(\frac{P_c}{P_ш}\right)^{тр} = \left(\frac{P_c}{P_ш}\right)_{\min}, \qquad (2)$$

где $\left(\frac{P_c}{P_ш}\right)_{\min}$ – минимальное (критическое) отношение сигнал/шум, при котором обеспечивается эффективность функционирования РСПИ.

На рис. 1 представлена структурная схема радиоканала, образованного передатчиком (ПРД) базовой радиостанции (БС) и приемником (ПРМ) абонентской радиостанции (АС).

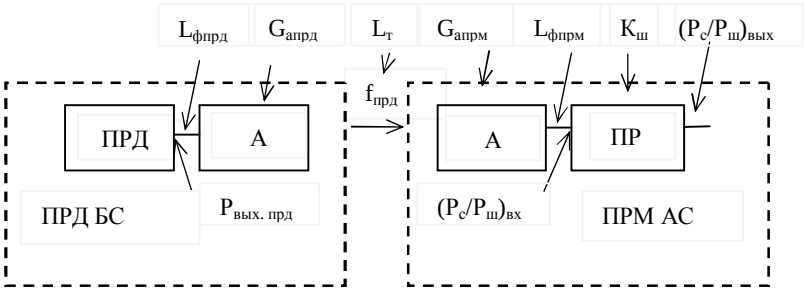


Рис. 1. Структурная схема радиоканала РСПИ

А – антенна, $P_{вых.\ прд}$ – мощность сигнала на выходе ПРД БС, дБм; $L_{фпрд}$ и $L_{фпрм}$ – соответственно потери в фидере ПРД БС и ПРМ АС, дБ, Lтр – потери сигнала на радиотрассе; дБ, $G_{апрд}$ и $G_{апрм}$ – соответственно усиление антенн ПРД БС и ПРМ АС, дБ; $(P_c/P_ш)_{вх}$ – защищенность сигнала на входе ПРМ АС, дБ; $К_ш$ – коэффициент шума ПРМ АС, дБ; $(P_c/P_ш)_{вых.}$ – защищенность сигнала на выходе ПРМ АС, дБ.

Защищенность сигнала на выходе ПРМ АС будет определяться выражением:

$$\left(\frac{P_c}{P_ш}\right)_{вых.} = \left(\frac{P_c}{P_ш}\right)_{вх} - K_ш,$$

откуда

$$P_c = \left(\frac{P_c}{P_ш}\right)_{вых} + K_ш + P_{швх},$$

где $P_{швх}$ – мощность шумов на входе ПРМ АС, дБм.

В свою очередь

$$P_c = P_{вых.прд} - L_{фпрд} + G_{апрд} - L_{тр} + G_{апрм} - L_{фпрм}$$

Помеховая обстановка, где функционируют РСПИ, может меняться, а следовательно могут меняться требования к помехозащите. С этой точки зрения необходима адаптация РСПИ к изменяющимся внешним условиям.

Необходимо предусмотреть в РСПИ наличие обратного канала между радиостанциями с возможностью анализа переданных данных и принятия решения о повышении помехозащищенности РСПИ. Системы, использующие такой канал, можно отнести к системам с обратной связью (рис. 2).

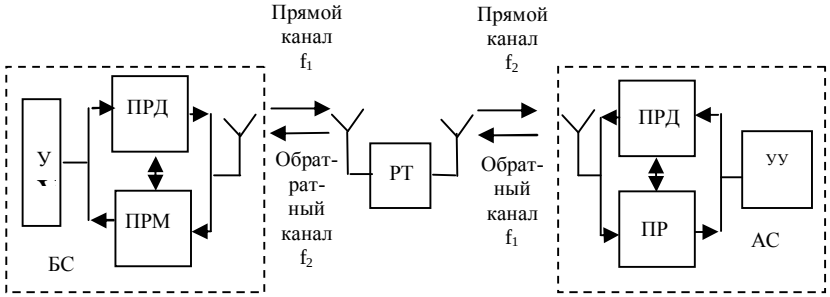


Рис. 2 Структурная схема РСПИ с обратной связью

РТР – ретранслятор, УУ – устройство управления; f_1 и f_2 – частоты работы РСПИ.

С учетом (1) и (2) для РСПИ как радиосетей, относящихся к узкополосным системам, необходимо использовать следующие способы повышения помехозащищенности:

1. Применение пространственной помехозащиты за счет формирования «нулей» диаграммы направленности антенн приемников РСПИ на источник помех, применение направленных антенн в радиоканале.
2. Передача информации в радиоканале с уровнями сигналов, отвечающих требованию (2).
3. Контроль работы радиоканала в реальных условиях эксплуатации.
4. Применение помехоустойчивого кодирования.
5. Передача полезных сигналов на фоне маскирующих сигналов.

УДК

Е.С. Б

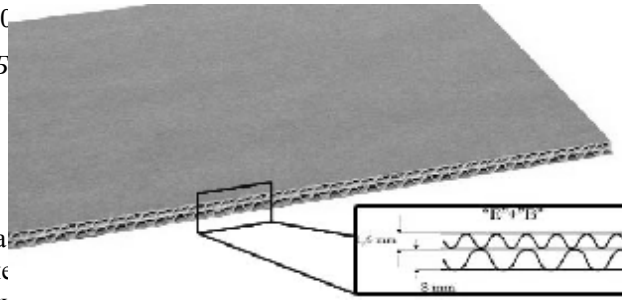


Рис. 1. Целлюлозное основание
(5-слойный листовой гофрированный картон)

На мно-
гоцел щение
утечки и несанкционированного доступа к охраняемым сведениям. Так, например, в радиоэлектронном канале передачи носителем информации является электрический ток и электромагнитное поле с частотами колебаний от звукового диапазона до десятков ГГц. Перехват электромагнитного, магнитного и электрического полей, а также электрических сигналов с информацией осуществляют органы радиотехнической разведки. Меры по защите направлены на снижение эффектив-
ной поверхности актерных участ-
ков, содержащи изнаки. Струк-
турное скрытие я объекта экра-
нами, изменяющ раженного элек-
тромагнитного ного излучения
(ЭМИ) предъяв ть, использова-
ние дешевых ма ивость к измене-
ниям температур ым материалом
для изготовлени я, так как обла-
дает высокой проводимостью. Проводимость шунгитовой породы изменяется от 265 до 1050 См/м, при этом такой широкий разброс значений проводимости объясняется неоднородностью структуры и его собственной проводимостью [2].

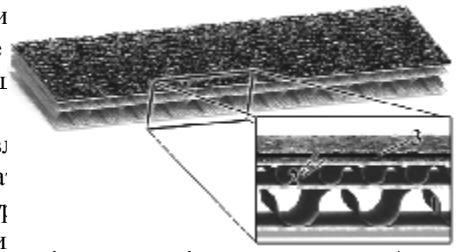


Рис. 2. Внешний вид радиопоглощающего покрытия
на гофрированном целлюлозе:
1 – проводящее облако; *2* – гофрированный картон; *3* – слой распыляемого клея; *4* – порошок шунгита

В данной работе представлены гибкие конструкции экранов ЭМИ на основе распыляемого клея и шунгита. В качестве основы для формирования композиционных радиопоглощающих материалов была выбрана целлюлоза (5-слойный листовой гофрированный картон профиля «Е+В» толщиной 4,8 мм (рис. 1)). Целлюлоза является радиопрозрачным материалом, поэтому коэффициент передачи электромагнитного излучения составляет 0… –1,8 дБ в диапазоне частот 0,7–17 ГГц.

Исследование экранирующих ЭМИ характеристик покрытия на целлюлозе проводилось с помощью измерительного комплекса ZNA 0,01–18 в диапазоне 0,7–17 ГГц. Измерения коэффициента отражения ЭМИ проводились, располагая материал целлюлозным основанием к излучателю и радиопоглощающим покрытием к измерительной антенне (рис. 3).

Коэффициент передачи ЭМИ в диапазоне частот 0,7–4 ГГц (–0,8… –1,4 дБ), с ростом частоты коэффициент отражения незначительно повышается до значений –3,9 дБ. Незначительная величина коэффициента передачи обусловлена толщиной слоя нанесения радиопоглощающего покрытия на радиопрозрачный материал.

Значение коэффициента отражения ЭМИ с металлическим отражением в диапазоне частот 0,7–4 ГГц составляет –0,13… –1,7 дБ. В диапазоне частот 4–17 ГГц при установке стороной радиопоглощающего материала к излучателю коэффициент отражения составляет 0… –10,15 дб, при установке стороной основы материала к излучателю – 0… –10,7 дБ, с выраженным резонансом на частоте 6–7 ГГц со значением коэффициента отражения с металлическим отражателем –9,3… –10,7 дБ. Как видно из рис. 5, имеется резонанс на частоте 8–8,5 ГГц, соответветсвующий полному отражению электромагнитной энергии, обусловленный слоистой структурой материала.

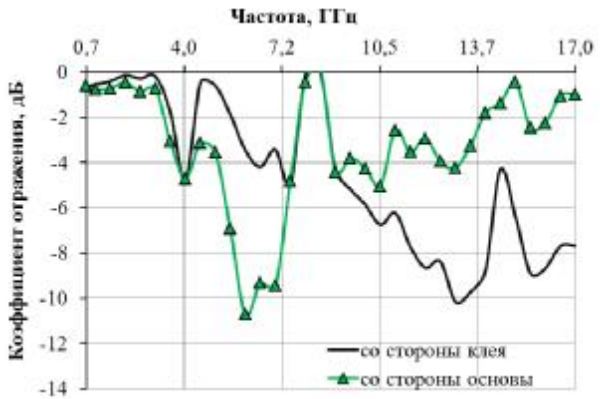


Рис. 5. Частотные зависимости коэффициента отражения с металлическим отражателем радиопоглощающего покрытия на целлюлозной основе

В дальнейшем планируется проводить исследования, направленные на понижение коэффициента отражения электромагнитного излучения до значения –10 дБ в широком диапазоне частот. При этом планируется исследовать влияние волокнистых основ и закрепление в них порошка шунгита.

1. Титов А.А. Технические средства зашиты информации. Томск : Том. гос. ун-т систем упр. и радиоэлектроники, 2010. 77 с.

2. Зайцев Г.Н., Ковалевский В.В. Влияние структуры и влажности шунгитовых пород на их электрические свойства // Геология и полезные ископаемые Карелии. Вып. 9. Петрозаводск : КарНЦ РАН, 2006. С. 135–139.

Рис. 3. Частотные зависимости коэффициента передачи радиопоглощающего покрытия на целлюлозной основе

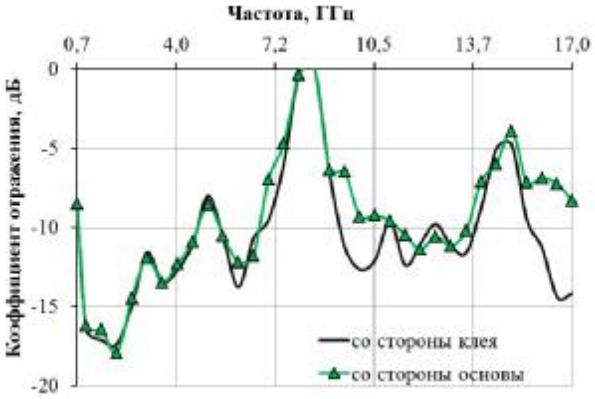


Рис. 4. Частотные зависимости коэффициента радиопоглощающего покрытия на целлюлозной основе

Коэффициент отражения радиопоглощающего материала в диапазоне частот 0,7–17 ГГц составляет 0… –17 дБ при воздействии ЭМИ на стороны основы (0… –17 дБ) с резонансом на частоте 8–8,5 ГГц, обусловлен слоистой структурой основы (целлюлозы). Значение коэффициента отражения, измеренного при установке радиопоглощающим слоем на основе клея с шунгитом к излучателю, незначительно изменяются (0… –17,9 дБ).

УДК 535.015

О.В. Бойправ, Т.В. Борботько

СПЕКТРАЛЬНО-ПОЛЯРИЗАЦИОННЫЕ ИМИТАТОРЫ ПОДСТИЛАЮЩИХ ПОВЕРХНОСТЕЙ НА ОСНОВЕ КОМПОЗИЦИОННЫХ ПЕРЛИТОСОДЕРЖАЩИХ МАТЕРИАЛОВ

Для снижения заметности объектов на фоне местностей различного типа, способствующего уменьшению вероятности утечки информации о данных объектах по оптическим каналам, используются конструкции спектрально-поляризационных имитаторов природных и антропогенных сред. Как правило, они создаются на основе композиционных материалов. Путем варьирования физических свойств компонентов этих материалов возможно управляемо изменять спектрально-поляризационные свойства конструкций имитаторов на их основе. В частности, на рис. 1 показано, что одним и таких физических свойств является размер фракций порошкообразного наполнителя. При этом тип последнего определяет особенности изменения спектрально-поляризационных свойств композиционных материалов на его основе по мере варьирования размера его фракций.

Цель работы – исследовать влияние размера фракций порошкообразного перлита на спектрально-поляризационные свойства композиционных исследованных коновый герметик

Обще алов – 3. Компози ошкообразного е порошкообразн Объемное соотноше ционном материал ечивается равно м герметике и ра змерения параметр коэффициентов ии (СП)) исследованных композиционных материалов проводились в диапазоне длин электромагнитных волн (ЭМВ) 400…1000 нм с использованием оборудования и методики (рис. 1). При этом угол падения ЭМВ составлял 45°, углы визирования – 0°, 25°, 45° и 65°. Установлено, что значения КСЯ композиционного материала типа 1 составляют в зависимости от угла визирования 0,35…0,65, на основе перлита типа 2 – 0,4…0,48, на

основе перлита типа 3 – 0,38…0,45. Увеличение угла визирования от 0° до 65° приводит к увеличению значений КСЯ исследованных композиционных материалов на 0,02…0,3 (для композиционного материала типа 1), 0,01…0,08 (для композиционного материала типа 2), 0,01…0,05 (для композиционного материала типа 3). Это позволяет сделать вывод о том, что размер фракций порошкообразного перлита оказывает влияние на индикатрису рассеяния ЭМВ композиционными материалами на его основе. Зависимости КСЯ исследованных композиционных материалов от длины взаимодействующих с ними ЭМВ (λ) при угле визирования 65° (рис. 1). Показано, что уменьшение размера фракций порошкообразного перлита приводит к снижению значений КСЯ композиционных материалов на его основе. Это связано с особенностями технологии изготовления перлита каждого из типов. Процесс получения порошкообразного перлита меньшего размера фракций сопровождается увеличением длительности обжига сырья на основе перлитовой или обсидиановой пород, что, в свою очередь, приводит к увеличению соотношения фракций черного и белого цветов в получаемом материале.

Кроме того, уменьшение размера фракций порошкообразного перлита приводит к снижению значений СП композиционного материала на его основе. Это связано с тем, что в перлите меньшего размера фракций содержится меньший объем связанной воды, характеризующейся свойством поляризации ЭМВ оптического диапазона.

Рис. 1. Зависимости КСЯ композиционных материалов типов 1 (кривая 1), 2 (кривая 2) и 3 (кривая 3) от длины взаимодействующих с ними ЭМВ

Рис. 1. Зависимости СП композиционных материалов типов 1 (кривая 1), 2 (кривая 2) и 3 (кривая 3) от длины взаимодействующих с ними ЭМВ

Композиционный материал типа 1 по своим спектрально-поляризационным характеристикам наиболее схож с сухим снегом с настом (диапазон длин волн – 400…900 нм, значения КСЯ – 0,65…0,75), композиционный материал типа 2 – с кварцевым песком (диапазон длин волн – 580…780 нм, значения КСЯ – 0,57…0,6), композиционный материал типа 3 – с известняком (диапазон длин волн – 600…780, значения КСЯ – 0,42…0,45).

С использованием измеренных значений КСЯ для исследованных композиционных материалов рассчитаны величины спектральных отличий электромагнитного излучения (ЭМИ) (ККСЯ), отраженного этими материалами и названными подстилающими поверхностями. При этом для расчета использовалась формула

$$K_{КСЯ} = \frac{\left|КСЯ_{КМ} - КСЯ_{объект}\right|}{КСЯ_{КМ} + КСЯ_{объект}},$$

где $КСЯ_{КМ}$ и $КСЯ_{объект}$ – соответственно значения КСЯ композиционного материала и подстилающей поверхности на определенной длине ЭМВ [1, 2].

Установлено, что наименьшие значения спектральных отличий ЭМИ, отраженного исследованными композиционными материалами и подстилающими поверхностями типа сухого снега с настом, известняка и кварцевого песка, составляют 0,001, наибольшие – 0,01.

Полученные результаты позволяют сделать вывод о том, что исследованные композиционные перлитосодержащие материалы пригодны для скрытия объектов на фоне подстилающих поверхностей (в том числе и в зимний период) [3].

1. Спектры отражения природных объектов – база данных [Электронный ресурс] // GIS-Lab. 2012. Режим доступа: http://radiostrim.ru/220-moh.htm (дата обращения: 14.04.2014).

2. Кринов Е.Л. Спектральная отражательная способность природных образований М. ; Л. : Изд-во АН СССР, 1937. 274 с.

3. Джамаль Саад Омер, Беляев В.С., Цикман И.М. Метод оценки оптических свойств материалов для снижения контраста объект-фон // Доклады БГУИР. 2013. № 2 (72). С. 31–37.

УДК 004.056

В.И. Воробьёв, Е.Л. Евневич, Р.Р. Фаткиева

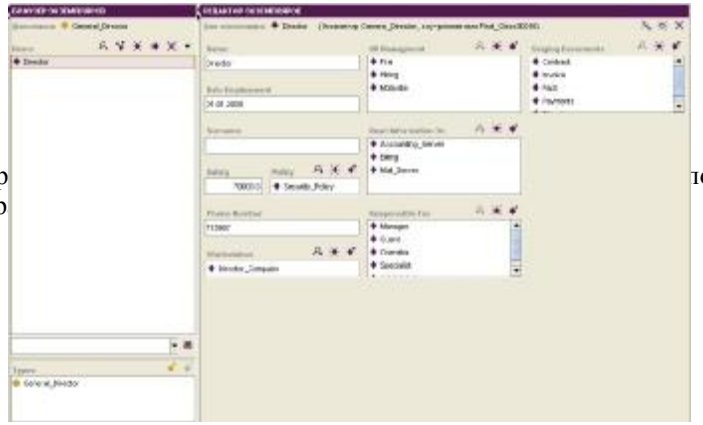
ИНСТРУМЕНТАЛЬНЫЙ АНАЛИЗ ПОЛИТИКИ И ПРОФИЛЕЙ БЕЗОПАСНОСТИ

Рассматривается система автоматизированного анализа документа «Политика безопасности» и «Профиль пользователя» предприятия. Предлагаемый анализ направлен на выявление проблемных цепочек, которые влекут за собой ошибку в способе доступа к системе, что приводит к утере или искажению корпоративной информации. Представленные на рынке программные продукты, используемые для проверки соответствия политики информационной безопасности требованиям стандарта ISO 17799: Cobra (компания C & A SystemsSecurityLtd); КОНДОР+ (компания DigitalSecurity); Метод CRAMM (CCTA Risk Analysis and Management Method); RiskWatch; ГРИФ 2006 из состава Digital Security Office и др. имеют свои недостатки, в частности невозможность установки пользователем веса на каждое требование; отсутствие русскоязычной версии; требование специальной подготовки и высокой квалификации аудитора; высокая стоимость лицензии.

Предлагается онтологическая модель политики безопасности предприятия на основе системы Protégé. Процесс создания онтологий начинается с создания «чернового варианта» политики безопасности с последующей детализацией для определения деталей, со следующей итерацией до тех пор, пока наша онтология не будет отражать концепцию предметной области с определенной степенью точности. На практике данная технология включает: определение классов в онтологии, иерархии классов (базовый класс –> подкласс); определение слотов и их допустимых значений; заполнение значений слотов для экземпляров классов.

Покажем классы онтологии на примере условного предприятия, описывающие понятия предметной области. Каждый из классов может

иметь свой подкласс, который изображает более подробное описание, чем его надкласс (рис. 1).



Пр позво-
ляет р

Рис.2. Способы хранения и доступ к информации

Носители информации: бумажные документы (счета, выписки по банку, контракты, договоры, различные важные документы, устав компании, печать, судебные акты, кадровые документы, документация отдела эксплуатации и т. д.).

Создание свойств и их ограничений позволяют специфицировать общие факты о членах классов. Различают два типа свойств: свойства-значения, отношения между представителями классов и типами данных; свойства-объекты, отношения между представителями двух классов.

Заполнение классов и слотов онтологии политики безопасности конкретными экземплярами довольно долгий процесс, поэтому покажем заполнение одной группы экземпляров. В качестве примера возьмем класс Director (генеральный директор). В начале необходимо заполнить те слоты, которые являются типом слот-значение: фамилия, имя сотрудника, стаж работы, заработная плата, рабочая станция, телефон (рис. 3).

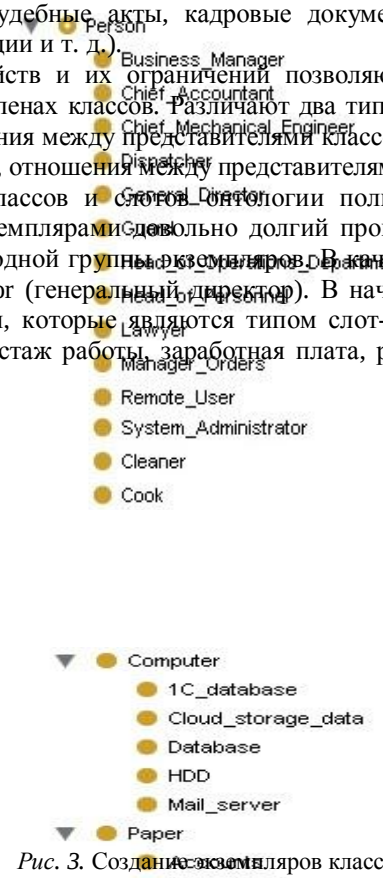


Рис. 3. Создание экземпляров класса

Используя разработанную политику безопасности, генеральный директор имеет доступ ко всем компьютерам сотрудников, подписывает документацию, организует работу сотрудников, управляет персоналом, принимает участие в формировании бюджета. Для выявления несоответствия учетной политики политике безопасности сформируем поисковые запросы. В качестве примера запроса представим запрос поиска лиц, ответственных за учет запчастей. Для этого в поле Slot выберем Other duties и соответствующий экземпляр «Ведение базы запчастей», после нажатия кнопки Find результат запроса отобразится в поле Search Results справа:

Рис.4. Создание запроса

Имеется ошибка в разграничении доступа к корпоративной информации. Онтологическая модель выявила ошибку в распределении прав доступа. К данной информации имеет право доступа (чтение/запись) только лишь бухгалтер.

Структуру представленной онтологической модели можно расширить при необходимости путем добавления большого количества сотрудников и обязанностей, сделав поиск ошибки автоматизированным.

УДК 002:004.056

А.Н. Гавриченко, Д.А. Комликов

ОСОБЕННОСТИ РАЗРАБОТКИ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА ДОВЕРЕННЫХ ЦЕНТРОВ ОБЕСПЕЧЕНИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

На сегодняшний день очень остро стоит проблема организации трансграничного обмена электронными документами и оказанию электронных услуг. Она заключается в создании доверенной инфраструктуры, содержащей центры доверенных сервисов, используемых информационными системами (ИС), юридическими и физическими лицами при трансграничном взаимодействии. При этом доверенные сервисы не должны зависеть от используемых средств электронной цифровой подписи (ЭЦП) или национального законодательства и стандартов в области ЭЦП.

Технические концепции доверенной третьей стороны (ДТС) изложены в международных рекомендациях ITU-T X.842, определяющих требования по использованию услуг доверенной третьей стороны и их управлению.

Единое пространство доверия представляет собой свод нормативных правовых, национальных и межгосударственных актов, а также технических условий для обеспечения юридической значимости электронного взаимодействия.

С технической точки зрения Единое пространство доверия при использовании ЭЦП представляет собой совокупность систем доверенных сервисов ДТС и доверенных удостоверяющих центров.

Основными функциями центров ДТС при трансграничном обмене электронными документами между сторонами являются:

проверка действительности ЭЦП на электронном сообщении (документе);

проверка валидности сертификата;

выработка штампа времени, связанного с проверкой, и отправки квитанции, подписанной ЭЦП центра ДТС.

С целью решения проблем организации трансграничного обмена электронными документами и оказания электронных услуг государственное предприятие «НИИ ТЗИ» выполнило опытно-конструкторскую работу (ОКР) «Разработка программно-аппаратного комплекса доверенных центров обеспечения электронного документооборота». Основанием для выполнения ОКР являлась программа Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий на 2011–2015 годы», утвержденная постановлением Совета Министров Союзного государства от 20 апреля 2012 г. № 6.

Результатом выполнения ОКР является программно-аппаратный комплекс «Доверие», реализующий функции доверенной третьей стороны (ПАК-ДТС).

ПАК-ДТС является технологической основой системы, реализующей функции ДТС в инфраструктуре открытых ключей (ИОК) Союзного государства.

Объектом автоматизации в ПАК-ДТС являются процессы, связанные с предоставлением услуг валидации сертификатов и электронных документов трансграничного электронного документооборота. Таким образом, услуги, оказываемые ПАК-ДТС, являются субъектами ИОК Союзного государства, предназначенными для подтверждения юридической силы электронных документов при трансграничном обмене этими документами и их архивном хранении, а также подтверждением подлинности ЭЦП, цепочек сертификатов, относящихся как к одному домену доверия (Республика Беларусь или Российская Федерация), так и к различным.

ПАК-ДТС обеспечивает автоматизацию следующих основных процессов ДТС в ИОК Союзного государства:

а) транспортировка заявок пользователей на проведение в ПАК-ДТС регламентных процедур в режиме on-line по методу POST с enctype multipart/form-data;

б) транспортировка квитанций, инкапсулируемых в MIME-объект с Content-Type нескольких видов в кодировке DER, по результатам проведения регламентных процедур в режиме on-line;

в) проведение анализа соответствия представленных пользователем в заявке данных, полученных при установлении TLS-соединения в виде CMS-сообщений;

г) выполнение в режиме on-line операций по установлению действительности сертификата, содержащегося в заявке, и построение цепочки сертификатов для проверки данного сертификата;

д) переоформление заявки для передачи ее в доверенную службу ДТС, с которой подписано соглашение об оказании услуг ДТС, и выполнение процессов перечислений е), ж);

е) передача CMS-сообщения пользователя, содержащего заявку на проведение регламентных процедур, в доверенную службу ДТС;

ж) прием от доверенной службы ДТС CMS-сообщения, содержащего квитанцию;

и) выработка ЭЦП на сформированном ответе – квитанции;

к) размещение в репозитории ДТС квитанции;

л) отправка пользователю квитанции.

При оказании услуг ДТС, связанных с подтверждением подлинности ЭЦП, цепочек сертификатов, подтверждением юридической силы и архивного хранения электронных документов, в ПАК-ДТС используются криптографические преобразования, выполняемые аппаратно-программным комплексом, реализующим криптографические сервисы (АПК-К), который обеспечивает автоматизацию следующих процессов:

генерация личных и открытых ключей подписи и идентификация;

выработка и проверка ЭЦП;

шифрование;

архивирование личных ключей подписи и шифрование с применением технологии разделения секрета;

самодиагностика и обеспечение защиты целостности программных средств АПК-К, личных ключей подписи и шифрования;

взаимодействие с программным обеспечением ПАК-ДТС по протоколу TCP/IP с поддержкой интерфейса в соответствии с СТБ 34.101.21-2009;

администрирование (настройка, конфигурирование, мониторинг, аудит) АПК-К через его внутренний веб-сервер по протоколу HTTPS;

контроль доступа для авторизованных серверов и приложений ПАК-ДТС и для администрирования АПК-К с использованием носителя ключевой информации (НКИ);

контроль попыток вскрытия корпуса АПК-К и получение от внутреннего аппаратного датчика случайной числовой последовательности АПК-К.

НКИ обеспечивает выполнение следующих функций:

самотестирование при включении электропитания;

вычисление и проверка ЭЦП в соответствии с СТБ 1176.2-99, СТБ П 34.101.45-2011;

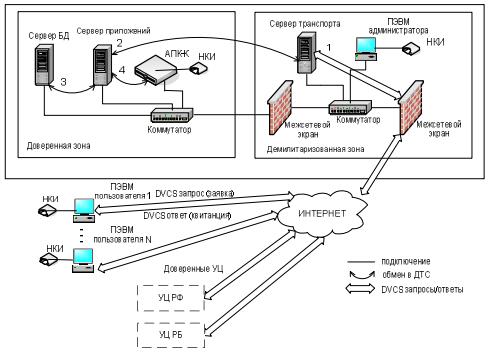
вычисление хэш-значения согласно СТБ 34.101.31-2011;

зашифрование/расшифрование информации согласно СТБ 34.101.31-2011, ГОСТ 28147-89;

хранение ключевой информации и контрольных характеристик комплекса программных средств организации защищенного канала передачи данных (идентификаторы криптоалгоритма, параметры и личные ключи шифрования и подписи, открытые ключи подписи, сертификаты открытого ключа) в энергонезависимой памяти, доступной только для чтения;

генерацию псевдослучайных чисел в соответствии с СТБ 34.101.47-2012 на базе аппаратного генератора случайных числовых последовательностей.

Схему функционирования ИС, технологической основой которой является ПАК-ДТС, можно представить в виде рисунка, где сервер транспорта обеспечивает получение и транспортировку заявок в доверенную зону ДТС, транспортировку квитанций доверенным клиентам, а также переоформление DVC-заявок для передачи их доверенному УЦ и получение от доверенного УЦ-ответа (1); сервер приложений, обеспечивает обработку DVC запросов и формирование квитанций (2); доступ к репозиторию сервера БД (3); отправку запросов в АПК-К по подтверждению ЭЦП СОК, ЭЦП электронного документа, по удостоверению ЭЦП электронного документа в целом, по удостоверению электронного документа по его хэш-значению и ЭЦП, получение ответов от АПК-К (4).



УДК 004.056.53

Г.Л. Горбачёв

ПРОБЛЕМЫ ПОДГОТОВКИ ДОКАЗАТЕЛЬСТВ ЮРИДИЧЕСКОЙ ЗНАЧИМОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ ПРИ ДОЛГОВРЕМЕННОМ ХРАНЕНИИ

Создание, использование и хранение электронных документов (ЭД) обусловливает использование ЭД в качестве официального свидетельства деловой деятельности организации.

Важность использования ЭД возрастает вследствие того, что организации все чаще фиксируют свою деятельность в электронном виде, не документируют ее на бумажных носителях, а передают ЭД на хранение в архив.

Как показывает зарубежная практика, долговременное хранение ЭД создает для организаций серьезные проблемы, так как важно сохранить не только содержание, но и юридическую значимость документов, чтобы всегда можно было доказать их пригодность при разрешении споров.

Проблема обеспечения долговременной доступности ЭД относится, прежде всего, к ЭД с постоянным сроком хранения и по личному составу, хранящимся в архивах ЭД.

Факторами, влияющими на юридическую значимость ЭД при долговременном хранении, является деградация носителей информации, устаревание программного обеспечения, оборудования, форматов.

Для предотвращения ущерба от риска, в виде невозможности использования юридически значимого ЭД при длительном хранении, необходимо, чтобы организации разработали и применяли на практике тщательно продуманную политику обеспечения долговременного хранения ЭД, направленную на обеспечение надежности этих документов, которая характеризуется достоверностью, пригодностью для использования.

Достоверным является ЭД, содержание которого можно считать полным и точным представлением подтверждаемых операций, деятельности или фактов, которому можно доверять в последующих операциях или в последующей деятельности.

Пригодным для использования является ЭД, который можно локализовать, найти, воспроизвести и интерпретировать. При воспроизведении он должен отражать связь с деятельностью или операцией, в результате которой он был создан. Контекстные ссылки в ЭД должны нести информацию, необходимую для понимания операций деловой деятельности, в которых эти документы были созданы и применялись.

Одним из элементов политики долговременного хранения являются правила, подготавливающие доказательства надежности ЭД и определяющие, каким образом осуществлялось управление ЭД при передаче в архив и хранении в архиве.

Доказательства надежности ЭД являются важными для разрешения споров, поэтому их следует хранить в архиве вместе с ЭД.

В число таких доказательств должны входить: сопроводительные документы; контрольные журналы, отражающие выполнение процедур миграции и конвертации; результаты периодически проводимых проверок по контролю сохранности ЭД; метаданные ЭД; протоколы событий.

В состав сопроводительных документов должны входить: список отозванных сертификатов; запросы на регистрацию пользователя организации, запросы на выпуск, аннулирование (отзыв), приостановление/возобновление действия сертификатов открытых ключей пользователя организации у поставщика услуг по распространению открытых ключей; запросы/ответы по проверке сертификатов.

В организации для архива ЭД должны быть разработаны документы, описывающие процедуры, направленные на сбор доказательства надежности ЭД для разрешения споров и разногласий между пользователями архива, государственными органами и архивом ЭД, а также в случае судебных разбирательств.

Обеспечение долговременного хранения ЭД и сбор доказательства надежности ЭД является комплексной проблемой. Поэтому для обеспечения функционирования архивов ЭД в Республике Беларусь необходимо разработать нормативную базу, которая должна включать технические нормативные правовые акты, охватывающие политику обеспечения долговременного хранения ЭД, проблемы конвертации ЭД в открытые форматы, защиты, учета и использования ЭД в архивах.

При разработке данных документов целесообразно использовать международный опыт и взять за основу стандарты и рекомендации США, ISO и Европейского союза в области защиты информации, управления документами и архивного дела.

УДК 004.056

В.А. Десницкий, Е.В. Дойникова

РАЗРАБОТКА КОМПОНЕНТОВ ЗАЩИТЫ ВСТРОЕННЫХ УСТРОЙСТВ С УЧЕТОМ ЭКСПЕРТНЫХ ЗНАНИЙ

Стремительный рост количества встроенных устройств и их повсеместное распространение ставят особенно остро вопросы разработки систем их защиты от широкого круга угроз информационной безопасно-

сти. Сложность проектирования защищенных встроенных устройств обусловливается во многом слабой структуризацией и формализацией знаний об информационной безопасности таких устройств. Спецификой данной области является появление новых экспертных знаний, их устаревание, сбор информации из различных источников – индустрии, исследовательских и аналитических работ в области информационной безопасности и программной инженерии, опыта работы с существующими системами, анализа защищенности систем и отдельных устройств.

Чтобы защитить эти устройства, требуется вовлечение экспертов высокой квалификации по информационной безопасности на всем протяжении процесса разработки. При этом поиск такого эксперта и предполагаемые задачи, возлагаемые на него, в общем случае значительно усложняют процесс разработки, вводя дополнительные итерации, обратные связи между разработчиком, экспертом и другими вовлеченными в процесс, а также увеличивает финансовые затраты на выполнение процесса разработки.

Вместе с тем современная тенденция в области разработки встроенных устройств – делегирование части функций экспертов разработчикам за счет применения специализированных, в том числе автоматизированных, методик и программных инструментов разработки, тестирования, оценки и анализа, т. е. знания о конкретных индустриальных системах и устройствах совместно с выявленными экспертными знаниями подвергаются обобщению и преобразуются в конкретные алгоритмы, методики и инструменты для последующего их использования разработчиками.

Еще одной тенденцией в области разработки встроенных устройств является разработка семейств устройств, в рамках каждого из которых устройства имеют некоторую общую базовую функциональность, но различаются дополнительными деталями и расширениями, определяющими особенности эксплуатации устройства и в конечном итоге его стоимость. В результате нет необходимости проводить полностью процесс проектирования для каждой разновидности устройства в рамках одного семейства с привлечением экспертов по информационной безопасности, а вместо этого следует проводить лишь адаптацию уже разработанных процедур защиты и проектирования защиты с учетом специфики конкретных устройств, что также может быть по большей части делегировано разработчику.

Цель работы – формирование, структуризация и уточнение экспертных знаний, характеризующих различные аспекты проектирования и верификации механизмов защиты встроенных устройств, а также поиск и адаптация существующих и разработка новых методик и автоматизированных программных инструментов для их последующего использования разработчиками встроенных устройств.

Выявляемые в процессе настоящего исследования знания организуются в онтологической форме с использованием среды моделирования Protégé. Особенность такого представления – унификация разнородной экспертной информации для ее последующего использования разработчиками устройств как непосредственно в процессе принятии решений проектирования, так и в качестве входных данных автоматизированных программных средств разработки.

На стадии формирования требований к защите, а также нефункциональных требований и ограничений процесс выявления экспертных знаний включает анализ существующих фундаментальных и прикладных работ, раскрывающих ключевые проблемы в области; известные модели нарушителей; индустриальных систем со встроенными устройствами в нескольких областях приложения; методологии MARTE – обобщенного онтологического представления программно-аппаратных модулей встроенных устройств и систем реального времени с использованием UML.

Источники экспертных данных о способах определения релевантных компонентов и конфигураций защиты включают информацию о конкретных базовых и комплексных компонентах защиты, типовых шаблонах защиты, а также доменно-независимых и доменно-специфичных UML-метамоделей. В качестве экспертных знаний, применяемых при комбинировании программных и программно-аппаратных компонентов защиты встроенных устройств, используются оптимизационные эвристики (в частности, эвристики порядка учета критериев ресурсопотребления), применяемые при выборе оптимальных конфигураций.

Верификация спецификаций систем со встроенными устройствами базируется на экспертной информации о потенциальных видах конфликтов и аномалий внутри конфигураций защиты устройств и применяемых политик безопасности и проводится на основе метода проверки на модели (model checking) с использованием средства верификации SPIN.

Информационный поток задается с использованием языка Promela как кортеж (*Us, Ns, Is, Ut, Nt, It, T*), где *Us* – пользователь-источник, *Ns* – хост-источник, *Is* – интерфейс-источник, *Ut* – пользователь-получатель, *Nt* – хост-получатель, *It* – интерфейс-получатель, *T* – тип передаваемой информации. Задаются также правила разрешения и запрета с учетом их приоритета как для конкретных информационных потоков, так и для групп потоков в виде кортежа с частично определенными параметрами. Верификатор SPIN позволяет выполнить процесс проверки политики разрешения/запрета информационных потоков путем модели-

рования в динамике большого количества тестовых потоков и последовательного применения к ним правил политики. Если в условиях полноты покрытия тестовых потоков было обнаружено, что какое-либо правило не сработало ни разу, то, вероятно, такое правило ошибочно. Наличие такой аномалии означает, что правило не срабатывает из-за того, что имеется одно или несколько правил с более высоким приоритетом.

К особенностям предложенной верификации можно отнести возможность гарантировать безопасность системы при условии совпадения поведения модели и реальной системы. К недостаткам можно отнести: большой объем вычислительных ресурсов, необходимый для анализа сложных моделей; ложные срабатывания, т. е. предупреждения о потенциальных информационных потоках, которых в реальной системе не будет; и неполнота, так как проверяется не реальная система, а ее модель.

Процесс верификации включает также выявление возможных скрытых несовместимостей компонентов защиты встроенных устройств. Выделяется следующие три вида несовместимостей.

Несовместимости типа 1 возникают вследствие недостаточной согласованности некоторого компонента защиты и бизнес-логики устройства. Несовместимости типа 2 представляют собой логические противоречия между функциями защиты нескольких компонентов. Несовместимости типа 3 появляются в рамках составного компонента защиты (суперкомпонента), функции защиты которого базируются на использовании нескольких подкомпонентов, входящих в его состав. Несовместимость может проявляться вследствие того, что отдельные компоненты защиты, входящие в суперкомпонент, помимо требований к устройству выдвигают также требования к другим элементам этого суперкомпонента, т. е. компоненты, представляющиеся в виде иерархической структуры, могут иметь внутренние несовместимости на разных уровнях иерархии.

Например, конфликт типа 1 возникает при наличии аппаратного модуля защищенного хранения критически важных пользовательских данных, а также требования дублирования этих данных с использованием нескольких моделей хранения в целях обеспечения их повышенной надежности. Вследствие возможности интеграции в устройство лишь одного защищенного модуля хранения данных, незащищенное дублирование данных автоматически сделает их незащищенными.

В качестве примера несовместимости типа 2 рассматривается логическое противоречие между компонентом резервного копирования и компонентом, реализующим гарантированное уничтожение хранимых на устройстве данных при наступлении определенного события. Несовместимость проявляется в том, что при встраивании в устройство

двух отдельных компонентов один из них может не обеспечивать заявленного требования из-за противоположности их действий. Такая несовместимость устраняется путем спецификации специального сценария интеграции двух компонентов и проверки корректности их совместной работы.

Примером несовместимости типа 3 является встроенное устройство, требования к которому включают реализацию избыточности хранения данных в соответствии с принципом RAID. Отметим, что формальная спецификация устройства предполагает лишь наличие одного модуля хранения данных, в результате чего обеспечение принципа RAID невозможно без изменения самой спецификации.

Потребность в поиске несовместимостей обусловливается требованиями защиты устройства, которые формулируются в процессе его проектирования. На практике выявление несовместимостей может проводиться на базе известных видов несовместимостей с учетом особенностей разрабатываемого устройства.

Работа выполняется при финансовой поддержке РФФИ (13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417), программы фундаментальных исследований ОНИТ РАН (контракт № 2.2) и проекта ENGENSEC программы Европейского сообщества TEMPUS.

УДК 004.056

Е.В. Дойникова

ВЫЧИСЛЕНИЕ ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ В СИСТЕМАХ МОНИТОРИНГА И УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ

Развитие атак на компьютерные системы и увеличение объема связанной с ними информации привело к необходимости возникновения систем мониторинга и управления безопасностью (Security In formation and Events Management, SIEM). При этом важной проблемой в рамках функционирования таких систем является выделение значимой и показательной информации и представление ее администратору системы в виде набора показателей защищенности, которые позволяют отслеживать текущую ситуацию по безопасности и определять необходимые контрмеры. Поэтому была поставлена задача разработки такой системы показателей и методик их вычисления.

Предлагаемый подход основывается на следующих аспектах: ориентированность на архитектуру SIEM-систем, анализ защищенности

системы на основе графов атак и графов зависимостей сервисов, использование иерархической системы показателей защищенности.

С точки зрения SIEM-систем были выделены следующие важные задачи: определить текущую ситуацию по безопасности компьютерной системы (сети) и поддержать решения по выбору возможных контрмер. Для решения первой задачи при вычислении показателей защищенности необходимо учитывать события безопасности, появляющиеся в системе во времени, близком к реальному. Для решения второй задачи в рамках разрабатываемой системы необходимо выделить соответствующую группу показателей, чтобы поддержать решения по выбору контрмер.

Отображение сценариев атак в виде графов позволяет отслеживать последовательность атакующих действий, пока нарушитель продвигается в целевой системе. Использование зависимостей сервисов позволяет определить влияние атак и контрмер на безопасность и функциональность защищаемой системы с точки зрения отношений доверия и функциональных отношений, реализованных в системе.

Иерархическая система показателей защищенности, предлагаемая в работе, учитывает режимы функционирования SIEM-системы (офлайн и онлайн), различные уровни представления компьютерной системы (топологический, графа атак, атакующий, события и системы), и включает показатели, основанные на последних исследованиях в области анализа защищенности.

При анализе релевантных работ в области показателей защищенности были выделены следующие основные группы показателей: топологические характеристики системы (задаются на основе топологии сети и включают, например, уязвимость хоста и критичность хоста), характеристики атаки (такие, как потенциал или вероятность атаки и ущерб от атаки), характеристики атакующего (например, уровень навыков атакующего и атрибуты атакующего, включающие его имя, позицию, квалификацию и т. п.) и интегральные (системные) показатели, отражающие уровень защищенности системы в целом (к ним относятся, например, поверхность атаки и уровень риска). Кроме того, отдельно необходимо отметить такие группы показателей как стоимостные показатели (например, ожидаемые годовые потери, общий выигрыш), показатели, отражающие возможность атак нулевого дня (например, вероятностная мера уязвимости и k-безопасность нулевого дня), и показатели, учитываемые при принятии решений по реагированию на атаку (например, эффективность реагирования, затраты на реагирование и побочные потери при реагировании).

На основе рассмотренных аспектов была разработана система показателей защищенности, включающая следующие уровни: топологический, графа атак, атакующего, событий, интегральных показателей.

Каждый уровень включает три категории показателей: основные, стоимостные и показатели 0-дня.

Взаимосвязи между уровнями определяют порядок вычисления показателей в рамках разработанного подхода и информацию, учитываемую в процессе их вычисления.

Первые три уровня относятся к статическому режиму работы системы. На топологическом уровне на основе модели системы и информации о ее слабых местах рассчитываются следующие основные показатели: уязвимость хоста, слабость хоста, внутренняя критичность, внешняя критичность, процент систем без известных критичных уязвимостей; уязвимость хоста к атакам 0-дня и ценность хоста для бизнеса (стоимостной показатель). При расчете используются как известные, так и модифицированные методики.

На уровне графа атак на основе графа атак, с учетом информации с предыдущего топологического уровня рассчитываются следующие основные показатели: критичность атакующих действий, потенциал атаки, ущерб от атаки; потенциал атаки с учетом 0-дня и стоимостные показатели: стоимостной ущерб от атаки, затраты на реагирование.

На уровне атакующего на основе профиля атакующего с учетом информации с двух предыдущих уровней рассчитываются следующие основные показатели: уровень навыков атакующего, профильный потенциал атаки; профильный потенциал атаки с учетом нулевого дня и следующие стоимостные показатели: профильный стоимостной ущерб от атаки, профильные затраты на реагирование. Профиль атакующего при этом включает уровень навыков атакующего и его потенциальные цели и может корректироваться в соответствии с информацией, полученной со следующего уровня событий.

Уровень событий относится к динамическому режиму работы системы и позволяет корректировать оценки показателей в соответствии с получаемыми событиями и тем самым отслеживать появление и развитие атаки в системе, определять профиль атакующего и прогнозировать его дальнейшие действия. На уровне событий рассчитываются следующие основные показатели: позиция атакующего, динамический уровень навыков атакующего, вероятностный уровень навыков атакующего, динамический потенциал атаки; динамический потенциал атаки с учетом нулевого дня и следующие стоимостные показатели: динамический стоимостной ущерб от атаки, динамические затраты на реагирование.

Интегральные показатели могут рассчитываться на основе показателей любого уровня различных методик, что позволяет иметь оценки разной степени точности на разных уровнях работы системы. При этом сложность алгоритмов увеличивается с ростом количества учитываемой информации. На интегральном уровне рассчитываются следующие

основе показателей: уровень риска, уровень защищенности, поверхность атаки.

Тестирование подхода, основанного на предложенных показателях, включало следующие этапы: формирование модели сети (эксперименты проводились для сетей различного объема и различной структуры зависимостей, сервисов); задание параметров (моделей атакующего, критичностей и т. п.); формирование графа атак; анализ графа атак; обработка событий безопасности и тревог. Модели атакующего определялись позицией атакующего в системе (внешний или внутренний), уровнем знаний атакующего и его целями в системе, события безопасности – соответствующим хостом системы и уровнем ущерба на хосте. Для смоделированных атак и выбранных моделей атакующих вычислялись показатели защищенности разных уровней. Результаты экспериментов показали достаточно высокую степень совпадения между заданными путями атаки и профилями атакующих и определенными на основе вычисления показателей. Тем не менее проблемой являются достаточно высокие временные затраты на уровне событий, что неприемлемо для режима работы во времени, близком к реальному, и является темой дальнейших исследований.

Работа выполнена при поддержке РФФИ (проекты 13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417) и программы фундаментальных исследований ОНИТ РАН (проект 2.2).

УДК 534.781

В.К. Железняк, И.Б. Бурачонок

АНАЛИЗ ТОНКОЙ СТРУКТУРЫ ГЛАСНЫХ ЗВУКОВ РЕЧЕВОГО СИГНАЛА ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЕМ

В ряде опубликованных работ исследованы первичные признаки речевого сигнала: период (частота) основного тона – необходимый кри... ...ка пол... ...ко о р... ...го. Изв... ...ль- ной... ...ым инф... ...ак- тер... ...ых, так и временных характеристик сигнала необходимо использовать базисные функции, обладающие свойствами частотно-временной локализации – вейвлеты.

Эффективность методики вейвлет-анализа тонкой структуры речевого сигнала рассматривались Л. Фалек, А. Амруш, Л. Фергани, Г. Теффаки, А. Джеради, С.Н. Гайказовой и др. В работе авторов В.И. Саловьева, С.В. Рыбальского, В.К. Железняка на основе базиса Морле с экспериментально установленным постоянным параметром ширины вейвлета получена объемная скейлограмма, представляющая фрагмент фонемы «а» русского языка в виде набора мультифрактальных структур. Однако применение постоянных для всех преобразований настроек вейвлета может существенно повлиять на интерпретацию результатов, так как при изменении характеристик исследуемого сигнала можно получить неполную информацию о его тонкой структуре. Таким образом, для обеспечения возможности более детального анализа возникает необходимость выбора типа материнского вейвлета и подбора его параметров. Повторив результаты эксперимента с постоянными параметрами вейвлета для других ударных и безударных изолированных гласных русского языка, воспроизведенных различными дикторами, нами дополнительно исследовано влияние изменения частотных характеристик и типа материнского вейвлета на результаты вейвлет-анализа. Проведено сравнение некоторых материнских вейвлетов, исследована информативность вейвлет-представления частотно-временной области сигнала при изменении масштабных коэффициентов a и b.

Из сравнительного анализа известными вейвлет-функциями (Гауссова типа, «Мексиканская шляпа», Морле и Меера) тонкой структуры гласных звуков русского языка получены их частотно-временные преобразования. Перечисленные вейвлеты обладают минимумом свойств, обеспечивающих полноценные возможности в технике преобразования, а также свойствами частотно-временной локализации. Из исследованных вейвлет-функций комплексный вейвлет Морле (КВМ) имеет более узкий Фурье-образ и продолжителен во временной области (рис.1). Присутствие доминирующей частоты позволяет варьировать избирательностью КВМ в частотной области.

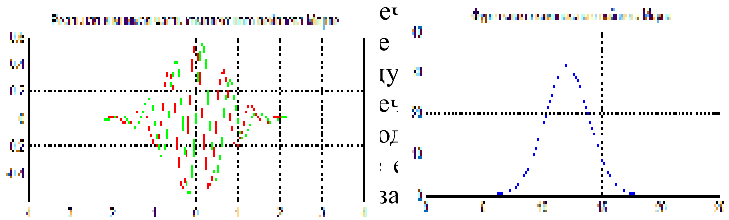


Рис. 1. Комплексный вейвлет Морле

Во временной области КВМ представляет собой комплексную экспоненту, модулируемую функцией Гаусса. В частотной же области КВМ имеет форму Гауссова окна с центральной частотой f_0 и шириной B. Таким образом, частотный диапазон, покрываемый окном КВМ, ограничен интервалом $[f_0 - B/2, f_0 + B/2]$ (полосой его пропускания), где сосредоточена наибольшая часть его энергии. Если выполнить преобразование Фурье КВМ, то оно равно нулю для отрицательных частот, что позволяет разделить фазовые и амплитудные компоненты сигнала. КВМ имеет близкое сходство с речевыми фрагментами (подобен импульсным составляющим нестационарных сигналов) и обладает частотной локализацией, лучшей среди других базисов, а значит наиболее информативен для оценки тонкой структуры речевых сигналов.

Проанализируем, как на определение тонкой структуры сигнала влияет форма материнского вейвлета. Из записанного в обычных условиях речевого сигнала (произнесенный диктором мужским голосом звук «а» длительностью 0,25 с и частотой дискретизации $f_s = 11\,025$ Гц) выделим фрагмент длительностью 0,1 с, где сосредоточены основные форманты f_1, f_2 (рис. 2).

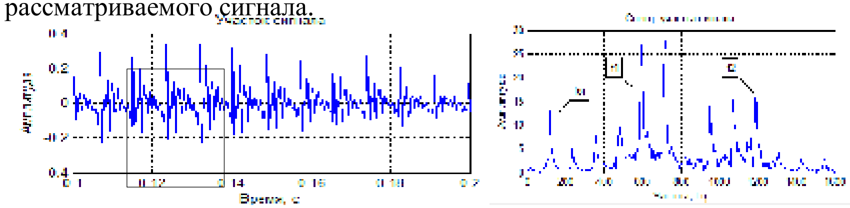


Рис. 2. Участок фонемы «а» на интервале от 0,1 до 0,2 с

Фрагмент гласного звука представим временным рядом со значениями функции, следующими друг за другом с постоянным интервалом времени Δt: $s_k = s(t_k)$, $t_k = \Delta t k$, $k = 0,1,\ldots N-1$. Рационально установим интервал временного окна $\Delta t \le 20$ *мс*, так как на данном интервале процесс можно считать квазистационарным. Оценка вейвлет-преобразования (ВП) этой последовательности проводится с помощью вейвлет-функции, причем эта функция вычисляется от множества значений аргументов a_i и b_j, которые являются масштабными коэффициентами по частоте и времени соответственно: $i = 0,1,\ldots,N_a - 1$; $j = 0,1,\ldots,N_b - 1$ -

$$W_\psi(a,b) = \frac{1}{n(a,b)} \sum_{k=0} s_k \psi^*\left(\frac{t_k - b}{a}\right),$$

где $n(a,b) = \sum_{k=0}^{N-1} e^{-\frac{1}{B}\left(\frac{t_k - b}{a}\right)^2}$, $\psi(t) = \frac{1}{\sqrt{\pi B}} e^{-\frac{t^2}{B}} e^{i2\pi f_0 t}$ – комплексный вейвлет Морле.

Оценка локального спектра энергии проводится на основании скалограммы: $S(a_i, b_j) = |W_\psi(a_i, b_j)|^2$, которую можно отобразить в трехмерном пространстве координат (a,b,S) и в виде топологической карты изображения поверхности, т. е. $S(a,b)$ в координатах (a,b) (рис. 3).

Цветовая гамма (рис. 3) наглядно демонстрирует зависимость интенсивности от изменения вейвлет-коэффициента S. Гармоники основного тона остаются устойчивыми на протяжении всего временного промежутка, в то время как выявленные гармоники высших порядков со временем затухают. Изображение вейвлет-спектров достаточно ясно выявляет наличие разномасштабной периодичности, содержащейся в анализируемых зависимостях, показывая наличие появившихся частотных составляющих, не соответствующих собственным частотам рассматриваемого сигнала.

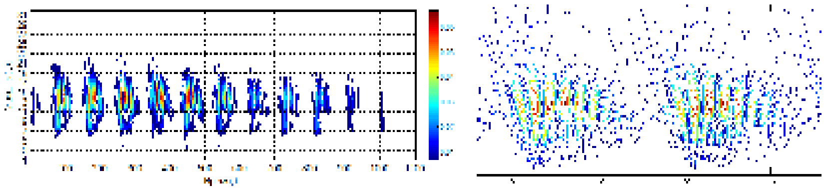


Рис. 3. Топологическая карта фонемы «а»

Можно отсечь влияние контуров, выделив те точки скалограммы, в которых она имеет максимумы по переменным *а* и *в*, построив скелетон:

$$S_c(a_i, b_j) = \begin{cases} S_{ij}, \text{ если } S_{i-1,j} < S_{i,j} > S_{i+1,j} \\ \text{или } S_{i,j-1} < S_{i,j} > S_{i,j+1} \\ 0, \text{ в остальных случаях.} \end{cases}$$

Используя скалограмму, можно провести оценку глобального спектра энергии и построить скейлограмму:

$$G(a_i) = \frac{1}{N^*} \sum_j S(a_i, b_j),$$

где N^* – число точек, по которым осуществляется осреднение.

Таким образом, при анализе ВП выделяют допороговые характеристики (в частности, спектральные) и также получить возможность оценки информативных параметров сигналов. Выбор же в качестве материнского формант за счет возможности исключения резонансных (ложных) формант. Анализ скейлограмм (рис. 4) показывает, что расположение пиков по временному параметру строго соответствует локальным экстремумам амплитуды звуковой волны во временной области, которые соответствуют всплескам амплитуды звуковой волны, заданным частотой основного тона $f_{осн}$ (рис. 2).

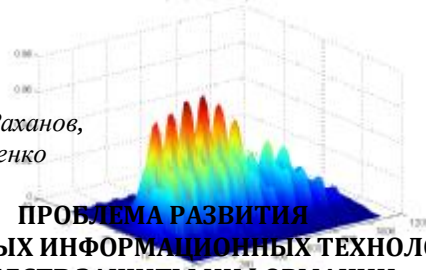
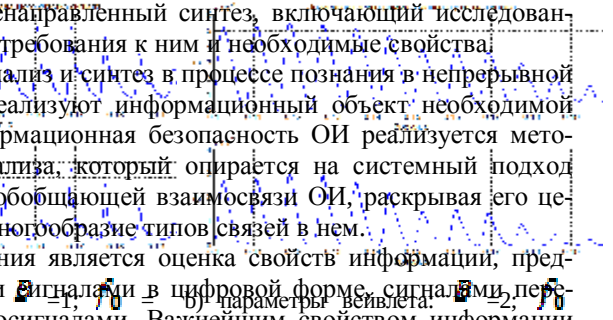


Рис. 4. Пространственная скейлограмма

В отличие от преобразования Фурье и применения других вейвлетов КВМ дает более высокую степень «гладкости» скейлограммы. Форма нормированных пиков индивидуальна при отличии характеристик голоса.

На примере фрагмента фонемы «а» продемонстрируем двумерные срезы трехмерной скейлограммы при различных значениях параметров вейвлета (рис. 5). На основании данного анализа в равной мере можно получить результаты для других фонем гласных звуков русского языка.



a) параметры вейвлета: $\beta = 1$, $f_0 = 1.5$ b) параметры вейвлета: $\beta = 2$, $f_0 = 0.5$

Рис. 5. Двумерные срезы трехмерной скейлограммы

УДК 681.327

В.К. Железняк, К.Я. Раханов,
А.В. Барков, Д.С. Рябенко

ПРОБЛЕМА РАЗВИТИЯ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Объекты информатизации (ОИ) являются многокритериальными системами, представляющими единое целое. Цель анализа таких систем – выделение новых признаков. Рациональным являются исследование входящих в нее элементов, формирующих ее конфигурационное информационное пространство. Любой объект включает взаимосвязанные предметную, энергетическую и информационные системы. Кроме внутренней информационной взаимосвязи они взаимодействуют с внешними аналогичными системами.

Непрерывным условием рациональных многокритериальных систем является их целенаправленный синтез, включающий исследованные новые признаки, требования к ним и необходимые свойства.

Таким образом, анализ и синтез в процессе познания в непрерывной связи с практикой реализуют информационный объект необходимой конфигурации. Информационная безопасность ОИ реализуется методами системного анализа, который опирается на системный подход построения модели, обобщающей взаимосвязи ОИ, раскрывая его целостность, выявляя многообразие типов связей в нем.

Предметом познания является оценка свойств информации, представляемой речевыми сигналами в цифровой форме, сигналами передачи данных и видеосигналами. Важнейшим свойством информации является ее защищенность от утечки по техническим каналам. Цель –

методологические исследования в виде морфологической модели объективного раскрытия неопределенности и оценки свойств информации.

Научное направление реализуется с использованием информационной технологии совместно с законами физики и математики, устанавливающими связь между физическими величинами и физическими процессами, их моделированием, а также теориями акустики, системотехники, радиотехники, оптики, инфракрасной техники, и, несомненно, средствами вычислительной техники и автоматизированных систем.

Безопасность информации в узком смысле – научное направление информатики, устанавливающее методологию сохранения неопределенности семантических, структурных свойств защищенности от утечки информации от НСД, вредоносных программ, а также обладающие конфиденциальностью, целостностью.

Методологическое исследование защищенности информации включает анализ моделей КУИ, методы оценки показателей КУИ и методические погрешности, обоснование измерительных сигналов, точность и меру точности оценки показателей измерительными сигналами, критериями, оценивающими меру защищенности ОИ, чувствительность аппаратно-программной системы и ее первичных измерительных преобразователей, их метрологические характеристики, сравниваемые с известными.

Точность результата измерений отображает его близость к истинной величине, сходимость результата измерений – близость друг к другу одной и той же величины, выполненные одним и тем же методом в одинаковых условиях.

Точность и достоверность утверждений опирается на обоснованные экспериментальные результаты при достаточном объеме статистических данных. Математические модели составляют элемент методологии эффективности защищенности КУИ.

В Республике Беларусь с 1 марта 2012 г. для оценки защищенности речевой информации используют методы шумового и гармонического сигналов в октавных полосах и полосах равной разборчивости.

Шумовой сигнал в качестве измерительного неадекватен речевому, не обладает оптимальностью обнаружения в условиях воздействующих факторов (например, шумы высокого уровня, искусственные помехи). Метрологические характеристики для шумового сигнала не установлены, несмотря на то, что некоторые его характеристики возможно измерить шумомером. Основные параметры речевого и шумового сигналов значительно различаются.

Гармонический сигнал научно обоснован в качестве измерительного на базе корреляционной теории разборчивости речи и апробирован в

СИА «К6-6», «ФИЛИН-А». Высокая селективность средств измерений и измерительного сигнала решает задачу достоверного выявления всех видов КУИ (акустического, виброакустического, ПЭМИН, электроакустического, ВЧ при подключении СИА к выходу НЧ-приемника).

Среди множества сложных сигналов преимуществами обладает ЛЧМ-сигнал, который позволяет расширить возможность оценки защищенности речи. Использование ЛЧМ-сигнала позволяет контролировать всю полосу частот ($^1/_3$ октавы, полосы равной разборчивости), а не только отдельные 20 точек на оси частот, в отличие от гармонического. Методами гармонического и ЛЧМ-сигналов достигнута предельная чувствительность, высокая избирательность по частоте, исключена погрешность, обусловленная неравномерностями АЧХ, повышена точность за счет снижения методической погрешности, которая зависит от совершенства метода, повышающего точность результата измерений. Предложен цветной и черно-белый тестовый видеокадр, определяющий тонкую структуру сигнала, обусловленную крупноплановыми и мелкодетальными элементами.

Обработка в частотной области случайного процесса для оценки защищенности от утечки зашумленного гармонического и видеосигналов позволила восстановить синхроимпульсы, накопить статический видеокадр и гармонический сигнал. Для маскирования статических видеокадров сформированы статические синхронные видеошумовые кадры с помощью хаотических импульсных последовательностей. Это обеспечило повышение защищенности видеосигнала пропорционально $\sqrt{n}$, где n – количество статических видеокадров. При обработке в частотной области случайного процесса для оценки неизвестных параметров одновременно n зашумленных гармонических сигналов в 20 раз быстрее по сравнению с известными методами.

Высокая достоверность, помехоустойчивость передачи речевых сигналов в цифровой форме, передача данных обусловили формирование методов и средств оценки защищенности и средств маскирования таких сигналов. Многообразие представления цифровых битовых и модулированных (тональных) сигналов в виде АМН, ЧМН, ФМН, КАМ обусловило обоснование измерительного сигнала, адаптивного к особенностям КУИ, моделям m-ичных сигналов и сигнальным конструкциям. Теоретически обоснован единый критерий численного нормированного значения величины разборчивости речи с однозначно установленным численным значением величины ошибочного приема бита вблизи предела Шеннона. На новых принципах сформированы маскирующие сигналы для аналогового и цифрового сигналов. Предложены помехоустойчивые измерительные сигналы в виде меандровой

последовательности для битовых последовательностей и ортогональный по частоте квадратурный по фазе модулированный сигнал без разрыва фазы для оценки защищенности КУИ.

Таким образом, методом статистической обработки многократных отсчетов оценивается случайная погрешность, определяющая область неопределенности исходных экспериментальных данных в КУИ, а также находится более точное усредненное значение, экспериментальные данные, анализируются погрешности обработанного результата в более узкой области неопределенности.

УДК 621.3.037.3:006.013

С.Г. Клюев

СИСТЕМНЫЕ ОСОБЕННОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

Федеральным законом Российской Федерации от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» дано следующее определение электронной подписи – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с ней и используется для определения лица, подписывающего информацию.

Исходя из данного понятий и норм указанного закона, необходимо отметить, что электронная подпись предназначена для аутентификации лица, подписавшего документ, но не для защиты документа от подделки. Безусловно, при определенных условиях электронная подпись позволяет определить факт внесения изменений в документ после момента его подписания, также, как и отпечатки пальцев могут помочь выявить преступника. Тем не менее отпечатки пальцев обычно не определяют как средство защиты от преступления. Аналогично нельзя рассматривать электронную подпись как средство защиты документа от подделки.

Одновременно с этим подлинность электронной подписи никак не связана с подлинностью электронного документа. Рассмотрим, например, письменное поручение руководителя организации на перевод денежных средств. Документ на бумажном носителе будет выполнен в единичном экземпляре и соответственно будет исполнен однократно. Совсем другая картина складывается при использовании электронной подписи. Если электронная подпись подлинная, лицо, подписавшее поручение, определено, отсутствие искажений информации в тексте поручения подтверждено, то согласно федеральному закону Российской Федерации от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» документ является равнозначным документу на бумажном носителе, подписанным собственноручно, но согласно ГОСТ Р 51141-98 «Государственный стандарт Российской Федерации. Делопроизводство и архивное дело. Термины и определения» никак не подлинным. Согласно этого же стандарту подлинный документ – документ, сведения об авторе, времени и месте создания которого, содержащиеся в самом документе или выявленные иным путем, подтверждают достоверность его происхождения. Также в стандарте указывается, что подлинник (официального) документа – первый или единичный экземпляр официального документа. А это говорит о том, что при получении копии письменного поручения руководителя организации на перевод денежных средств в виде электронного документа, подписанного электронной подписью, в настоящее время согласно действующему законодательству и стандартам лицо, ответственное за перевод денежных средств, обязано будет совершить повторный перевод, так как невозможно определить, является ли электронный документ, подписанный электронной подписью, подлинником или нет.

Таким образом, подлинность электронной подписи никак не связана с подлинностью электронного документа.

Также электронная подпись не позволяет установить отсутствие искажения в электронном документе, а является средством обнаружения его подделки. Правильность электронной подписи говорит только о том, что возможные искажения не выявлены, при этом вероятность не определить подделку электронного документа не равна нулю, хотя и очень мала.

В работах М.М. Грунтовича рассмотрены случаи, когда владелец, исходя из известных хэш-кодов двух различных сообщений, может рассчитать две пары (закрытый-открытый) ключей таким образом, что построенные на разных закрытых ключах электронные подписи этих разных сообщений будут тождественны. При наличии злого умысла владелец может отказаться от подписанного им при помощи первого закрытого ключа сообщения, утверждая, что на самом деле он подписывал второе сообщение другим закрытым ключом. По закону электронная подпись защищает от подделки и подтверждает отсутствие искажений, так что за случайное совпадение владелец не отвечает и может потребовать компенсации морального вреда.

Статистическая значимость количества ошибок в столь важных позициях ответственных документов, разрабатываемых разными коллективами и в разных странах, исключает субъективные причины. Это не отдельные результаты, которые можно было бы объяснить субъектив-

ными причинами, неудачно выбранными словами для изложения в целом правильного положения: нечеткость семантики языка позволяет по-разному понимать любое определение. Это парадоксы в исходных понятиях, лежащие на поверхности.

Системные положения существующих законов и разрабатываемых законопроектов не учитывают структурный сдвиг в электронном взаимодействии, обусловленный отказом от взгляда на компьютер как на «пишущую машинку». Еще некоторое время существующие нормативные материалы будут достаточно эффективны. Однако этот этап подходит к своему логическому завершению.

Законы отражают доминирующее в обществе представление об электронной информации и электронных документах в частности. Господствующие взгляды на электронный документ уже не соответствуют требованиям ближайшей перспективы развития и внедрения информационных технологий. Становится очевидным, что в рамках традиционного описания информационного взаимодействия между мыслящими субъектами невозможно адекватное отображение процессов в электронной среде. Существующий подход, опирающийся на понятийную базу обмена информацией посредством традиционного (аналогового) документа, не соответствует требованиям перспективного этапа развития электронного взаимодействия.

Исходя из вышесказанного, можно сказать, что в настоящее время назрела необходимость исследования системных особенностей электронного документа, его отличий от традиционного, разработка новой модели электронного документа.

УДК 614.8

А.Н. Ковалевич

СОВРЕМЕННЫЕ СПОСОБЫ ПРОТИВОДЕЙСТВИЯ КРАЖАМ ЭЛЕКТРОННЫХ СРЕДСТВ ПОСРЕДСТВОМ СКИММЕРА

В современном мире информационные технологии активно входят в нашу повседневную жизнь. Появляются технические средства, которые могут нанести вред информационной безопасности. Одним из таких средств является скиммер – миниатюрное считывающее переносное устройство, которое крепиться к банкомату с помощью обычного скотча.

Например, только за 2013 г. в США зафиксировано более 20 тыс. скимминговых атак, по сути преступлений. Аналогичная ситуация и в

странах Европы (ежегодные потери европейский банков составляют примерно 300 млн евро).

Масштабы данных уголовных преступлений в данном направлении растут, к сожалению, ежегодно. Лидерами по количеству денежных средств, украденных с пластиковых носителей, являются США и Великобритания. В странах Латинской Америки число подобных преступлений за последние четыре года выросло на 15 %.

Ситуацию по данному направлению правоохранительные органы Республики Беларусь контролируют. Однако правоприменители уже обращают внимание общественности на тот факт, что в нашей стране активно применяются гражданами свыше 10 млн банковских пластиковых карточек для ведения различного рода операций с денежными средствами. Как следствие, из-за значительного объема платежных средств количество преступлений в Беларуси, связанных с кредитными картами, пусть и незначительно, но растет. Так, например, только в 2012 г. было выявлено более 2 тыс. преступлений по ст. 212 «Хищение путем использования компьютерной техники» УК Республики Беларусь. Именно под эту норму УК подпадают преступные действия граждан, связанные с незаконным оборотом банковских карт.

Следует отметить, что пластиковые карты с магнитными лентами имеют низкий уровень защиты, а карты с чипом более безопасные. В связи с этим Российская Федерация уже делает первые шаги в решении данной проблемы. Ряд крупнейших российских банков с 1 июля 2013 г. уже отказались от выпуска карт, имеющих только магнитную полосу. И теперь все новые карты VISA и MasterCard оборудуются чипом. Эта мера позволяет значительно повысить уровень безопасности хранящихся на карте данных и является действенным методом борьбы со скиммингом.

Следует отметить, что в ряде стран Европы уже применяются только карты с чипом (Германия, Франция, Голландия и др.). В Японии, например, банки начали предоставлять клиентам доступ к их счетам только по отпечаткам их ладони (в 2012 г. в стране было уже установлено 18 таких банкоматов). Работа такого устройства обеспечивается за счет уникального считывателя биометрической информации и индивидуального рисунка руки человека. В целях повышения безопасности существует ряд программных антискиммеров. Это специальные аппаратные комплексы, которые очень быстро обнаруживают посторонние предметы на карте-приемнике. Несколько сообщений подряд о сбоях в работе картридера либо ошибки карты автоматически активизируют механизм ее блокировки. После этого преступник даже не сможет вынуть скимминговое устройство из картридера, не разломав его. Карта

при этом не может быть извлечена посторонними лицами – требуется вмешательство сервисных инженеров.

Иные программные антискимминговые устройства представляют собой специальную плату либо блок, который устанавливается внутри банкомата. Датчики обнаруживают магнитные поля, излучаемые скимминговым устройством и видеокамерой (для подглядывания ПИН-кода), блокируют часть функций банкомата (например, прием карты) и подают скрытый сигнал в службу безопасности банка. Банкомат снова начнет работать только после выезда на место инженеров и специалистов по безопасности для удаления антискимминговых устройства. Физический мониторинг банкоматов включает в себя периодический осмотр банкомата сотрудниками банка, инкассаторами либо специалистами сервисной службы. Банк устанавливает на картоприемник специальные антискимминговые накладки, препятствующие установке посторонних устройств. Накладка может быть подключена к специальному датчику, который срабатывает в случае попытки мошенника снять антискиммер с банкомата. Это самый дорогой, но эффективный способ борьбы со скиммингом. Устройство устанавливается внутри банкомата и незаметно снаружи. Активный антискиммер контролирует пространство перед банкоматом и позволяет моментально выявить несанкционированную установку на него посторонних устройств. Антискиммер может также создавать радиопомехи в области щели картоприемника, препятствующие работе данных устройств. Датчики антискиммера позволяют анализировать электромагнитное поле в зоне размещения картридера, ПИН-клавиатуры и монитора и в случае резкого изменения напряженности поля (включения излучающих устройств при радиопередаче, установки постороннего оборудования) устройство подает команду на управляющий блок банкомата, который выводится из режима обслуживания клиентов. Все эти варианты достаточно повышают безопасность электронных платежных средств, но и требуют значительных существенных затрат. Каждая пластиковая карточка привязана к определенному номеру мобильного телефона, в качестве решения данной проблемы можно ввести специальный сеансовый пароль при снятии денежных средств. Операция будет осуществляться следующим образом: когда клиент подходит к банкомату и хочет снять определенную сумму денег либо осуществить любой другой платеж, посылает пластиковую карточку в карт-приемник, ему на мобильный телефона в автоматическом режиме приходит сообщение, которое содержит сеансовый пароль для входа в систему, тем самым проходя процедуру идентификации помимо стандартного ввода ПИН-кода. Данный способ также имеет свои существенные

минусы, например затрата большего количества времени, неумение населения пожилого возраста пользоваться мобильными устройствами.

Таким образом, исходя из рассмотренных выше вопросов противодействия кражам электронных средств посредством скиммера, данная проблема для правоохранительных органов и банковских систем не только Республики Беларусь, но и для иных (прежде всего развитых) стран начинает приобретать значительную актуальность в вопросе информационной безопасности государства.

УДК 002:004.056

Д.А. Комликов, А.Н. Гавриченко

ОСОБЕННОСТИ РАЗРАБОТКИ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА МЕЖГОСУДАРСТВЕННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ОТКРЫТЫМИ КЛЮЧАМИ

Для решения задач, связанных с предоставлением основных сервисов удостоверяющего центра (УЦ) инфраструктуры открытых ключей (ИОК), для обеспечения юридически значимого обмена электронными документами между юридическими и физическими лицами Республики Беларусь и Российской Федерации Государственное предприятие «НИИ ТЗИ» выполняет опытно-конструкторскую работу (ОКР) «Разработка программно-аппаратного комплекса доверенных центров обеспечения электронного документооборота». Основанием для выполнения ОКР являлась программа Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий на 2011–2015 годы», утвержденная постановлением Совета Министров Союзного государства от 20 апреля 2012 г. № 6.

Результатом выполнения ОКР является программно-аппаратный комплекс «Инфраструктура», который служит технологической основой для межгосударственной системы управления открытыми ключами (далее – ПАК-МСУОК).

Объектом автоматизации в ПАК-МСУОК являются процессы, связанные с предоставлением услуг УЦ ИОК Союзного государства для обеспечения юридически значимого обмена электронными документами между юридическими и физическими лицами Республики Беларусь и Российской Федерации.

ПАК-МСУОК обеспечивает автоматизацию следующих основных процессов управления открытыми ключами в ИОК Союзного государ-

ства: формирование запроса на издание сертификата открытого ключа (СОК);издание СОК и списка отозванных сертификатов (СОС); распространение СОК; отзыв СОК; приостановление и возобновление действия СОК; предоставление информации о статусе СОК; достоверное подтверждение принадлежности открытого ключа определенному юридическому или физическому лицу; электронный нотариат; генерация личных и открытых ключей подписи и идентификации (шифрования); выработка и проверка электронной цифровой подписи (ЭЦП); выпуск и управление сертификатами атрибутов; ведение реестра и архива СОК и СОС; долговременное хранение и управление электронными документами, карточками открытых ключей; резервное хранение и восстановление ключей идентификации (шифрование); проверка статуса СОК в режиме on-line; проставление меток времени.

МСУОК представляет собой распределенную многокомпонентную иерархическую систему управления ключами, назначение которой – поддерживать удостоверенный электронный документооборот между юридическими и физическими лицами Союзного государства и гарантировать, что лицо, идентифицируемое как отправитель электронного сообщения, действительно является его отправителем; лицо, выступающее получателем электронного сообщения, действительно является тем получателем, которого имел в виду отправитель; целостность передаваемой информации не нарушена.

Все пользователи МСУОК должны иметь зарегистрированное удостоверение, признаваемое другими пользователями законным и надежным. Эти удостоверения хранятся в цифровом формате, известном как сертификат. Сертификат представляет собой цифровой документ, который связывает с пользователем некоторую информацию. Если этой информацией является открытый ключ пользователя, то сертификат называется СОК. Если этой информацией являются полномочия пользователя, то сертификат называется сертификатом атрибутов.

Каждый выдаваемый пользователю сертификат имеет свой срок действия, по истечении которого он становится недействительным. Недействительными также могут стать и сертификаты с неистекшим сроком действия, информация в которых перестала быть достоверной, а также сертификаты, содержащие компрометирующие данные. Недействительные сертификаты с неистекшим сроком действия называются отозванными. Срок действия сертификата, а также его статус (действителен или отозван) должны проверяться перед каждым использованием сертификата.

Сертификаты пользователям выдаются удостоверяющими центрами, которые являются уполномоченными юридическими лицами. УЦ, выпуская сертификат, тем самым подтверждает, что информация, связанная с пользователем и содержащаяся в сертификате, является достоверной. Для удостоверения сертификата используется ЭЦП УЦ, выпустившего сертификат.

УЦ известен пользователям по двум атрибутам: своему имени и открытому ключу. В каждый выпущенный сертификат включается имя УЦ и подпись под сертификатом, выработанная при помощи личного ключа УЦ. Пользователи могут легко идентифицировать УЦ, выпустивший сертификат, и убедиться в подлинности сертификата, используя открытый ключ УЦ.

Обычно при выпуске сертификата УЦ указывает области, в которых может быть использован выпущенный сертификат. Например, один сертификат может использоваться для защиты данных общего назначения, а другой – для защиты данных ограниченного распространения. Последнее для юридических лиц – потребителей услуг УЦ является более приоритетной задачей. Используемые секретные ключи должны храниться на аппаратных устройствах, в то время как ключи для защиты данных общего назначения могут храниться в базах данных юридического лица – потребителя услуг УЦ с установленными правилами разграничения доступа.

Области, в которых может быть использован сертификат, задаются в политике применения сертификата, под которой понимается набор правил, характеризующих возможность применения сертификата определенным сообществом, и возможность его применения для класса приложений с определенными требованиями безопасности. Каждая политика применения сертификата имеет свой регистрационный номер и соответствующее текстовое описание. Приложения, использующие сертификаты, обычно содержат собственный набор политик, которым должны удовлетворять используемые ими сертификаты. На основании набора политик применения сертификата приложение принимает решение о допустимости использования указанного сертификата.

Детальное описание политики применения сертификата содержится в соответствующем регламенте УЦ, который открыто публикует свой регламент, чтобы пользователи могли с ним ознакомиться. Решив, что они доверяют УЦ, пользователи могут полагаться на сертификаты, выпущенные им.

Справочники сертификатов обеспечивают их хранение и распространение, а также предоставление информации о статусе. Справочники сертификатов обслуживаются УЦ.

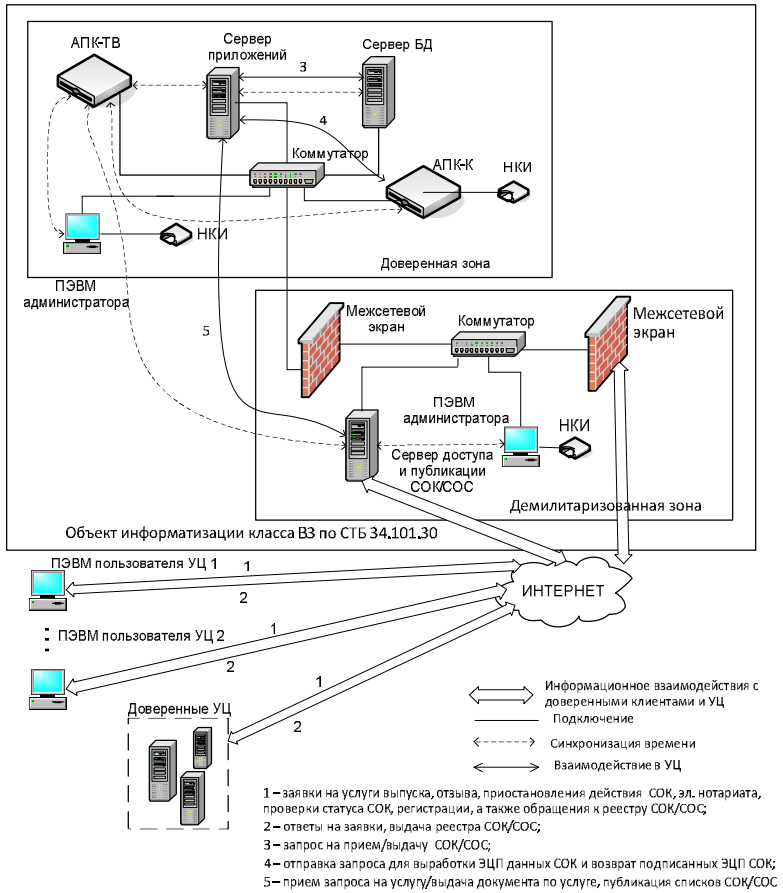
Распространение сертификатов выполняется одним из двух способов:

предоставлением сертификата по запросу пользователя к справочнику сертификатов. Применяется при наличии постоянной (on-line) связи между пользователем и справочником сертификатов;

рассылкой новых сертификатов всем пользователям. Применяется при наличии у пользователей и справочника сертификатов общей распределенной базы данных (БД) сертификатов. В этом случае рассылка новых сертификатов происходит в момент репликации этой БД.

Информация о статусе сертификатов передается справочником сертификатов пользователям в результате распространения СОС или исполнения протокола OCSP (Online Certificate Status Protocol).

Схему функционирования ИС, технологической основой которой является ПАК-МСУОК, можно представить в виде, приведенном на рисунке.



УДК 004.056

А.С. Кравченко

ПРИМЕНЕНИЕ АЛГОРИТМОВ АНАЛИЗА ДАННЫХ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ НА ОСНОВЕ МЕТАДАННЫХ

В современных условиях роль технических средств охраны в обеспечении информационной безопасности чрезвычайно высока. Многочисленные исследования в области информационной безопасности показали, что широкое использование технических средств позволяет исключить либо свести к минимуму негативное влияние человека, которому присущи ошибки, преднамеренные несанкционированные действия и т. п. Организация системы технического обеспечения информационной безопасности значительно надежней.

Существует широкий спектр технических средств обеспечения безопасности. Каждая из категорий объектов, обрабатывающая информацию ограниченного доступа, имеет свою специфику, поэтому главной задачей является формирование единой технической политики, направленной на обеспечение информационной безопасности.

Одной из основных составляющих технического обеспечения информационной безопасности является система контроля и управления доступом с использованием средств видеонаблюдения.

Основной задачей совершенствования систем видеонаблюдения является минимизация возможности «квалифицированного» обхода аппаратуры существующей охранной сигнализации.

Вторая задача в направлении технического перевооружения подразделений – увеличение количества информации, поступающей с объекта. Ее решение позволяет оптимизировать действия групп реагирования за счет постоянного мониторинга возможных проявлений негативных внешних воздействий, нарушающих информационную безопасность.

Третья задача – это организация охраны объектов по альтернативным каналам передачи информации, а именно цифровым каналам Ethernet (TCP/IP), каналам операторов сотовой связи (GSM-канал).

Средства технического обеспечения информационной безопасности включают в себя большой круг технических средств, устанавливаемых на охраняемом объекте.

Практика показывает, что наиболее перспективным путем организации защиты объектов является применение интегрированных систем безопасности (ИСБ), которые, как правило, включают подсистемы: автоматизированной охранной сигнализации; автоматизированной по-

жарной сигнализации; контроля доступа; видеонаблюдения и охранного телевидения.

Оснащение объектов интегрированными системами позволяет существенно поднять уровень их безопасности и обеспечить защиту не только от несанкционированного проникновения (криминальные и террористические угрозы), но и расширить возможности по защите от других видов угроз (аварии оборудования, природные факторы и др.). Кроме этого, ИСБ позволяют оптимальным образом сократить людские и материальные ресурсы, а также финансовые затраты на содержание объектов.

ИСБ обеспечивают: модульную структуру, позволяющую оптимально оборудовать как малые, так и очень большие распределенные объекты; контроль и управление доступом через точки входа (двери, турникеты, шлюзы, шлагбаумы); видеонаблюдение, видеоконтроль и видеорегистрацию тревожных ситуаций; управление установками пожарной автоматики; управление инженерными системами здания (кондиционирования, отопления, вентиляции, оповещения, аварийной сигнализации); защищенный протокол обмена по каналам связи, имитостойкие шлейфы сигнализации; протоколирование всех событий, происходящих в системе.

В настоящее время проводятся работы по усовершенствованию и функциональному расширению данных систем за счет: введения блоков и программного обеспечения для автоматизации инженерных подсистем здания и контроля технологических систем; обеспечения поддержки полномасштабной подсистемы контроля доступа, а также интеграции с подсистемой видеонаблюдения с использованием цифровых технологий и функциями видео- и аудиозаписи, детекции движения, просмотра и управления видеоизображений по информационной сети объекта; использования новых технологий идентификации для подсистемы контроля доступа и защиты от несанкционированных действий (радиочастотная бесконтактная и биометрическая идентификация); введения возможности удаленной передачи данных по цифровым сетям и сетям сотовой связи.

Для повышения эффективности ИСБ ведутся работы, направленные на изучение возможности применения современных алгоритмов анализа видеоизображений, позволяющих обеспечить возможность автоматизированного выявления потенциальных угроз различного вида, в том числе в местах массового скопления людей.

Для автоматизированного видеомониторинга используются современные системы поиска информации, на выходе которых получаются сведения в систематизированном виде. В области видеоаналитики появляются новые технологии анализа обстановки, большинство из которых основано на анализе метаданных.

Процесс поиска информации в сегодняшних системах видеонаблюдения – это перебор десятков камер, серверов, множество часов видеозаписи. Усложнение системы влечет за собой сильное повышение ресурсоемкости поисковой деятельности. От эффективности поиска в архиве видеозаписей и распознавания в реальном времени зависит финальная эффективность системы безопасности. Часто при известных вводных данных на поиск конкретной записи уходит значительное время.

Видеодетекторы помогают оператору выбирать из потока информации значимые данные. Однако они фиксируют только те события, на которые предварительно настроены. Такая аналитика в реальном времени приносит пользу, только если задано искомое событие. Видеодетектор применим к задаче охраны периметра, распознавания номерных знаков на транспорте и т. д.

Для автоматизации поиска информации в видеоархиве можно использовать инструмент, который постоянно индексирует информацию в видеоархиве и создает базу данных индексов (или метаданных) для быстрого поиска. Метаданные – это формальное логическое описание всего, что находится в кадре. Такая информация занимает очень мало места по сравнению с видео и сохраняется одновременно с записью. Чтобы найти нужную видеозапись, достаточно ввести запрос и получить результаты.

Под метаданными понимается описание того, что происходит в поле зрения камеры.

Поступающие от камеры данные обрабатываются алгоритмами, которые формируют некоторое формализованное описание пространства, наблюдаемого камерой. Какая именно информация извлекается из видеопотока и становится основой для метаданных, зависит от самого алгоритма.

Метаданные всегда формируются на уровне обработки видеопотока, а исполняться алгоритм их создания может как на самой камере, так и на компьютере за счет возможностей программного обеспечения.

Если есть описание происходящего в поле зрения камеры, то можно в реальном времени зафиксировать момент, когда меняются события, т. е. можно построить логические правила принятия решения о том, является ли обстановка в поле зрения камеры штатной. Таким образом, метаданные – это базовое описание поля зрения камеры, а детекторы – некоторые критерии штатности происходящих событий.

Метаданные не только анализируются в реальном времени, но и сохраняют базу данных, что позволяет оператору проверять наличие каких-либо событий в прошлом, причем критерий отбора событий возможно задавать произвольно (в отличие от мониторинга в реальном времени, в котором критерии задаются заранее).

Метаданные описывают сцену в поле зрения камеры. Сохранить такую информацию в стандартной базе возможно, но запрос к ней может быть очень ресурсоемок. Становятся актуальными технологии поиска и хранения метаданных. Компания AxxonSoft разработала собственную СУБД, предназначенную специально для хранения метаданных и поиска по ним. В результате поиск в архиве нужного фрагмента записи может составить очень короткий промежуток времени.

Новая структура базы данных имеет собственную систему хранения метаданных, которая позволяет осуществлять поиск именно по геометрическим запросам: координатам, скорости, размеру, цвету. Результат поиска даже в крупных архивах можно получить в течение нескольких секунд.

УДК 004.056

С.Е. Крупенко, В.И. Новосельцев,
М.В. Пономарёв, Д.Е. Скоробогатова

ПРЕДСТАВЛЕНИЕ ЗНАНИЙ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

Неотъемлемой составной частью современных и перспективных систем защиты информации являются интеллектуальные базы знаний. В настоящее время для их построения используются готовые программные продукты типа Oracle, MSSQL, SyBASE и другие, дополняемые различными программными модулями, в которые по схеме «естественный язык → компьютерная программа» закладываются знания о проблемной области. В результате получается некий конгломерат, в котором первичной выступает программная среда, отражающая в основном предметные и частично лингвистические данные, а декларативные, процедурные и лингвистические знания присутствуют постольку, поскольку это допускают возможности данного программного продукта и квалификация программистов-разработчиков. Другими словами, основу существующей технологии поддержки проектных решений при создании интеллектуальных систем защиты информации (ИСЗИ) составляет принцип «делаем то, что можем, а не то, что нужно». Негативные последствия такого подхода очевидны: конечный пользователь, владеющий максимальными знаниями о предметной области, фактически исключается из процесса проектирования и разработки баз знаний. В результате на выходе проекта он получает не то, что ему нужно для обеспечения профессиональной деятельности, а то,

что могут сделать программисты-разработчики, используя имеющиеся программные платформы. И обусловлено это не квалификацией программистов и не низкими функциональными возможностями используемых программных продуктов, а самой технологией поддержки проектных решений по созданию баз знаний.

Таким образом, в настоящее время существует и все более прогрессирует реальное противоречие между насущной потребностью широкого внедрения и использования интеллектуальных баз знаний в составе ИСЗИ и несовершенством применяемых технологий. При этом главная причина существования этого противоречия состоит в том, что в рамках традиционной технологии для представления знаний используются два типа языков: естественный язык, которым оперирует конечный пользователь, и математико-программный язык, который используют разработчики ИСЗИ. Если исключить из рассмотрения многочисленные подробности технического плана, то смысл и сущность традиционной технологии заключается в непосредственном переводе описаний предметной области с естественного языка на математико-программный язык, понятный компьютеру. А такой перевод фактически исключает конечного пользователя из процесса проектирования ИСЗИ, оставляя ему только «начало» и «конец». Именно ограниченность палитры используемых языковых средств обусловливает все те трудности, которые приходится преодолевать разработчикам проектов по созданию ИСЗИ, и предопределяет те неудачи, которые фактически превращают компьютеры не в интеллектуальных партнеров человека, а в хранилище данных или в быстродействующие логарифмические линейки. Вместе с тем в современной теории искусственного интеллекта происходит интенсивное развитие новых языковых средств, в частности реляционного и ролевого типов. Эти языки позволяют записывать и генерировать правила логического вывода, т. е. работать с декларативными знаниями, а также создавать управляющие структуры (оперировать с процедурными знаниями). Их использование открывает более широкие возможности по описанию фактов и закономерностей предметной области и позволяет предложить более совершенную технологию поддержки проектных решений по созданию ИСЗИ, свободную от указанных выше недостатков.

Понятие интеллектуальной базы знаний. Интеллектуальная база знаний (ИБЗ) является ядром ИСЗИ и представляет собой управляемый комплекс языковых, алгоритмических, программных и технических средств, предназначенных для восприятия, обработки, хранения и выдачи (отображения) знаний о предметной области, включающий четыре компоненты:

а) упорядоченные каким-либо способом факты и данные, отражающие модель профессиональной сферы (предметные данные);

б) правила, модели, алгоритмы и программы, позволяющие рассчитывать показатели объектов профессиональной сферы, строить цепочки логических выводов и на этой основе делать обобщения и заключения, а также вызывать определенные ассоциации (декларативные знания);

в) управляющая и интерпретирующая структура, определяющая порядок и способы применения моделей и правил логического вывода для получения или трансформации информации (процедуальные знания);

г) правила морфологического, синтаксического и семантического анализа входных и выходных текстов, а также списки основ слов, которые используются для организации диалога между базой знаний и пользователем (лингвистические знания).

Если оставить в стороне практически бесплодные рассуждения о том, чем данные отличаются от знаний, то формально различия между понятиями «база данных» и «база знаний» можно выразить в виде следующих формул: «база данных» = «предметные данные» + «управление данными» + «лингвистические единицы»; «база знаний» = «предметные данные» + «декларативные знания» + «процедуальные знания» + «лингвистические знания».

Как видно из приведенного определения, ИБЗ представляют собой дальнейшее развитие баз данных и их наращивание по следующим главным направлениям:

интеллектуализации общения с конечным пользователем в форме, не требующей участия посредника-программиста;

формирование моделей проблемных ситуаций по их содержательному описанию пользователем;

расширения понятия «данные» от уровня чисел, текстов, схем и других простейших информационных атрибутов до уровня закономерностей, правил, алгоритмов и других операций, обеспечивающих интеллектуальную поддержку принятия управленческих решений в условиях неопределенности;

обеспечение семантической целостности знаний и данных;

усложнения алгоритмов обработки информации до уровня имитации таких интеллектуальных механизмов мышления человека, как обобщение информации, вывод новой информации, построение логических цепочек вывода новых утверждений, генерация альтернативных вариантов решений и др.;

планирование вычислений, обеспечивающих решение сформулированных пользователем задач количественного и качественного анализа моделей проблемных ситуаций;

интерпретация результатов решения задач в удобном для пользователя виде.

Таким образом, ИБЗ должна предоставлять пользователю следующие возможности: пользователь на своем профессиональном языке (разумеется, по необходимости ограниченном и формализованном) вводит в компьютер описание проблемной ситуации, ставит задачи ее анализа и задает исходные данные, после чего компьютер сам формирует программу решения задач и выдает их решения в удобном для пользователя виде.

При этом основной эффект перехода от баз данных к интеллектуальным базам знаний заключается в более полном удовлетворении потребностей пользователя в информации, необходимой ему для принятия решений, за счет повышения статуса компьютера, поставляющего пользователю не информацию к размышлению, а мотивированные варианты возможных решений. Естественно, что речь идет не об однократном решении какой-либо задачи, а о диалоговом общении с ИБЗ при многократном повторении цикла: подготовка исходных данных, решение задачи, анализ решения, коррекция исходных данных.

Языки представления знаний. В проблеме представления знаний много трудных вопросов, окончательные ответы на которые до сих пор не получены. Среди них – кардинальный вопрос о структуре самого языка представления знаний. На вопросы о том, как и в какой языковой форме хранятся у человека знания о внешнем мире, прошлом опыте и своих возможностях, каким образом осуществляется обработка знаний, как на базе старых происходит формирование новых знаний, современная наука пока не дает исчерпывающих ответов. Есть только гипотезы. Это вынуждает разработчиков ИБЗ использовать паллиативный подход к решению проблемы представления знаний. Сущность этого подхода заключается в том, что язык для представления знаний рассматривается как инструментальное средство, аналогичное естественному языку, с тем существенным отличием, что в нем алгоритмы выявления смысла сообщений и текстов зафиксированы в более строгой (естественно, и более ограниченной) форме по сравнению с естественным языком.

В настоящее время наибольший практический интерес представляют следующие типы языков представления знаний (рис. 1).

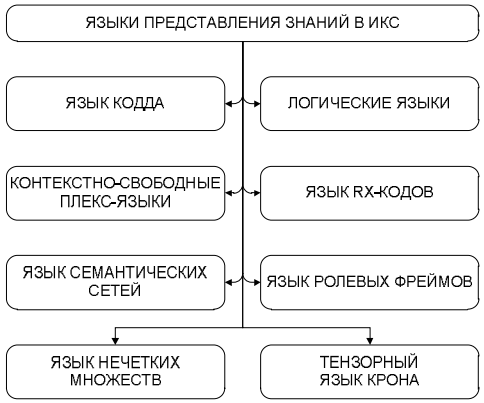


Рис. 1. Типы языков представления знаний в ИКС

На рис. 2 приведена диаграмма, отражающая результаты анализа указанных языков. На этой диаграмме языки представления знаний упорядочены по двум характеристикам, определяющим возможности их практического использования при управлении проектами создания ИБЗ в составе ИСЗИ. Первая характеристика, названная семантической силой языка, отражает его описательные возможности, т. е. возможности адекватного и полного описания проблемных областей. Эта характеристика отложена на горизонтальной оси диаграммы. Вторая характеристика, названная мощностью инструментальных средств языка, отражает его возможности по построению эффективных систем эквивалентных преобразований предложений языка, т. е. аппарата, позволяющего (за конечное число шагов) однозначно определять синтаксическую и семантическую правильность предложений. Эта характеристика отложена на вертикальной оси диаграммы.

Рис. 2. Сравнительная характеристика языков представления знаний по мощности инструментальных средств и семантической силе

Из этой диаграммы видно, что требования наибольшей выразительности и наибольшей мощности инструментальных средств языка являются противоречивыми: чем выше семантическая сила языка, тем ниже мощность его инструментальных средств, и, наоборот, с ростом мощности инструментальных средств семантическая сила языка падает. Отсюда следует, что при практическом проектировании и создании ИБЗ невозможно выбрать какой-либо один язык, адекватно удовлетворяющий указанным требованиям. Речь может идти о некоторой совокупности языковых средств, которые совместно могут обеспечить как требуемый уровень выразительных возможностей ИБЗ, так и необходимую «суммарную» мощность ее инструментальных средств. В силу сказанного укажем предпочтительные области применения рассматриваемых языков применительно к проектированию и разработке ИБЗ в составе ИКС.

Предпочтительные области применения языков представления знаний при создании ИБЗ в составе ИСЗИ

Тип языка	Область применения при создании ИБЗ в составе ИСЗИ
Классические математические языки	Разработка математических моделей для компьютерной имитации различных аспектов проблемной области и их использование в качестве прикладных модулей в структуре ИБЗ
Тензорный язык Крона	Перспективные исследования по развитию методологии управления проектами создания ИБЗ знаний в ИСЗИ
Классические логические языки	Разработка моделей и методов анализа и оптимизации структуры ИБЗ. Создание моделей, обеспечивающих функционирование ИБЗ
Язык нечетких множеств	Как одна из основных форм учета неопределенности знаний пользователя об объектах и процессах предметной области
Контекстно-свободный плекс-язык	Представление в ИБЗ структур различных объектов. Анализ структур на полноту, непротиворечивость и достаточность
Язык RX-кодов	Ограниченное применение как частный случай языка семантических сетей
Язык семантических сетей	Построение общей и частных технологий поддержки проектных решений при создании ИБЗ в составе ИСЗИ
Язык ролевых фреймов	
Естественный язык	Представление знаний о предметной области в виде текстов, таблиц, графиков, диаграмм и т. п. Справочники, инструкции и другие документы, необходимые пользователю для выполнения служебных обязанностей

Технология проектирования ИБЗ. Суть предлагаемой технологии заключается в том, что проектирование базы знаний осуществляется не одноактно (как это обычно делается) и не методом спонтанных итераций (как это часто практикуется), а путем последовательной реализации следующих этапов (рис. 3).

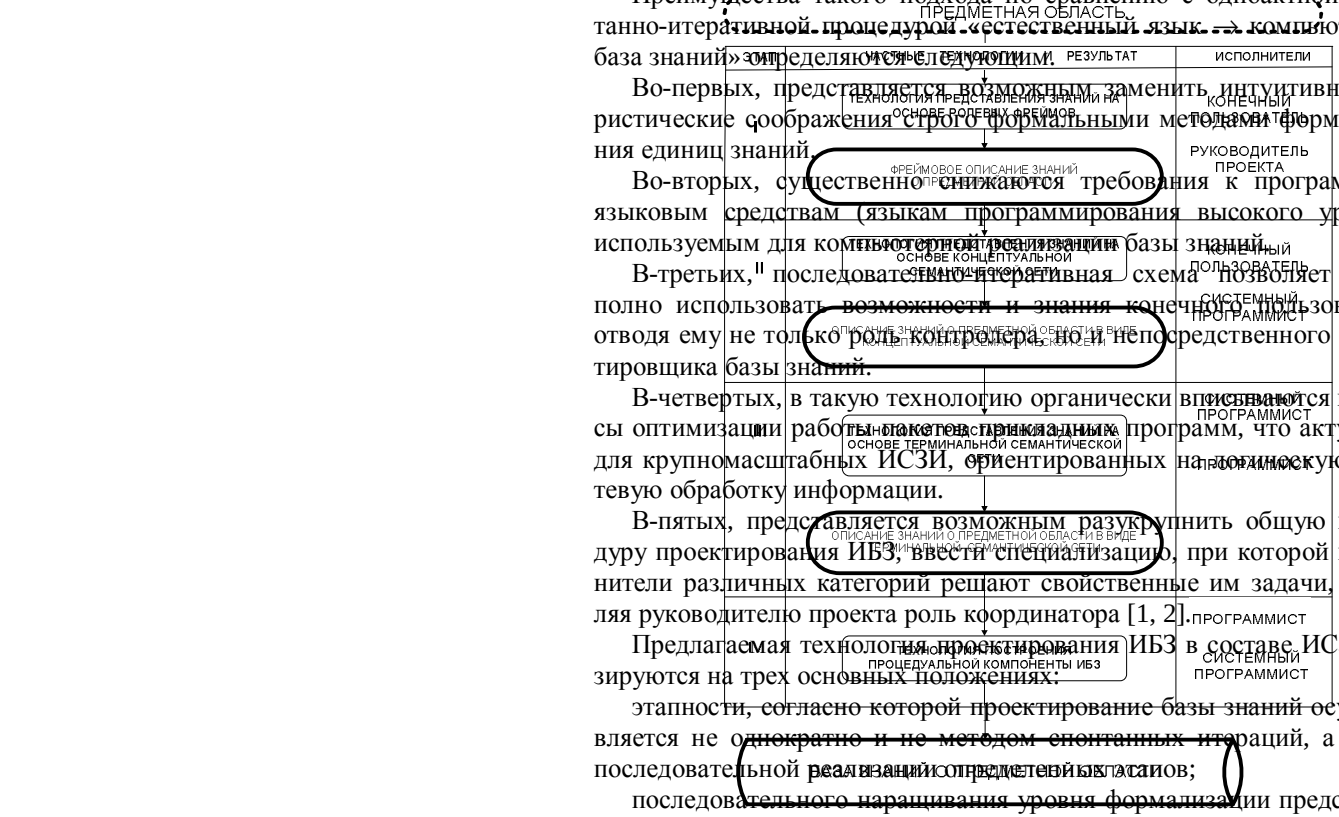


Рис. 3. Общая технология проектирования ИБЗ в составе ИСЗИ

Этап I. Представление знаний на основе ролевых фреймов (переход от естественного языка к фреймовым описаниям).

Этап II. Представление знаний с помощью концептуальной семантической сети (переход от фреймовых описаний к описаниям в виде концептуальной семантической сети).

Этап III. Представление знаний с помощью терминальной семантической сети (переход от описаний в виде концептуальной семантической сети к описаниям в виде терминальной семантической сети – расширение концептуальной семантической сети).

Этап IV. Построение процедуальной компоненты ИБЗ, отражающей динамику предметной области, оптимизация работы прикладных модулей и формирование полной структуры ИБЗ.

Преимущества такого подхода по сравнению с одноактной спонтанно-итеративной процедурой «естественный язык → компьютерная база знаний» определяются следующим.

Во-первых, представляется возможным заменить интуитивные эвристические соображения строго формальными методами формирования единиц знаний.

Во-вторых, существенно снижаются требования к программным языковым средствам (языкам программирования высокого уровня), используемым для компьютерной реализации базы знаний.

В-третьих, последовательно-итеративная схема позволяет более полно использовать возможности и знания конечного пользователя, отводя ему не только роль контролера, но и непосредственного проектировщика базы знаний.

В-четвертых, в такую технологию органически вписываются вопросы оптимизации работы комплекса прикладных программ, что актуально для крупномасштабных ИСЗИ, ориентированных на логическую и сетевую обработку информации.

В-пятых, представляется возможным разукрупнить общую процедуру проектирования ИБЗ, ввести специализацию, при которой исполнители различных категорий решают свойственные им задачи, оставляя руководителю проекта роль координатора [1, 2].

Предлагаемая технология проектирования ИБЗ в составе ИСЗИ базируются на трех основных положениях:

этапности, согласно которой проектирование базы знаний осуществляется не однократно и не методом спонтанных итераций, а путем последовательной реализации определенных этапов;

последовательного наращивания уровня формализации представления знаний при переходе от этапа к этапу, начиная с естественного языка и заканчивая языком семантических сетей, допускающего компьютерную реализацию с использованием языков программирования высокого уровня;

поддержки проектных решений путем использования частных технологий в процессе управления проектом.

Реализация этих положений позволяет при управлении процессом проектирования и разработке базы знаний заменить эвристические соображения строго формальными методами задания единиц знаний,

снизить требования к языкам программирования, а также более полно использовать знания конечного пользователя о предметной области. Принципиальное преимущество данной технологии заключается в том, что она позволяет минимизировать исследовательские циклы, тем самым упорядочить работу исполнителей проекта и повысить качество проведения проектных работ.

1. Дёмин Б.Е. Методологические основы и модели обоснования проектов крупномасштабных информационно-коммуникационных систем. Воронеж : Науч. книга, 2006. 332 с.

2. Самков Е.Ю. Алгоритмы и методы поддержки проектных решений по созданию интеллектуальных баз знаний на основе логико-лингвистических средств искусственного интеллекта : монография. Воронеж : Науч. книга, 2010. 130 с.

УДК 681.3

С.Е. Крупенко, В.И. Новосельцев, Д.Е. Скоробогатова

ВЫБОР ЯЗЫКА ПРЕДСТАВЛЕНИЯ ЗНАНИЙ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

Выбор языков представления знаний при управлении проектами создания ИС всегда сталкивается с двумя противоречивыми требованиями. С одной стороны, требуется, чтобы такой язык содержал развитую систему формальных эквивалентных преобразований, обеспечивающую возможность определения синтаксической и семантической правильности выражений и формального построения выводов. С другой стороны, такой язык должен позволять адекватно описывать ситуации в проблемной области во всем их многообразии, т. е. обеспечивать некоторое отображение естественного языка на формально-логический язык.

Эта двойственность приводит к тому, что выбор того или иного варианта языка представления знаний является компромиссом между различными требованиями к его структуре. Одним из перспективных языков представления знаний является контекстно-свободный плекс-язык (КСПЯ).

Основными компонентами этого языка являются: плекс-элементы, операция канкатенации и КСП-грамматика. Плекс-элемент – это абстрактный объект, имеющий определенное количество контактов (входов и выходов) для соединения с другими плекс-элементами. Множество различающихся плекс-элементов, из которых может быть образована

некоторая структура, образуют алфавит КСПЯ. Конкатенацией называется соединение плекс-элементов (их контактов) из алфавита, что формально задается матрицей , элементы которой отражают связи между контактами плекс-элементов. КСП-грамматика – это правила соединения плекс-элементов между собой.

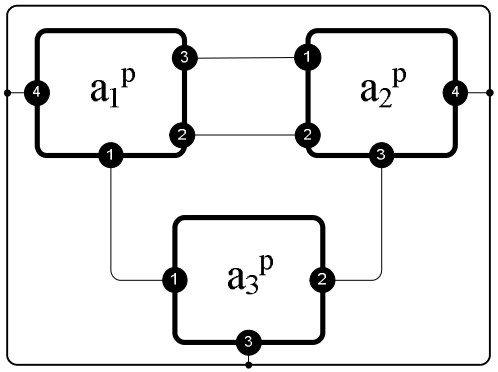


Рис. 1. Представление 3-компонентной системы с помощью КСПЯ

Эта система (рис. 1) состоит из трех компонентов или в терминах КСПЯ – трех плекс-элементов: a_1^p, a_2^p, и a_3^p. В каждом плекс-элементе контакты выделены точками на его контуре и перенумерованы. При этом часть контактов замкнута на контакты других плекс-элементов (внутренность системы), а другая часть контактов – на контакты внешнего контура поверхности системы. Матрица конкатенации для этого плекса (системы) представляется следующим образом:

(1)

Элемент , расположенный над главной диагональю матрицы, отличается от элемента , стоящего ниже диагонали, только порядком записи индексов для каждой пары, что отражает направленность связей между плекс-элементами.

Грамматикой КСПЯ называется четверка:

(2)

где v_0 – начальный символ; – алфавит терминальных плекс-элементов; – алфавит вспомогательных плекс-элементов; – множество правил вывода.

Правила вывода имеют вид:

(3)

где Ψ_1 – подстановка, указывающая порядок конкатенации контактов при подстановке вспомогательного плекса вместо терминального.

Символика $PI(A \vee V)^+$ означает, что плекс PI есть подмножество объединения алфавитов A и V, значок «+» указывает на то, что при таком объединении должны учитываться все возможные в конкретной грамматике индексы (рис. 2).

При этом КСП-грамматика имеет следующие правила вывода:

$$\Gamma_6 = \begin{Vmatrix} 0 & (2-2,3-3) \\ (2-2,3-3) & 0 \end{Vmatrix}; \quad \Psi_6 \qquad (4)$$

(4)

Эти правила построены на двух вспомогательных плекс-элементах $r: v_0 \to \Psi_1\Gamma_1(\Psi_3\Gamma_3 a_1^p a_2^p a_3^p)(\Psi_6\Gamma_6 a_4^p a_5^p)$.
v1 и v2, пяти терминальных плекс-элементах при подстановках .

Начальный символ v_0 в этой грамматике представляет некоторый объект предметной области (систему) в целом, т. е. на нулевом уровне членения.

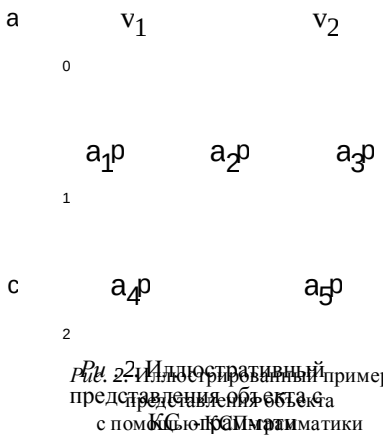


Рис. 2. Иллюстративный пример представления объекта с помощью КСП-грамматики

Вспомогательные плексы v_1 и v_2 заданы, например, альтернативными графами, вершинами которых служат функции, представляющие подпроцессы функционирования некоторого объекта (системы) как целого, а ребрами – отношения между функциями. Заданы и терминальные плексы (ими могут быть также альтернативные графы). На рис. 2, b, c показаны *альтернативные варианты* заданной через v_0 структуры объекта (системы) с применением различных комбинаций терминальных плекс-элементов.

Таким образом символика (4) означает (на примере первой строки) «плекс v_0 образован плексами v_1 и v_2 по правилам подстановки и

матрицы конкатенации Γ_1». Матрицы конкатенации и подстановки в рассматриваемом примере выглядят так:

$$\Psi_{(i=a_i \times v_k)}$$

$$PI(A \vee V)^+$$

$$v_0 \to \Psi_1\Gamma_1 v_1 v_2;$$

$$v_1 \to \Psi_3\Gamma_3 a_1^p a_2^p;$$

$$v_2 \to \Psi_6\Gamma_6 a_4^p a_5^p.$$

В этой грамматике возможен вывод «r» такого вида:

(5)

$$a_1^p, a_2^p, a_3^p,$$

Этот вывод записан в так называемой неприведенной форме, позволяющей определять элементный состав плекса и содержащей указатели матриц конкатенации и подстановки, по которым можно выявить способы соединения плекс-элементов между собой. С точки зрения построения ИБЗ это означает, что, используя записи типа (5), можно строить дерево выводов.

$$\Psi_1, \Psi_3, \Psi_6$$

Основным достоинством КСПЯ является возможность его использования как достаточно гибкой формы представления структур различных объектов в базах знаний. Причем, когда появляется некоторая новая структура, всегда можно установить, достаточно ли алфавита и грамматики данного языка для ее адекватного представления в базе знаний или необходимо пополнять его новыми плекс-элементами и модифицировать КСП-грамматику.

Основные ограничения данного языка следующие:

$$a_1^p, a_2^p, a_3^p, a_4^p, a_5^p$$

в КСПЯ практически отсутствуют средства формальных эквивалентных преобразований, что не позволяет установить синтаксическую и семантическую правильность выражений и формального построения выводов (эти функции, важные для построения интеллектуальных баз знаний, как и при использовании текстов естественного языка, остается за человеком);

с помощью КСПЯ достаточно трудно описывать свойства и качества реальных объектов предметной области, поскольку он ориентирован на описание преимущественно отношений «вход-выход»;

$$\Psi_1$$

пока отсутствуют компьютерные программы-трансляторы, обеспечивающие перевод текстов, написанных на КСПЯ, в машинные коды или на языки программирования высокого уровня.

УДК 621.039

Э.П. Крюкова

ПРИМЕНЕНИЕ СТАНДАРТОВ В ОБЛАСТИ БЕЗОПАСНОСТИ АТОМНОЙ ЭНЕРГЕТИКИ ДЛЯ РАЗРАБОТКИ И ОЦЕНКИ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Атомная энергетика играет важную роль в энергетических программах многих стран при условии обеспечения ее безопасного использования. Этой отрасли исторически присущи сложность технологических процессов, высокий уровень технологичности конечной продукции, повышенные правила безопасности и жесткость национальных и международных нормативных требований, в том числе к системам менеджмента качества.

При использовании атомной энергии основные требования к качеству функционирования АЭС определяет Международное агентство по атомной энергии (МАГАТЭ). Признавая значение безопасности атомной отрасли, МАГАТЭ учредило программу разработки руководящих документов для государств – членов МАГАТЭ по вопросам безопасности АЭС.

В 1996 г. МАГАТЭ разработало комплект документов 50-C/SG-Q «Гарантия качества безопасности на атомных электростанциях и других ядерных установках». В 2006 г. оно было заменено на Руководство IAEA GS-R-3 «Система менеджмента для предприятий и деятельности» и затем дополнено рядом других стандартов, развивающих это направление.

Сравнение ISO 9001:2008 «Системы менеджмента качества. Требования» с IAEA GS-R-3 показывает, что цели документов различны, хотя их нельзя назвать несовместимыми. В то время как в стандартах МАГАТЭ акцент управления качеством делается на безопасности АЭС в целом, в ИСО 9001:2008 акцентируется важность обеспечения результативности системы менеджмента качества при выполнении требований потребителя. По стандартам ИСО проектирование систем идет «снизу вверх» на основе коммерческих стандартов, использования продукции, изготовленной и оцененной по этим стандартам. Класс безопасности выбирается, исходя из приемлемости бизнес-рисков организации, т. е. экономических аспектов покрытия ущерба.

Поэтому в рамках атомной энергетики при рассмотрении вопроса об обеспечении качества функционирования АЭС встал вопрос о необходимости дополнения требований ИСО 9001, которые не рассматриваются этим стандартом. Система менеджмента для любого предприятия атомной энергетики интегрирует требования к надежности функционирования, охране здоровья, окружающей среды, безопасности и экономические требования.

Большое внимание в документах МАГАТЭ уделяется культуре безопасности, которая не нашла отражение в ISO 9001:2008, но должна развиваться и поддерживаться системой управления качеством. Как правило, стандарты, разработанные ISO, являются дополнительными техническими документами к документам МАГАТЭ, которые акцентируются на приложениях в промышленности и аспектах контрактов.

Безопасность – основная цель системы управления качеством АЭС, требования по достижению которой широко отражены в руководствах и стандартах МАГАТЭ, подробно разработаны и представлены в стандартах международной электротехнической комиссии (IEC/МЭК).

Процесс создания систем, применяемых на АЭС, представлен в основополагающем стандарте IEC 61513:2011 («Атомные электростанции. Системы контроля и управления, важные для безопасности. Общие требования»). Он вводит концепцию безопасного жизненного цикла системы и оборудования как среды, в которой можно управлять процессом разработки и из принятия которой следует в качестве результата доказательство, необходимое для подтверждения надежности и эффективности систем безопасности.

В IEC 61513 принят формат представления, аналогичный основной публикации по безопасности IEC 61508 с полной схемой безопасного жизненного цикла системы. Он предусматривает интерпретацию общих требований IEC 61508:2010 («Функциональная безопасность электрических/электронных/программируемых электронных систем, относящихся к безопасности») для применения в области атомной энергетики.

IEC 61513 обращается непосредственно к другим стандартам по общим вопросам, отнесенным к категорированию функций и классификации систем, оценке, разделению систем, защите от отказа по общей причине, программным аспектам компьютерных систем, аппаратным аспектам компьютерных систем, проектированию щитов управления и др.

Проектирование важных для безопасности систем АЭС осуществляется в соответствии с принципом «сверху вниз», т. е. начинается с анализа общей безопасности АЭС. Исходя из данных анализа, определяются категории безопасности функций, назначаются классы безопасности систем, идет их разработка, реализация одновременно с оценкой качества разработки и реализации в жестком соответствии со стандартами МАГАТЭ и МЭК.

Под безопасным жизненным циклом системы (system safety life cycle) понимаются необходимые мероприятия, включаемые в реализацию системы контроля и управления, важной для безопасности, имеющие место на протяжении периода времени, который начинается на стадии концепции детализацией требований к системе и оканчиваются, когда система контроля и управления более недоступна для использования.

Понятие безопасного жизненного цикла общей архитектуры контроля и управления и безопасного жизненного цикла отдельных систем подчеркивает зависимость между целями безопасности АЭС, требованиями к общей архитектуре систем контроля и управления, важных для безопасности, и между общей архитектурой и требованиями к отдельным системам, важным для безопасности. Полный безопасный жизненный цикл архитектуры контроля и управления является итеративным процессом, в котором выходные данные каждого этапа должны проверяться на соответствие входным данным предыдущих мероприятий.

В период развития стандарта IEC 61513 разработана и продолжает развиваться серия стандартов по различным аспектам безопасности АЭС. IEC 61513 ссылается на ISO, а также на руководства МАГАТЭ GS-R-3 и МАГАТЭ GS-G-3.1 по вопросам, связанным с обеспечением качества.

При проектировании и разработке по общим промышленным стандартам системы могут не соответствовать современным требованиям технологий безопасности АЭС. В частности, программное обеспечение, используемое в системах контроля и управления на АЭС, часто требуется только в аварийных ситуациях и поэтому должно пройти полную верификацию и оценку годности до его применения в эксплуатации (IEC 60880). Для систем, выполняющих функции категории «А» и «В» (системы 1-го и 2-го классов безопасности), программно-технические средства и комплексы аппаратуры должны проектироваться по требованиям IEC 60880, IEC 62138 (программные средства), IEC 60987 (аппаратные средства) с доказательством реализации безопасного жизненного цикла систем и средств, выполнением верификации/валидации готовых изделий.

МАГАТЭ устанавливает несколько отдельных принципов безопасности, которые вместе образуют интегрированный подход к общей безопасности АЭС. Эти принципы рекомендуется использовать в процессе проектирования при анализе всех относящихся к ним постулируемых исходных событий.

Правила, применяемые при разработке требований, реализующих эти принципы, включают: использование наилучших доступных технологий; проектирование «сверху вниз»; модульность; верификацию на каждом этапе; ясность документации; возможность проверки документов; валидационное тестирование.

Эти принципы и правила, а также реализующие их требования подробно отражены в стандартах МЭК. Они определяют уровень качества функционирования систем и оборудования, необходимый для обеспечения состояния нормальной эксплуатации, правильного реагирования на события и облегчения стабильного управления оборудованием после аварии.

В настоящее время в рамках Государственной программы «Научное сопровождение развития атомной энергетики в Республике Беларусь на 2009–2010 годы и на период до 2020 года» разрабатываются ряд стандартов на основе документов МАГАТЭ и МЭК, осуществляется прямое введение стандартов МЭК. Стандарты постоянно отслеживаются на соответствие новым тенденциям в обеспечении различных аспектов безопасности АЭС, отражают самый современный подход к классификации систем и компонентов по безопасности, устанавливают общие и специальные требования на основе этой классификации, дают подробные рекомендации по реализации этих требований.

Четкая классификация систем по уровню безопасности, назначение требований безопасности для компонентов этих систем в соответствии с принятой классификацией, жесткие требования к организации безопасного жизненного цикла систем, компонентов и архитектуры объекта в целом делают целесообразным использование стандартов МЭК при разработке и обеспечении надежного функционирования критически важных объектов информатизации в различных отраслях экономики, где безопасность носит комплексный характер.

УДК 343.534

В.В. Маликов, И.В. Бенедиктович, С.А. Чурюканов

ИССЛЕДОВАНИЕ СТРУКТУРЫ РЫНКА КИБЕРПРЕСТУПНОСТИ И ЭФФЕКТИВНОСТИ ДЕЯТЕЛЬНОСТИ ЕГО СУБЪЕКТОВ

В настоящее время использование информационно-коммуникационных технологий со стороны организаций различных форм собственности, а также физических лиц приобрело трансграничный характер. Государства, на территории (или через территории) которых осуществляется активное использование таких технологий, должны принимать меры для нормативно-правового, организационно-технического и технического регулирования в данной сфере. Обеспечение внутригосударственного регулирования невозможно без учета аспектов международного законодательства и сотрудничества между ведущими индустриально развитыми странами.

Глобальный рынок киберпреступности активно развивается и совершенствуется в соответствии с передовыми направлениями информатизации общества, внедрением электронных систем коммуникаций, электронных платежных систем.

В целях организации действенной системы противостояния современным вызовам и угрозам, реализуемым для противоправной деятельности со стороны преступного сообщества, необходима разработка и совершенствование методической базы, способствующей пресечению и раскрытию киберпреступлений.

В рамках исследования проведена декомпозиция рынка киберпреступности на законченные функциональные уровни и модули (рис. 1). Предлагается использование варианта декомпозиции, который учитывает полный технологический цикл осуществления атак, включающий как разработку вредоносного программного обеспечения, так и непосредственно его использование в преступных целях. В качестве базовых уровней предлагаются следующие: интернет-мошенничество; спам; DDos-атаки; рынок криминальных средств систем и услуг.

Основным ...иалистиче-
ского расс... ...ия являет-
ся кримин... ...истически
значимая и... ...я, данные,
технологич... ...итные па-
раметры сд...

1. Явля... ...цифрового
следа, воз... ...пьютерно-
техническ...

2. Внос... ...ния в ори-
гинальные... ...код, опти-
ческие/эле... ...гоге нару-
шающие св... ...льности.

3. По способу документирования является энергозависимой и энергонезависимой.

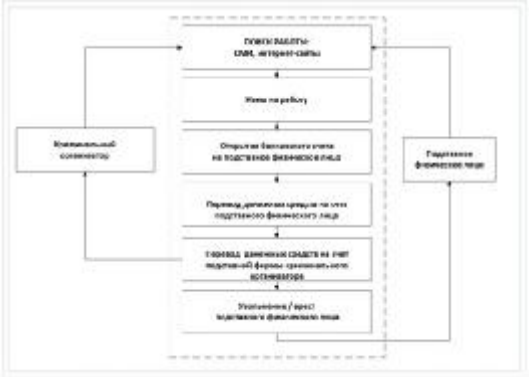
Основную роль в подготовке и реализации компьютерно-технических преступлений играет криминальный организатор.

Криминальный организатор – физическое лицо/группа лиц, юридическое лицо/группа лиц, незаконные организации/группировки, государство/группа государств, осуществляющих полное или частичное планирование и/или разработку, внедрение механизмов, приводящих к осуществлению компьютерно-технического преступления.

В настоящее время можно выделить следующие основные типы криминальных организаторов: спецслужбы иностранных государств и блоков государств, террористы и террористические организации, конкурирующие организации и структуры, криминальные структуры, взломщики программны... ...партнеры, бывшие сотруд... ...ов).

В качестве ... ...отметить: мест..., достиж... ...гство, профессиональное... ...ую выгоду.

Криминальн... ...преступления может осу... ...разработку, внедрение мех... ...ением сторонних средст... ...основе. Условный механ... ...уг показан на рис. 2.



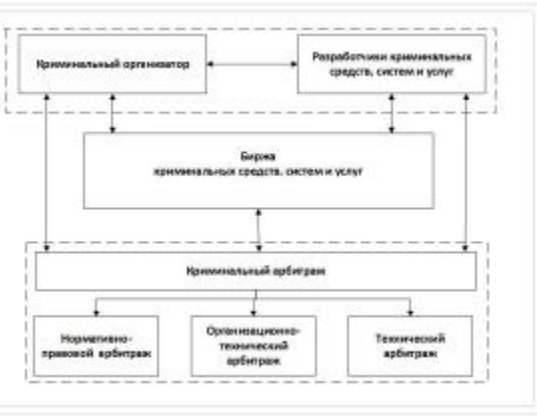


Рис. 2. Схема организации функционирования биржи криминальных средств, систем и услуг

Криминальный арбитраж – криминальные структуры, осуществляющие незаконные услуги по обеспечению имущественных и неимущественных прав/гарантий между криминальным организатором и разработчиками на бирже криминальных средств, систем и услуг, а также взыскания/возмещения ущерба, понесенного сторонами в ходе нарушения условий криминальной сделки.

Основной задачей криминального организатора компьютерно-технических преступлений, связанной с завершением реализации механизмов хищения финансово-регистрационных данных, является вывод финансовых средств через подставные юридические и/или физические лица. Один из таких криминальных механизмов с использованием подставных физических («дропов») и юридических лиц показан на рис. 3.

Рис. 3. Схема вывода финансовых средств через подставные физические и юридические лица

Проведенное исследование структуры рынка киберпреступлений, включающее организационно-технические, технические аспекты предупреждения и раскрытия таких преступлений, позволяет повысить эффективность работы специалистов отрасли информационной безопасности.

УДК 658.29-049.5

тивными правовыми актами действия, в которых компьютерно-техническая информация является объектом преступного посягательства.

Компьютерно-техническая информация – сведения (сообщения, данные, технологический/аппаратный код, оптические/электромагнитные параметры среды обработки), представленные в электронно-цифровой форме, зафиксированные на материальном носителе, обрабатываемые аппаратно-программными устройствами, а также передающиеся по каналам сопряжения и коммуникации посредством электромагнитных сигналов.

Наибольший интерес для криминального организатора компьютерно-технических преступлений представляют безналичные электронные платежи пользователей сервисов сети Internet.

Атака на сервисы безналичных электронных платежей возможна как на сторону серверной инфраструктуры владельца сервиса, так и на компьютер конечного пользователя. Учитывая то, что, как правило, серверная инфраструктура защищена более надежно, на практике быстрее и экономически целесообразнее осуществить компьютерно-технический взлом компьютера конечного пользователя. Масштабируя эффект взлома на тысячи пользователей таких сервисов, криминальный организатор достигает крупного финансово-экономического результата.

Основные варианты перехвата управления в сервисах безналичных электронных платежей приведены на рис. 1.

Рис. 1. Схема перехвата управления
в сервисах безналичных электронных платежей

Для устранения возможностей перехвата и повышения уровня безопасности платежными сервисами используется алгоритм 2-факторной аутентификации пользователя.

Однако наиболее развитые и технологичные троянских программы, используемых киберпреступниками, например банковский троянец ZeuS (Zbot) совместно с мобильным троянцем ZeuS-in-the-Mobile (ZitMo), могут обходить данную систему защиты (рис. 2).

Рис. 2. Схема обхода 2-факторной аутентификации
в сервисах безналичных электронных платежей

Другие системы защиты сервисов безналичных электронных платежей также нейтрализованы киберпреступниками:

chipTAN – банковский троянец SpyEye;

на основе USB-токена – банковский троянец Lurk.

Механизм заражения компьютера пользователя сервиса безналичных электронных платежей вредоносным программным обеспечением (ПО), основан на эксплойт-паках (Nuclear Pack, Styx Pack, BlackHole, Sakura) реализующих уязвимости в легитимном ПО (рис. 3).

Рис. 3. Схема заражения компьютера на основе эксплойт-паков ПО

Эксплойт-пак – сборка компьютерных программ, фрагментов программного кода или последовательность команд, использующих уязвимости в программном обеспечении и применяемые для проведения атаки на компьютерно-техническую систему. Наиболее известные базы знаний по уязвимостям и сборники эксплойт-паков: ICS-CERT, NVD, CVE, Bugtraq, OSVDB, Mitre Oval Repositories, exploit-db, Siemens Product CERT, SAINTexploit, Metasploit Framework, Immunity Canvas, Agora Pack, Agora SCADA+, D2 Exploit Pack, White Phosphorus exploit pack, VulnDisco Exploit Pack, BlackHole, Sakura.

Таким образом, проведенное исследование технологий совершения компьютерно-технических преступлений позволяет повысить эффективность предупреждения и расследования таких преступлений.

УДК 355.40

А.Ф. Мельник

СОВЕРШЕНСТВОВАНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В УСЛОВИЯХ СОВРЕМЕННОГО СОСТОЯНИЯ И ДАЛЬНЕЙШЕГО РАЗВИТИЯ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Защита информации от утечки по техническим каналам является одной из важнейших задач в области обеспечения безопасности информации, обрабатываемой средствами вычислительной техники (СВТ). Как известно, под техническим каналом утечки информации (ТКУИ) понимают совокупность источника информации, линии связи (физической среды), по которой распространяется информационный сигнал, шумов, препятствующих передаче сигнала в линии связи, и технических средств перехвата информации.

Среди всего разнообразия ТКУИ, обрабатываемой СВТ, в настоящее время особое место занимают электромагнитные и электрические каналы утечки информации, к которым относятся канал побочных электромагнитных излучений (ПЭМИ) и канал электрических наводок на соединительные линии, посторонние проводники, линии электропитания и заземления, выходящие за пределы контролируемой зоны объекта СВТ.

Обрабатываемая средствами СВТ информация считается защищенной, если на границе контролируемой зоны объекта СВТ отношение информативный сигнал/шум не превышает некоторого нормиро-

ванного значения во всех возможных ТКУИ. Защищенность информации зависит как от уровней ПЭМИ и наводок от СВТ, которые определяются при проведении их исследований, так и от условий расположения СВТ. В случаях когда на границе контролируемой зоны объекта СВТ не удается достичь нормированного значения отношения сигнал/шум, для защиты информации от утечки по каналам ПЭМИ и наводок применяются технические средства защиты информации (ТСЗИ), которые по своему назначению и принципам действия можно разделить на три большие группы: фильтры сетевые помехоподавляющие (ФСП); генераторы электромагнитного шума (ГЭМШ); генераторы линейного зашумления (ГЛЗ).

Рассмотрим каждую группу ТСЗИ более подробно.

ФСП относятся к пассивным ТСЗИ и предназначены для блокирования распространения информативных наведенных электрических сигналов по линиям электропитания и заземления СВТ путем внесения затухания в рабочем диапазоне частот. Величина вносимого затухания и рабочий диапазон частот наиболее распространенных сетевых помехоподавляющих фильтров производства Беларуси и России приведены в табл. 1.

Таблица 1

Основные технические характеристики ФСП

Тип ФСП, изготовитель	Вносимое затухание, дБ, не менее	Диапазон частот, МГц	Тип ФСП, изготовитель	Вносимое затухание, дБ, не менее	Диапазон частот, МГц
ФПС-1 (Беларусь)	80	0,15–2 000	ФП-15Мск (РФ)	100	0,15–1 800
ФПГ-1Т (Беларусь)	60	0,15–2 000	ФП-15М (РФ)	95	0,15–1 800
ФП-Е (Беларусь)	60	0,015–2 000	ФП-11 (РФ)	80	0,15–1 800
ФП-Z (Беларусь)	60	0,01–2 000	ФП-6М (РФ)	60	0,15–1 800

ГЭМШ относятся к активным ТСЗИ и предназначены для защиты обрабатываемой СВТ информации от утечки по каналу ПЭМИ путем создания в окружающем пространстве широкополосного маскирующего электромагнитного поля шума (ЭМПШ) в рабочем диапазоне частот (табл. 2).

Таблица 2

Основные технические характеристики ГЭМШ

Тип ГЭМШ, изготовитель	Диапазон частот, МГц	Тип ГЭМШ, изготовитель	Диапазон частот, МГц
ГЭМШ (Беларусь)	0,1–2 000	ЛГШ-221 (РФ)	0,15–1 800
«Штиль» (Беларусь)	0,1–2 000	ГШ-2500М (РФ)	0,1–2 000
SEL SP-113 «Блокада» (РФ)	0,01–2 000	ГШ-К-1800М (РФ)	0,1–1 800
ЛГШ-513 (РФ)	0,01–2 000	«Маис-М» (РФ)	0,01–10 000

ГЛЗ относятся к активным ТСЗИ и предназначены для защиты обрабатываемой СВТ информации от утечки по линиям электропитания и заземления путем создания в указанных линиях широкополосных маскирующих электрических шумовых сигналов (ЭШС) в рабочем диапазоне частот (табл. 3).

Таблица 3

Основные технические характеристики ГЛЗ

Тип ГЛЗ, изготовитель	Диапазон частот, МГц	Тип ГЛЗ, изготовитель	Диапазон частот, МГц
«Рокот» (Беларусь)	0,15–1 000	SEL SP-113 «Блокада» (РФ)	0,01–300
«Штиль» (Беларусь)	0,1–2 000	ГШ-1000У (РФ)	0,1–1800
SEL SP-44 (РФ)	0,01–300	«Маис-М» (РФ)	0,01–10 000

Примечание. Основные технические характеристики в табл. 1–3 указаны на основании рекламных материалов ТСЗИ.

Методология применения ТСЗИ для обеспечения технической защиты от утечки информации по электромагнитным и электрическим каналам на объектах СВТ требует, чтобы величина вносимого затухания ФСП, спектральная плотность ЭМПШ ГЭМШ, спектральная плотность ЭШС ГЛЗ обеспечивали, соответственно, необходимое ослабление информативных сигналов в цепях электропитания и заземления, а также необходимое превышение ЭМПШ и ЭШС над информативными сигналами во всем рабочем диапазоне частот.

Рассмотрим, какое влияние на выполнение ТСЗИ-функций по обеспечению защиты информации оказывает современное развитие СВТ.

В настоящее время можно выделить следующие две основные тенденции, оказывающие влияние на нынешнее состояние обеспечения защиты информации, обрабатываемой СВТ, от утечки по каналам ПЭМИ и наводок с помощью ТСЗИ.

Тенденция первая – снижение уровня индустриальных радиопомех от СВТ и повышение помехоустойчивости передачи данных.

Жесткое нормирование допустимых значений индустриальных радиопомех, а также обязательная сертификация СВТ на соответствие международным стандартам по электромагнитной совместимости вынудило разработчиков предпринять ряд мер, направленных на снижение уровня индустриальных радиопомех и, соответственно, уровня ПЭМИ от СВТ в процессе их функционирования (дополнительное экранирование, применение микросхем с пониженным напряжением электропитания и малыми перепадами выходных напряжений, использование метода низковольтной дифференциальной передачи сигналов (LVDS) и специальных алгоритмов избыточного кодирования в последовательных интерфейсах обмена данными и т. п.). Вышеперечисленные меры при прочих равных условиях повышают эффективность СЗСИ (ФСП, ГЭМШ, ГЛЗ) по обеспечению защиты информации.

Тенденция вторая – повышение быстродействия современных СВТ.

Эту тенденцию рассмотрим на примере персональных компьютеров как наиболее распространенных СВТ, применяемых для обработки защищаемой информации. Практика показывает, что наиболее опасными с точки зрения возможной утечки обрабатываемой информации по электромагнитному и электрическому каналам являются цепи интерфейсов обмена данными, которые вследствие своей значительной протяженности представляют собой эффективные излучающие антенны.

Если рассматривать эволюцию интерфейсов обмена данными в персональных компьютерах, то следует отметить ярко выраженную тенденцию их развития, направленную на повышение максимальных скоростей обмена данными, а также на переход от параллельных интерфейсов к последовательным.

Так, например, параллельные интерфейсы обмена с НЖМД типа IDE, ATA и SCSI в современных ПЭВМ повсеместно заменены на последовательный интерфейс SATA, модификация SATA-3 которого имеет пропускную способность 750 Мбайт/с (или 6,0 Гбит/с).

Универсальный последовательный интерфейс USB обеспечивает скорость обмена данными до 5 Гбит/с (версия USB 3.0).

Совершенствуются также интерфейсы передачи данных для цифровых дисплеев. Так, например, ассоциацией VESA разработан видеоинтерфейс DisplayPort для соединения системного блока компьютера с дисплеем. Максимальная пропускная способность одного канала видеоинтерфейса DisplayPort составляет 2,7 Гбит/с. Производители электронной техники (Hitachi, Panasonic, Philips, Sony, Thomson) разработали новый быстродействующий интерфейс HDMI для передачи мультимедиа высокой четкости, позволяющий передавать цифровые видеоданные высокого разрешения и многоканальные цифровые аудиосигналы. HDMI начинает внедряться в современные персональные компьютеры. Следует отметить, что его максимальная пропускная способность составляет 10,2 Гбит/с.

Нетрудно заметить, что максимальные рабочие частоты всех вышеперечисленных интерфейсов обмена данными значительно превышают рабочий диапазон частот большинства ТСЗИ, приведенных в табл. 1–3, что может привести к утечке информации, обрабатываемой СВТ, по техническим каналам. Несколько лучше в плане обеспечения защиты информации выглядит генератор шума «Маис-М» (РФ) с максимальной рабочей частотой 10 ГГц, но и этого диапазона частот уже недостаточно для защиты информации, передаваемой, например, по интерфейсу HDMI.

Таким образом, применение для обработки информации современных персональных компьютеров с новыми типами интерфейсов обмена данными требует дальнейшего совершенствования ТСЗИ, применяемых для защиты обрабатываемой информации.

В связи с этим разработчикам следует максимально форсировать модернизацию ТСЗИ, в частности расширение их рабочего диапазона частот, а также решение других сопутствующих проблем (например, выделение расширенного диапазона частот для ГЭМШ).

УДК 004.056.53

В.В. Мирончик

ЗАЩИТА АУДИОФАЙЛОВ С ПОМОЩЬЮ ВНЕДРЕНИЯ СКРЫТОЙ ИНФОРМАЦИИ

В настоящее время аудиофайлы являются одним из наиболее уязвимых объектов в сети Интернет. Для защиты аудиофайлов эффективно объединение методов компьютерной стеганографии и криптографии. При использовании криптографии информация модифицируется по определенному алгоритму, в результате преобразований завуалирован смысл сообщения. Стеганография скрывает сам факт передачи или хранения информации внедрением ее в различные мультимедийные объекты, которые не теряют от этого своих потребительских свойств. В основе применения компьютерной стеганографии лежит неспособность органов чувств человека различать незначительные изменения в цвете изображения или качестве звука, что особенно легко использо-

вать применительно к объекту, несущему избыточную информацию. Органы слуха человека воспринимают звуковые частоты по-разному. Стеганографические алгоритмы обработки звука строятся с таким расчетом, чтобы максимально использовать окно слышимости и другие свойства речевых сигналов (тембр, скорость и т. д.), незначительные изменения которых человек различить не может.

Развитие и распространение сетевых методов общения привело к появлению новых способов передачи скрытой информации в аудиофайлах. Существует метод ее внедрения с помощью кодирования информации двоичным кодом, а двоичный код, в свою очередь, управляет громкостью звучания нот, следующих друг за другом. Используется следующий алгоритм: если скрывается логическая единица, то значение громкости должно быть нечетным числом, а если логический нуль – четным. Обнаружить сделанное вложение на слух невозможно, так как, во-первых, изменения громкости незначительны, а во-вторых, изменение громкости на одну единицу невозможно зарегистрировать на слух, однако можно использовать для скрытой передачи информации. Кроме того, запись секретной информации может быть осуществлена в партию лишь одного инструмента (например, контрабаса), что при звучании целого оркестра (или ансамбля) еще больше акустически маскирует скрытое сообщение.

Внедрение информации в аудиофайл также можно осуществить с помощью вариации порядка записи одновременно происходящих событий. При использовании данного метода к файлу не добавляется новая информация и размер файла не изменяется. С помощью этого метода удобно внедрять информацию в одновременно исполняемые ноты (аккорды). Порядок записи нот в листе событий не имеет никакого значения для воспроизводящей аппаратуры, а вариация их взаимного расположения при записи позволяет скрыто передать символы.

Известен также метод внедрения информации в аудиофайлы путем использования разности времени между записанными в файл событиями, которые не изменяют характеристики (настройки) устройства воспроизведения. Это происходит, например, когда подряд следуют несколько одинаковых управляющих событий. Суть данного метода заключается в кодировке скрытого сообщения временем между изменением уровня громкости аудиосигнала.

Ухо человека воспринимает звуковые волны длиной примерно от 20 м до 1,6 см, что соответствует 16–20 000 Гц при передаче колебаний по воздуху и до 220 кГц при передаче звука по костям черепа. Звуковые волны в диапазоне 300–4000 Гц соответствуют человеческому голосу. Среди музыкальных инструментов наибольшим частотным диапазоном обладает рояль (27–4200 Гц). Внедрение дополнительной информации в диапазоне частот, соответствующему голосу человека,

целесообразно с точки зрения дальнейшей передачи ее по каналам связи. Шифрование с помощью нот позволяет использовать различные комбинации в одном частотном диапазоне, а также удобно для записи в исходный аудиофайл. В данном методе нет необходимости изменять исходный сигнал и переносить скрываемую информацию за пределы окна слышимости, достаточно снизить уровень звука добавляемого музыкального фрагмента до уровня шума.

Субъективное восприятие шума зависит от его физической структуры и психофизиологических особенностей человека. Следует также учитывать и тот факт, что неслышимые звуки могут оказать вредное воздействие на здоровье человека. Следовательно, изменения в аудиосигнале не должны быть ощутимы для человеческого слуха и в то же время не должны оказывать вредное воздействие на психоэмоциональное состояние, выходить за частотную область, безопасную для жизнедеятельности человека.

Таким образом, аудиофайлы могут быть успешно использованы для передачи скрытой информации, которая может нести в себе сведения об авторе. Однако обязательным является наличие секретного ключа, который должен определять, каким способом и в каких местах скрыта конфиденциальная информация.

Применение компьютерной стеганографии одновременно с криптографией позволяет эффективно решать проблему защиты авторских прав на мультимедийную продукцию. Но в то же время использование музыкальных фрагментов для скрытой передачи сообщения значительно упрощает скрытие информации, так как нет необходимости переносить спектр сигнала за пределы окна слышимости, достаточно снизить уровень звука. Таким образом, музыкальные фрагменты будут расположены в аудиозаписи в пределах окна слышимости человека, но в то же время не будут заметны, так как уровень их звука будет значительно меньше уровня звука основной аудиоинформации.

УДК 004.056.5

А.А. Мытницкий А.А. Загуменнов, А.С. Кравченко

АСИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ В ПЕРСОНАЛЬНЫХ СРЕДСТВАХ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

При использовании шифрования с закрытым ключом возникают две достаточно серьезные проблемы. Первая проблема заключается в изготовлении секретных ключей и доставке их участникам информацион-

ного обмена. При большом количестве и территориальной распределенности участников информационного обмена, использующих каналы связи общего назначения, например обычную или электронную почту, часто бывает сложно гарантировать безопасность доставки такого ключа и его подлинность.

Второй проблемой является обеспечение подлинности партнеров при электронном общении. Развитие деловой переписки и электронной коммерции требует методов, при использовании которых невозможно было бы подменить кого-либо из участников процесса. Получатель корреспонденции должен иметь возможность удостовериться в подлинности документа, а создатель электронного послания – в состоянии доказать свое авторство получателю или третьей стороне. Следовательно, электронные документы должны иметь аналог обычной подписи.

В настоящее время асимметричные алгоритмы широко применяются на практике для обеспечения информационной безопасности телекоммуникационных сетей, в том числе сетей, имеющих сложную топологию; для обеспечения информационной безопасности в глобальной сети Internet; в различных банковских и платежных системах (в том числе использующих интеллектуальные карты) и т. д.

Асимметричные алгоритмы шифрования называются также алгоритмами с открытым ключом. В отличие от алгоритмов симметричного шифрования, в которых для шифрования и расшифрования используется один и тот же ключ, в ассиметричных алгоритмах один ключ используется для шифрования, а другой, отличный от первого, – для расшифрования. Алгоритмы называются асимметричными, так как ключи шифрования и расшифрования разные, следовательно, отсутствует симметрия основных криптографических процессов. Один из двух ключей является открытым (public key) и может быть объявлен всем, а второй – закрытым (private key) и должен держаться в секрете. Какой из ключей, открытый или закрытый, используется для шифрования, а какой для расшифрования, определяется назначением криптографической системы.

Алгоритмы шифрования с открытым ключом можно использовать для решения, как минимум, трех задач:

1) для шифрования передаваемых и хранимых данных в целях их защиты от несанкционированного доступа;

2) формирования цифровой подписи под электронными документами;

3) распределения секретных ключей, используемых потом при шифровании документов симметричными методами.

Для решения проблемы снабжения пользователей ключами шифрования/расшифрования можно использовать принцип шифрования

Диффи и Хеллмана, придуманный в 70-х г. XX в., основанный на использовании двух разных ключей, хотя и связанных между собой, но устроенных так, что вычислить по одному из них другой практически невозможно.

Согласно Диффи и Хеллману предварительно распределяемые закрытые ключи вообще не должны использоваться для шифрования данных. Закрытый ключ должен быть известен только одному лицу – его владельцу. Такой принцип использования асимметричных алгоритмов получил название открытого шифрования или шифрования с открытым ключом.

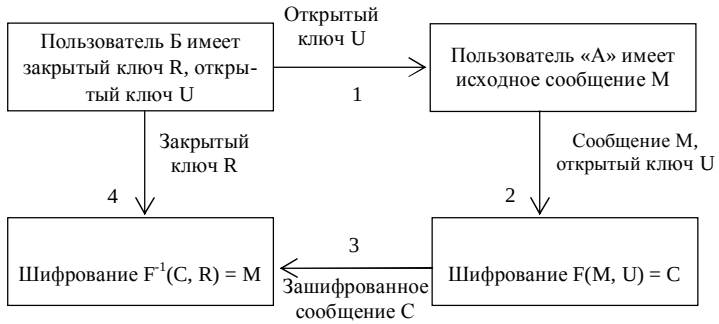
Используя это принцип, любой желающий может зашифровать сообщение открытым ключом. Расшифровать его сможет только владелец закрытого ключа. Например, пользователи А и Б, имеющие возможность обмениваться электронными сообщениями, используют схему открытого шифрования. Предположим, пользователь А должен передать секретное сообщение пользователю Б так, чтобы никто другой не смог его прочитать. Для этого необходимо выполнить следующие действия:

1. Пользователь Б посылает пользователю А свой открытый ключ U по любому каналу связи, например по электронной почте.

2. Пользователь А шифрует свое сообщение M полученным открытым ключом U и получает зашифрованное сообщение C.

3. Зашифрованное сообщение C пересылается пользователю Б.

4. Пользователь Б расшифровывает полученное сообщение C своим закрытым ключом R.



Если операцию шифрования обозначить как F, а операцию расшифрования как F^{-1}, то схему протокола обмена информацией между пользователями можно изобразить схематично.

Аппаратная реализация вычислений без привлечения ресурсов компьютера – это важное отличие персонального средства криптографической защиты информации (ПСКЗИ) ШИПКА от других известных решений на базе USB-ключей, которые фактически представляют собой только энергонезависимую память и адаптер USB-интерфейса, а весь критичный уровень вычислений реализован программно. В ШИПКЕ программно реализуются только не влияющие на безопасность транспортные процедуры и процедуры согласования форматов данных, все остальные функции выполняются аппаратно.

Сегодня ШИПКА является первым и пока единственным аппаратным персональным средством защиты информации в Российской Федерации.

В отличии от некоторых других разработок USB-устройства компании «ОКБ САПР» являются легальными, что обеспечивается членством «ОКБ САПР» в USB-ассоциации. Идентификатор USB-устройств разработки «ОКБ САПР»: 17E4. Являясь USB-устройством, ШИПКА не требует использования картридеров – довольно дорогих устройств, необходимых для работы со смарт-картами, а это значит, что использование ШИПКА в качестве смарт-карты не только удобнее, но и экономичнее.

Сертификат открытых ключей, или цифровой сертификат – это подписанная электронной цифровой подписью удостоверяющего центра (УЦ) пара ключей (персональные данные пользователя + его открытый ключ). Подпись УЦ гарантирует:

соотнесенность сведений, содержащихся в сертификате, с пользователем;

целостность этих сведений (попытка вмешательства в структуру или данные сертификата нарушают его целостность, соответственно, если подтверждена целостность, то изменений каких-либо данных в сертификате, в том числе и подмены открытого ключа, не было).

Цифровые сертификаты широко используются в системе управления открытыми ключами (Public-Key Infrastructure, PKI), так как позволяют пользователям обмениваться открытыми ключами уже непосредственно друг с другом фактически без участия третьей стороны. Применение цифровых сертификатов в системе PKI позволяет упростить процесс работы с ключевой информацией. При обмене зашифрованными данными сессионный ключ просто зашифровывается на открытом ключе получателя сообщения и подписывается на закрытом ключе отправителя.

Взаимодействие пользователя с УЦ обеспечивается с помощью программного комплекса «Атликс-клиент», который, в частности, генерирует ключевую пару (закрытый и открытый ключ) и записывает ее на ключевой носитель. В качестве такого носителя может использоваться ПСКЗИ ШИПКА.

В обновленном программном обеспечении ПСКЗИ ШИПКА предусмотрена возможность работы с самоподписанными сертификатами.

Таким образом, использование ПСКЗИ ШИПКА является актуальным и целесообразным в уголовно-исполнительной системе, так как позволяет безопасно и быстро передавать конфиденциальную информацию по открытым каналам связи.

УДК 681.5:002.5

Ф.Г. Нестерук

СПЕЦИФИКА ДВУХУРОВНЕВОЙ ОРГАНИЗАЦИИ АДАПТИВНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

В публикации рассмотрены особенности организации двухуровневой организации адаптивных систем защиты информации на базе средств интеллектуального анализа данных как начала многоуровневой.

Цель публикации – рассмотреть специфику использования интеллектуального анализа данных при организации адаптивных уровней системы защиты информации.

Рассматривается система защиты информации с двухуровневой структурой. Если в известных работах уровни адаптивных средств классификации имели одинаковую структуру, то в нашем случае она разная.

При проектировании адаптивной системы защиты информации следует учитывать комплексный характер решаемой задачи.

Связующим звеном адаптивной модели системы защиты информации является методика оценки защищенности ИТ-системы, которая координирует взаимосвязь классификаторов угроз и механизмов защиты (в виде нечетких сетей, нечетких нейронных сетей, систем нечетких предикатных правил), структурной модели системы информационной безопасности, инструментальных средств расчета показателей защищенности и рейтинга ИТ-системы.

Динамичный характер поля угроз выдвигает свойство адаптивности ИТ-систем в разряд первоочередных качеств, необходимых системе защиты информации (СЗИ). С другой стороны, не менее важным качеством является возможность реализации в СЗИ накопленного опыта, который представлен в виде информационной компоненты иерархии механизмов защиты. Тем не менее нецелесообразно в объекте информатизации использовать всевозможные механизмы защиты, а логичнее ограничиться минимальным комплектом, достаточным для отражения угроз, оговоренных в спецификации на проектирование ИТ-системы.

В соответствии с заданием на проектирование системы защиты информации выбирается структурная модель системы информацион-

ной безопасности в виде иерархии уровней механизмов защиты, а априорный опыт экспертов представляется массивами экспертных оценок, на базе которых формируются системы нечетких предикатных правил для классификации угроз по признакам атак, механизмов защиты на поле угроз.

Системы нечетких предикатных правил для последующей адаптации и анализа представляются в виде нечетких нейронных сетей, которые обучают на некотором подмножестве входных векторов признаков атаки. Одновременно обучают классификаторы в виде обычных нейронных сетей таким образом, чтобы число образуемых кластеров равнялось числу правил в системе нечетких предикатных правил, аналогичный процесс относительно нейросетевых классификаторов механизмов защиты по векторам известных угроз.

Для исходных массивов экспертных оценок производят расчет показателей защищенности и рейтинга ИТ-системы, которые используются методикой оценки защищенности ИТ-системы для анализа и коррекции как массивов экспертных оценок, так и функциональных параметров нейросетевых классификаторов и систем нечетких предикатных правил.

Информация в адаптивной СЗИ хранится и может передаваться в поколениях. Процесс адаптации связан с решением задач классификации, кластеризации, приводящих к расширению информационного поля известных угроз на нижних уровнях иерархии СЗИ. Изменение перечня известных угроз информационной безопасности отражается на верхних уровнях иерархии СЗИ в соответствующей модификации информационного поля жизненного опыта, реализованного в виде специализированных структур нечетких нейронных сетей, которые, в свою очередь, описываются системами нечетких предикатных правил. Процесс адаптации поля жизненного опыта рецепторных уровней защиты связан с обучением нечетких нейронных сетей, т. е. конструктивные алгоритмы обучения, которые адекватно видоизменяют систему нечетких предикатных правил, ставящую в соответствие известным угрозам механизмы защиты информации.

Целесообразно при сохранении двухуровневой иерархии систем защиты информации, содержащей адаптивные средства классификации, обеспечить различную степень автоматизации при реализации функций защиты информации, таким образом:

нижний уровень становится интеллектуальным (аналог иммунных механизмов в организме, которые работают оперативно и автоматически практически без коррекции со стороны головного мозга – центральной нервной системы организма);

верхний уровень соответствует процессам запоминания в центральной нервной системе организма, которая работает значительно медленнее и накапливает опыт под контролем и при участии администратора безопасности.

В момент создания интеллектуального уровня в него с верхнего уровня иерархии загружают (этап наследования-передачи опыта) исходные базы данных и базы знаний, начальные методы их взаимодействия с внешним миром и их собственной коррекции.

Нижний уровень постоянно взаимодействует с внешним миром (интернетом) и автоматически изменяется (постоянно реализуемый этап развития). Причем в процессе работы интеллектуального уровня в режиме текущего состояния изменяются как исходные базы данных и базы знаний, так и методы их взаимодействия с внешним миром и их собственной коррекции (постоянно выполняемый этап развития – адаптация к внешним условиям, реализуется основное свойство – пластичности). А в режиме памяти изменяются как исходные базы данных и базы знаний, так и методы их взаимодействия с внешним миром и их собственной коррекции, но в результате взаимодействия с информационной базой текущего состояния и целевых установок верхнего уровня (администратора безопасности) фиксируются в памяти только существенные изменения, и реализуется основное свойство – стабильность.

Для организации информационной связи с внешним миром необходимы посредники – параметры физической среды, через которые можно судить о динамике воздействия интернета. Когда речь идет, например, о сайте в интернете, то нельзя разделять функции анализа интересов от функций защиты информации, т. е. исходя из одной совокупности параметров будут классифицироваться как интересы, так и угрозы. Функции классификации интересов и классификации угроз будут разнесены, а при оценке рисков, наоборот, эти функции будут рассматриваться вместе как входные параметры интеллектуальной информационной системы.

В качестве входных параметров могут выступать (для рассмотренного примера):

статистика сайта (анализ интернет-адресов: из каких доменов, частота повторения адресов, частота посещения сайта, маршруты перемещения по карте сайта и пр.);

статистика операционной системы (открытие, закрытие файлов, операции над файлами, временные параметры, попытки обращения к системным файлам и защищаемым областям памяти и пр.)

На основе рассмотренной двухуровневой организации адаптивных систем защиты информации, на базе средств интеллектуального анализа данных возможно добавление и развитие создаваемых под поставленные задачи дополнительных уровней, реализующих требуемые функции.

УДК 004.056.53

К.С. Никитенков, М.А. Вус

РУКОВОДСТВО ПО АНАЛИЗУ И ОЦЕНКЕ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ ПРИЛОЖЕНИЙ

Доклад посвящен представлению авторского Руководства по анализу и оценке безопасности корпоративных приложений (далее – Руководство). Представляемое Руководство содержит рекомендации по проведению анализа и оценки, а также по повышению общего уровня безопасности корпоративных приложений. Разработанный в рамках дипломной работы методический материал предназначен для широкого использования, он успешно прошел апробацию, имеет положительные отзывы целевой аудитории.

Бизнес приложения – это программное обеспечение или набор компьютерных программ, которые используются для выполнения различных бизнес – функций, повышения производительности компании. Состав и характеристики таких программ определяются потребностями, возникающими в бизнесе, а также зависят от размеров компании и растут пропорционально увеличению объема выполняемых работ. Одним из типов бизнес-приложений, применяемых в крупном бизнесе, являются корпоративные приложения, или Enterprise Application Software (EAS). Под ними обычно подразумевается программное обеспечение, которое может быть использовано в бизнес-целях для решения проблем управления предприятием. Такие масштабные программные комплексы направлены на улучшение производительности и повышение эффективности работы предприятия и ориентированы на удовлетворение потребностей компании в целом, а не только отдельных пользователей.

Современные корпоративные приложения состоят из множества настраиваемых программ и сервисов, позволяющих повысить производительность подразделений хозяйствующего субъекта, а также обеспечить их непрерывное и оперативное взаимодействие. Область применения подобных приложений и интернета для управления бизнесом растет, как и требования к безопасности. Однако большинство существующих рекомендаций и способ изложения материала ориентированы преимущественно на специалистов достаточно высокой квалификации.

На рынке сегодня присутствуют продукты разных производителей, отличающиеся своими характеристиками. Выбор конкретного корпоративного приложения определяет множество факторов: масштабы компании и объем производства, бюджет на внедрение подобного решения и др.

В материалах аналитического исследования «The 2014 Manufacturing ERP Report» от Panorama Consulting по состоянию на 2013 г. поставщики ERP-систем разделены на четыре группы по мере уменьшения доли присутствия на рынке: SAP – 16,7 %; Oracle – 14,3 %; Microsoft – 7,1 %. На долю всех остальных (BatchMaster Software, CDC Software, Consona Corporation, IFS North America, NetSuite, Service Pro и др.) приходится 21,4 %.

Десятилетие назад при разговоре о каких-либо сложных комплексных информационных системах в бизнесе, прежде всего, имелись в виду ERP-системы. Enterprise Resource Planning (ERP) – это организационная стратегия интеграции производства и отдельных операций, а также организационная стратегия управления ресурсами (трудовыми, финансовыми и пр.), обеспечивающая общую модель данных и процессов для всех сфер деятельности. Соответственно, ERP-система – конкретный программный пакет, реализующий стратегию ERP. Следуя сложившимся в практике традициям, автор употребляет термины ERP и EAS как синонимы во всех случаях, где нет необходимости указания на их различия.

SAP NetWeaver – самый известный продукт компании SAP. ERP-система, ориентирована на крупные и средние предприятия. Центральным продуктом платформы NetWeaver является SAP NetWeaver Application Server (прежнее название – SAP Web Application Server). Этот продукт выполняет функции сервера корпоративных приложений для решений компании.

В течение последних семи лет специалистами в области безопасности SAP было представлено множество аналитических отчетов и докладов, в которых подробно рассматриваются особенности различных атак на подсистемы SAP. С каждым годом интерес к теме стремительно возрастает. Если в 2006 г. на специализированных технических конференциях по взлому и защите был всего 1 доклад по безопасности SAP, то в 2011 г. – более 20, а в 2012 г. о возрастающей популярности темы можно было судить по более чем 30 различным публикациям. В текущем году порядка 20 докладов были представлены только в первой половине года. Однако, как показывает практика, несмотря на увеличивающееся с каждым годом количество найденных в корпоративных приложениях уязвимостей это не только не повышает, но и в некотором смысле даже понижает уровень обеспечения безопасности таких приложений в различных компаниях.

Возрастающая актуальность проблемы безопасности «больших приложений» еще в начале века породила необходимость создания стандартов, описывающих корректное осуществление их настроек и последовательность выполнения таких операций. Разработкой и публикацией подобных стандартов в разное время начали заниматься та-

кие компании, как SAP, ISACA, DSAG, BIZEC. Примкнули к этому ряду и российские специалисты из Digital Security и ERPScan.

В целях повышения осведомленности пользователей, администраторов и разработчиков EAS об актуальных проблемах безопасности, а также в целях выработки и формализации руководящих принципов и описания инструментов безопасной настройки, разработки и оценки защищенности корпоративных приложений ведущим партнером SAP AG по обнаружению и закрытию уязвимостей – компанией ERPScan в 2010 г. был открыт крупный проект OWASP EAS (OWASP Enterprise Application Security – Безопасность корпоративных приложений OWASP). На протяжении трех лет своего существования этот проект стал охватывать все более широкую область приложений «большого масштаба» и в конечном счете вышел за рамки Web-приложений (что подразумевает под собой OWASP). Таким образом, проект стал полностью самостоятельным и получил новое название – Enterprise Application Software Security (безопасность бизнес-приложений), или EAS-SEC.

В ноябре 2013 г., на конференции по практической безопасности ZeroNights автором был анонсирован дочерний проект Enterprise Application Security Implementation Assessment Guide, а также выпущенное в его рамках «Руководство по анализу безопасности платформы SAP NetWeaver ABAP». Основанием для разработки этого документа явились результаты работ автора по анализу доступных ему существующих методических документов и фирменных материалов. Проведенный анализ выявил наличие в каждом из таких руководящих документов тех или иных недостатков. Это и побудило возникновение идеи о создании более совершенного документа.

При разработке данного руководства требовалось удовлетворить ряд противоречивых требований. Необходимо было охватить как можно более широкий спектр таких проблемных областей в корпоративных приложениях, для которых необходимо проведение анализа и оценки безопасности. Наряду с этим допустимый объем будущего документа диктовал требование обозначить и показать критичные проблемы, оказывающие негативное воздействие на систему, определить приоритеты для их ликвидации. В то же время требовалось не только обеспечить возможность использования Руководства для реализации первых шагов по настройке системы и по введению в производственную эксплуатацию, но и обозначить дальнейшие направления работы для каждой описываемой проблемы, представив их в виде дополнений к обязательным решениям по ее устранению. Важно было также обеспечить четкость и однозначность сформулированных требований и предписаний, показать важность и необходимость их выполнения и описать это языком, который был бы понятен специалистам любого

направления и уровня подготовки. Наряду с этим значимо было учесть возможность использования данного руководства для любых корпоративных приложений без ориентации на их производителя и вне зависимости от количества дополнительных модулей, пользовательских настроек и параметров. Помимо этого важно было предусмотреть в последующем возможное развитие, поддержку и (в случае необходимости) доработку документа на основе обратной связи и отзывов от целевой аудитории.

Таким образом, ставилась задача сделать его документом, в котором были бы формализованы обязательные технические требования для любых корпоративных приложений.

Разработка документа осуществлялась с учетом опыта международной компании ERPScan – партнера SAP AG на основе анализа материалов исследований, в том числе собственных исследований автора, а также материалов публикаций фирм и компаний, работающих в сфере защиты корпоративных приложений.

В ходе работы над проектом прежде всего были определены границы, внутри которых необходимо реализовывать безопасность. В данном контексте границами явились проблемы, возникающие в процессе внедрения корпоративных приложений. Эту роль на себя взял универсальный, сформированный автором список девяти наиболее известных проблем безопасности корпоративных приложений на этапе их внедрения и эксплуатации – «Top-9 Application Issues». Этот список стал основой для содержательной части документа – каждый из его пунктов соответствует одной из основных одноименных глав.

С позиции удобства использования практические разделы документа структурированы следующим образом. Каждая глава содержит: общее описание анализируемой проблемы; раздел «Что дальше?»; предписания и инструкции.

Каждый пункт предписаний также содержит в себе: описание объекта, в котором обнаружена уязвимость; наиболее характерную угрозу, в которой содержится описание возможных событий, способные привести к нарушениям безопасности; предлагаемые типовые решения, в которых содержатся указания по анализу или устранению уязвимости.

Руководство было официально представлено в ноябре 2013 г. (английская версия – в апреле 2014 г.) и доступно на сайте ERPScan и на сайте проекта eas-sec.org. Планируется к разработке новая расширенная версия на двух языках с публикацией во второй половине 2014 г.

УДК 681.3

А.Л. Осипенко, А.Н. Бабкин

ФОРМИРОВАНИЕ ПОКАЗАТЕЛЯ ЗАЩИЩЕННОСТИ РЕЧЕВОЙ ИНФОРМАЦИИ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Объекты информатизации (ОИ) органов внутренних дел (ОВД) относятся к объектам, ущерб от нарушения информационной безопасности которых, значительный.

С целью защиты речевой информации (РИ) необходимо сформировать показатель ее защищенности и провести комплекс организационных и технических мероприятий, направленных на предотвращение перехвата РИ с помощью средств акустической разведки в процессе проведения конфиденциальных переговоров в защищаемых помещениях.

При формировании показателя защищенности РИ в деятельности ОВД можно использовать следующие параметры:

1) объем $v_{(з)}$ процедур защиты РИ в ОВД и его минимально допустимую величину $v_{(з)}^{(\min)}$;

2) время $t(p)$ реакции на угрозу утечки РИ в деятельности ОВД и его максимально допустимую величину $t_{(p)}^{(\max)}$.

Данные параметры определяются как объективные показатели по защите РИ от ее утечки.

Деятельность по защите РИ в ОВД считается реализованной в полном объеме при выполнении следующего неравенства:

$v_{(з)} \geq v_{(з)min}$, является случайным событием.

Вероятность этого события $P(v_{(з)} \geq v_{(з)\min})$ представляет собой среднее количество адекватно принятых специалистами по защите информации ОВД корректных решений по выявлению и локализации канала утечки РИ относительно общего числа принятых решений по предотвращению.

$$P\left(v_{(з)} \geq v_{(з)\min}\right) = \frac{1}{R}\sum_{r=1}^{R} d_r ,$$

где $d_r = \begin{cases} 1, & при\ v_{(з)r} \geq v_{з}(\min)_r \\ 0, & в\ противном\ случае \end{cases}$,

где $v_{(з)r}$ – объем процедур деятельности по защите РИ ОВД при реагировании на r-ю ситуацию (r = 1, 2, …, R) по противодействию утечке РИ;

$v_{(з)\min\ r}$ – минимально допустимая величина объема процедур деятельности по защите РИ при реагировании на r-ю ситуацию;

R – общее число ситуаций, связанных с предотвращением перехвата РИ, циркулирующей в ОВД в течение интервала времени [t(н), t(о)] исследования его деятельности.

Минимально допустимая величина $v_{(з)\min}$ объема процедур защиты РИ определяется характеристиками источника угроз РИ и имеет для каждой ситуации конкретное значение.

Вероятность $P(v_{(з)} \geq v_{(з)min})$ характеризует полноту реализации в ОВД мер защиты РИ от утечки и может быть использована в качестве одного из частных показателей $Э_{(n)}^{(з)}$ защищенности РИ:

$$Э_{(n)}^{(з)} = P(v_{(з)} \geq v_{(з)\min}) .$$

Меры по защите РИ считаются реализованными своевременно, если время $\tau_{(p)}$ реакции на угрозу утечки РИ в деятельности ОВД не превышает максимально допустимой величины $t_{(p)}^{(\max)}$:

$\tau_{(p)} \leq t_{(p)}^{(\max)}$.

В общем случае входящие величины являются случайными, поэтому выполнение является случайным событием. Вероятность этого события $P(\tau_{(p)} \leq t_{(p)}^{(\max)})$ представляет собой среднее количество своевременно принятых мер по защите РИ в ОВД относительно их общего числа:

$$P\left(t_{(p)} \leq t_{(p)}^{(\max)}\right) = \frac{1}{R}\sum_{r=1}^{R} e_r ,$$

где $e_r = \begin{cases} 1, & при\ t_{(p)_r} \leq t_{(p)r}^{(\max)} \\ 0, & в\ противном\ случае \end{cases}$;

$\tau_{(p)r}$ – время реакции на угрозу утечки РИ в ОВД при реагировании на r-ю ситуацию (r = 1, 2, …, R) по противодействию утечки РИ;

$t_{(p)r}^{(\max)}$ – максимально допустимая величина времени реакции на угрозу на r-ю ситуацию.

Максимально допустимая величина времени $\tau_{(\max)}$ реализации процедур защиты РИ в ОВД определяется характеристиками источника угроз РИ и имеет для каждой ситуации конкретное значение.

Вероятность $P(\tau_{(p)} \le t_{(p)}^{(\max)})$ характеризует своевременность реакции на угрозы утечки РИ в ОВД и может быть использована также в качестве одного из частных показателей $Э_{(c)}^{(з)}$ защищенности РИ:

$$Э_{(c)}^{(з)} = P(t_{(p)} \le t_{(p)}^{(\max)}).$$

При этом в качестве показателя защищенности РИ в деятельности ОВД можно использовать комплексный показатель, учитывающий полноту и своевременность реакции на угрозы утечки РИ в рассматриваемых условиях:

$$Э^{(з)} = Э_{(n)}^{(з)} \cdot Э_{(c)}^{(з)}.$$

С целью аналитического представления показателя необходимо рассмотреть его статистическую интерпретацию как среднее количество своевременных и адекватных реакций на угрозы утечки РИ относительно общего числа ситуаций, связанных с предотвращением перехвата РИ, циркулирующей в ОВД.

Поток угроз утечки РИ в пределах временного интервала $[t_{(н)n}, t_{(о)n}]$ можно представить как стационарный, ординарный и с отсутствием последействия.

Стационарность, ординарность и отсутствие последействия потока угроз утечки РИ в пределах временного интервала $[t_{(н)n}, t_{(о)n}]$ позволяют величины минимально допустимого значения объема процедур защиты речевой информации и максимально допустимого значения времени реакции на угрозу утечки речевой информации представить как случайные величины, имеющие экспоненциальный закон распределения.

Вероятностная интерпретация группы событий, описывающих информационную деятельность ОВД в условиях обеспечения защищенности от утечки РИ, обеспечивает:

полноту представления целевой функции эффективности информационной деятельности ОВД;

представление основных физических параметров как информационной деятельности ОВД и процесса защиты РИ, так и способов реализации угроз ее утечки;

оценку степени влияния угроз утечки РИ и механизмов защиты информации на эффективность информационной деятельности ОВД.

УДК 004.047

Ю.Н. Познанский

ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОРГАНОВ ПРЕДВАРИТЕЛЬНОГО СЛЕДСТВИЯ СИСТЕМЫ МВД РОССИИ

Последние десятилетия отмечены широким вторжением современных информационных технологий в сферу жизнедеятельности людей. Создание высокопроизводительных компьютеров открыло большие перспективы роста производительности информационных систем. Уровень их развития создает предпосылки для решения задач по повышению эффективности расследования уголовных дел и управления деятельностью органов предварительного следствия (ОПС) в системе МВД России на качественно новом уровне.

Однако наряду с этим можно констатировать и факт очевидной тенденции «технизации» преступных деяний организованных преступных группировок, которые все чаще используют новые информационные технологии и возможности всемирной глобальной сети Интернет для совершения преступлений и оказания противодействия расследованию преступлений. С целью уклонения от ответственности за совершенное преступление или, по меньшей мере, с целью добиться незаслуженного смягчения наказания преступники или лица, оказывающие им содействие, различными способами (иногда преступными) желают получить информацию, которой располагает следователь по конкретному уголовному делу, либо о самом следователе или следственном подразделении и т. п.

Если в начале 90-х гг. XX в. информация по уголовным делам о сотрудниках следственных подразделений в основном содержалась на бумажных носителях, то с внедрением в деятельность ОПС в системе МВД России компьютерных технологий круг носителей информации значительно расширился. В этой связи организация защиты информации от несанкционированного доступа должна носить превентивный, комплексный характер и основываться на глубоком анализе возможных негативных последствий.

Однако прежде чем приступить к перечислению мер, способствующих обеспечению действенной защиты информации в следственной работе, необходимо определиться, какие информационные технологии используются в настоящее время в работе ОПС в системе МВД России и информация какого рода в них содержится.

С августа 2004 г. ОПС в системе МВД России принимают участие в реализации программы МВД России «Создание Единой информационно-телекоммуникационной системы органов внутренних дел» (ЕИТКС).

С этого времени началось активное создание в ОПС на всех уровнях (федеральном, окружном, региональном, районном) локальных вычислительных сетей (ЛВС), объединенных средствами телекоммуникации ЕИТКС, с задачей построить единую автоматизированную систему ОПС в системе МВД России (АС ОПС).

Целью создания АС ОПС является организация единого информационного пространства ОПС в системе МВД России, упорядочение информационных потоков, повышение качества, эффективности и оперативности деятельности ОПС в системе МВД России. АС ОПС должна стать основным источником получения оперативно-справочной, нормативной правовой и методической информации в процессе расследования преступлений следователями органов внутренних дел, обеспечивая при этом возможность контроля за своевременным и качественным выполнением следственных действий, соблюдением процессуальных сроков, законностью и обоснованностью принимаемых процессуальных решений на всех этапах расследования.

Структурно АС ОПС состоит из централизованного банка данных электронных копий (ЦБД) материалов уголовных дел, формируемого на федеральном и региональном уровнях и специализированной территориально-распределенной автоматизированной системы органов предварительного следствия (СТРАС ОПС). ЦБД электронных копий материалов уголовных дел предназначен для оперативного представления информации об органе расследования; о лицах, привлеченных к уголовной ответственности; фабуле и квалификации совершенного преступления; объектах преступных посягательств; о свидетелях и юридических лицах, проходящих по уголовным делам. СТРАС ОПС представляет собой комплексы программ, устанавливаемых на автоматизированные рабочие места (АРМ) следователей и руководителей органов предварительного следствия, объединенных в локальные вычислительные сети и работающих с выделенным сервером баз данных или на автономных рабочих местах.

Комплекс технических средств АС ОПС включает средства обработки данных АРМ, серверы баз данных, почтовые серверы, средства обмена данными в ЛВС с возможностью выхода в ЕИТКС (кабельная система, мосты, шлюзы, модемы и т. д.), а также средства хранения (в том числе архивирования) данных. АРМ являются структурообразующими компонентами ЛВС и подразделяются на две категории: рабочие станции пользователей и системных администраторов ЛВС. В свою очередь, рабочие станции пользователей можно подразделять на обеспечивающие работу следователей и руководителей следственных подразделений. АРМ пользователей оснащаются стандартным

набором прикладных программных средств для решения типовых задач служебной деятельности.

Таким образом, отличительной функциональной особенностью АС ОПС является ее двойственность. С одной стороны, решаются задачи непосредственной информационной поддержки деятельности следователей при выполнении ими своих функциональных обязанностей – расследовании преступлений и обеспечении их техникой, способной обрабатывать большое количество процессуальных документов в ходе расследования уголовных дел. С другой, обеспечивается решение управленческих задач с возможностью контроля за своевременным и качественным выполнением следственных действий, соблюдением процессуальных сроков, законностью и обоснованностью принимаемых процессуальных решений на всех этапах расследования.

В соответствии с законом Российской Федерации «Об информатизации, информационных технологиях и защите информации» по категории доступа делится на два вида: общедоступная информация и информация ограниченного (ограничен федеральными законами в целях защиты конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства). Доступ к информации ограничивается, если она содержит сведения, отнесенные к государственной тайне, или конфиденциальные сведения.

В настоящее время к конфиденциальным сведениям в Российской Федерации относятся: сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях; сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты.

Исходя из вышеприведенного перечня сведений, относящихся к конфиденциальной информации, можно сделать вывод о том, что в АС ОПС содержится или может содержаться информация ограниченного доступа, которую можно отнести к категориям: сведения, составляющие тайну следствия и судопроизводства; сведения о защищаемых лицах и мерах государственной защиты; служебные сведения. Наряду с этим сотрудниками подразделений по работе с личным составом ОПС в системе МВД России с использованием АРМ и различных специализированных АИС, предназначенных для кадровых подразделений, производится сбор, обработка и хранение сведений о личном составе, проходящем службу в ОПС. Данные сведения относятся к конфиденциальной информации как персональные данные. Таким образом, в АС ОПС за-

щите подлежат все информационные ресурсы – создаваемые, аккумулируемые (хранимые), обрабатываемые и используемые.

Под защитой информации понимается принятие правовых, организационных и технических мер, направленных на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; соблюдение конфиденциальности информации ограниченного доступа; реализацию права на доступ к информации.

В связи с этим целью обеспечения информационной безопасности АС ОПС можно определить защиту субъектов информационных отношений (интересы которых затрагиваются при создании и функционировании АС ОПС) от возможного нанесения им ощутимого материального, физического, морального или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования АС ОПС или несанкционированного доступа к циркулирующей в ней информации и ее незаконного использования.

Субъектами обеспечения защиты информации в АС ОПС являются: сотрудники ОПС, обеспечивающие эксплуатацию АС ОПС; сотрудники подразделений ОПС – пользователи и поставщики информации в АС ОПС в соответствии с возложенными на них функциями; сотрудники подразделений и служб центрального аппарата МВД России, подразделений МВД, ГУ (У) МВД России, обеспечивающие информационное взаимодействие и регламентированный доступ к информационным ресурсам АС ОПС; сотрудники подразделений и служб органов внутренних дел, а также вневедомственных организаций, являющиеся удаленными пользователями (в качестве поставщиков и потребителей информации) АС ОПС; другие юридические и физические лица, задействованные в процессе создания и функционирования АС ОПС (разработчики компонентов АС, вневедомственные организации, привлекаемые для оказания услуг в области информатизации, и др.).

Поставленная цель защиты АС ОПС достигается: строгим учетом всех подлежащих защите ресурсов системы; регламентацией с применением средств автоматизации, процессов обработки подлежащей защите информации и действий сотрудников структурных подразделений ОПС, использующих АС ОПС, а также осуществляющих обслуживание и модификацию программных и технических средств АС ОПС; полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов ОПС по вопросам обеспечения безопасности информации; назначением и подготовкой сотрудников ОПС, ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности информации и процессов ее обработки; наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к ресурсам АС ОПС; четким знанием и строгим соблюдением всеми сотрудниками, использующими и обслуживающими аппаратные и программные средства АС ОПС, требований организационно-распорядительных документов по вопросам обеспечения безопасности информации; персональной ответственностью за свои действия каждого сотрудника, участвующего в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющего доступ к ресурсам АС ОПС; реализацией технологических процессов обработки информации с использованием комплексов организационно-технических мер защиты программного обеспечения, технических средств и данных; принятием эффективных мер обеспечения физической целостности технических средств и непрерывным поддержанием необходимого уровня защищенности компонентов АС ОПС; применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования; эффективным контролем за соблюдением сотрудниками подразделений ОПС – пользователями АС ОПС требований по обеспечению безопасности информации; проведением постоянного анализа эффективности и достаточности применяемых мер и средств защиты информации, разработкой и реализацией предложений по совершенствованию системы защиты информации в АС ОПС.

Выбор программно-аппаратных и организационных (режимных) мероприятий по защите АС ОПС проводится на основании установления класса защищенности. В соответствии с Порядком проведения классификации информационных систем персональных данных АС ОПС является специальной многопользовательской информационной системой 1-го класса (К1).

Под угрожающими факторами понимаются любые действия или ситуации, которые могут привести к нарушению безопасности информации АС ОПС (неисправность оборудования, потеря данных, сбой в работе программного обеспечения, похищение паролей или внедрение вредоносной программы). Угрожающие факторы подразделяются на внутренние и внешние, преднамеренные и случайные. Внутренние угрожающие факторы связаны, прежде всего, с оборудованием и компонентами ЛВС следственных подразделений, а также обслуживающим персоналом и пользователями. Внешние факторы, как правило, исходят от лиц и объектов, находящихся за пределами АС ОПС. Преднаме-

ренные угрожающие факторы направлены на нарушение работы компонентов АС ОПС, которое приводит к похищению, искажению или уничтожению информационных ресурсов. Случайные (непреднамеренные) угрожающие факторы обусловлены различными обстоятельствами непреодолимой силы – природными и техногенными явлениями (пожары, отключение сети питания и т. п.). Вероятность возникновения этих обстоятельств невелика, однако по оказываемому негативному воздействию на АС ОПС они могут значительно превосходить другие угрожающие факторы.

Основные меры по нейтрализации угроз и снижению возможного наносимого ущерба АС ОПС условно можно разделить на организационные и технические. К организационным мерам можно отнести: регламентацию действий, введение запретов; удаление всех потенциально опасных программ с дисков, к которым возможен доступ пользователей АС ОПС; усиление ответственности и контроля; обучение персонала; применение физических средств, препятствующих неумышленному нарушению.

К техническим мерам можно отнести: средства разграничения доступа к ресурсам; резервирование критичных ресурсов; разграничение доступа к технологическим и инструментальным программам на дисках; применение специальных программ обнаружения и уничтожения вирусов и аппаратно-программных средств, препятствующих заражению компьютеров вирусами и несанкционированному внедрению и использованию неучтенных программ; технологические меры контроля за ошибками операторов ввода данных и некоторые другие. Тем не менее, несмотря на разработку достаточно эффективных мер защиты информации, циркулирующей в АС ОПС, на практике их реализация затруднена. В основном это связано с недостаточным обеспечением личного состава компьютерной техникой (в связи с чем используются личные компьютеры для выполнения служебных задач), а также с низким уровнем знаний о мерах по обеспечению защиты информации.

УДК 681.324.067

А.С. Поляков, В.Е. Самсонов

АНАЛИЗ ХАРАКТЕРИСТИК «ОБЛЕГЧЕННОГО» АЛГОРИТМА ШИФРОВАНИЯ PRESENT

Современные алгоритмы шифрования обеспечивают конфиденциальность зашифрованной информации в течение десятков и сотен лет

(разумеется, с учетом современного состояния вычислительной техники). Естественно, что такой большой период защиты информации возможен только благодаря высокой сложности алгоритмов шифрования и соответственно их большой трудоемкости, выражающейся в затратах необходимых ресурсов и времени на шифрование информации.

Вместе с тем появляется все больше приложений, в которых не требуется настолько долговременная защита информации с использованием ресурсоемких алгоритмов, имеющих к тому же сравнительно малое быстродействие (производительность).

В связи с этим в настоящее время активно развивается так называемая легковесная (облегченная) криптография – lightweight cryptography, имеющая своей целью разработку алгоритмов для применения в устройствах, которые не могут обеспечить реализацию большинства существующих шифров из-за недостаточности ресурсов (память, электропитание, размеры и т. п.). Разработка этого направления в последнее десятилетие идет настолько интенсивно, что в 2012 г. был принят международный стандарт – ISO/IEC 29192-2:2012. Information technology – Security techniques – Lightweight cryptography – Part 2: Block ciphers, включающий в себя два алгоритма: PRESENT и CLEFIA. Необходимо отметить, что алгоритмы lightweight cryptography изначально ориентированы на их аппаратную реализацию.

Поскольку эти алгоритмы относятся к новому классу, то для специалистов большой интерес представляют данные об их характеристиках (производительность, требуемые аппаратные ресурсы). В настоящей работе выполнено исследование характеристик алгоритма PRESENT при его реализации на платформе микросхем типа FPGA.

PRESENT – блочный шифр с размером блока 64 бита, имеющий варианты: PRESENT-80 с размером ключа 80 бит и PRESENT-128 с размерами ключей 128, 196 или 256 бит. Авторы алгоритма подчеркивают, что он пригоден для узкоспециальных применений, где не подходит ресурсоемкий алгоритм AES. Алгоритм рассчитан на аппаратную реализацию, его предлагается применять в сверхкомпактных микрочипах для случаев, когда не требуется высокая стойкость шифра.

Шифрование блока данных выполняется за 31 раунд, на каждом из которых производятся операции: сложение по mod 2 текущего состояния блока данных с очередным раундовым ключом; рассеивающее преобразование путем пропускания полубайтов блока данных через 16 одинаковых 4-битовых блоков подстановки; перемешивающее преобразование, предусматривающее перестановку бит в текущем состоянии блока данных в соответствии с заданными правилами; сложение по mod 2 с последним раундовым ключом.

Алгоритм PRESENT-80 и PRESENT-128 по составу операций и порядку их применения идентичны. Разница заключается лишь в том, что в PRESENT-80 раундовый ключ длиной 64 бита формируется из образующего 80-битового ключа, а в PRESENT-128 в качестве образующего используется ключ длиной 128 бит.

Для каждого из алгоритмов с помощью системы проектирования фирмы XILINX были разработаны реализующие их проекты в базисе микросхем типа FPGA, затем произведена имплементация проектов (этапы Synthesize, Translate, Map), в результате чего получены данные о количестве оборудования, необходимого для реализации алгоритмов. С помощью системы ModelSim проведено логическое моделирование проектов, результаты которого позволили определить количество тактов, необходимых для шифрования одного блока данных, а также проверить правильность реализации алгоритмов, для чего использованы тестовые примеры из приложения к стандарту.

Алгоритмы PRESENT могут быть реализованы на дешевых микросхемах серий Spartan 3 и Virtex 4, поскольку требуют использования лишь небольшой части имеющегося в микросхемах оборудования. Например, при реализации на микросхеме Virtex 4 xc4vlx15 для алгоритмов требуется:

Present-80 – логических элементов – 5 %, элементов памяти – 72 %;

Present-128 – логических элементов – 8 %, элементов памяти – 75 %;

ГОСТ 28147-89 – логических элементов – 9 %, элементов памяти – 18 %;

Belt – логических элементов – 14 %, элементов памяти – 87 %;

AES – логических элементов – 27 %, элементов памяти – 11 %.

Временные характеристики алгоритмов

Алгоритм	Размер блока данных, бит	Количество тактов на один блок данных	Количество тактов на блок данных размером 64 бита
PRESENT-80	64	97	97
PRESENT-128	64	97	97
ГОСТ 28147-89	64	129	129
Belt	128	211	106
AES	128	98	49

Как видно из приведенных данных, алгоритмы PRESENT при реализации на аппаратной платформе микросхем типа FPGA лишь незначительно выигрывают у стандартных алгоритмов по требуемым затратам ресурсов, а по быстродействию соизмеримы с алгоритмом Belt и существенно проигрывают алгоритму AES. Такие показатели основных характеристик никак не подтверждают зафиксированный международным стандартом статус алгоритмов PRESENT как легковесных (lightwight) шифров.

УДК 681.324.067

А.С. Поляков, Г.Л. Матюшкова

ДЕЙСТВИТЕЛЬНО ЛИ ЛЕГОК «LIGHTWEIGHT» АЛГОРИТМА CLEFIA?

Появившееся в последние годы направление lightweight cryptography (в русскоязычной литературе переведенное как «облегченная криптография», «легковесная криптография») ориентировано на создание криптографических алгоритмов, реализуемых на различных аппаратных платформах с ограниченными ресурсами, обеспечивающих достаточно высокую производительность при небольших затратах оборудования и, возможно, некоторую потерю криптостойкости. Быстрое развитие этого направления привело к быстрому появлению в 2012 г. международного стандарта ISO/IEC 29192-2:2012. Information technology – Security techniques – Lightweight Cryptography – Part 2: Block ciphers, включающего алгоритмы PRESENT и CLEFIA.

Судя по скорости принятия международного стандарта, есть основания полагать, что направление lightweight-алгоритмов будет активно развиваться и далее в сторону «наилегчайших» (ultra-lightweight) алгоритмов шифрования для устройств, сильно ограниченных в ресурсах. Основанием для такого прогноза является тот факт, что алгоритм PRESENT, включенный в стандарт, авторами изначально был заявлен как ultra-lightweight алгоритм, а один из основоположников этого направления Аксель Пошманн анонсировал облегченную криптографию как криптографическую технику для «общества всепроникающей компьютеризации», имея в виду повсеместное и бурное развитие компьютеризации всех аспектов жизнедеятельности общества, внедрение компьютерных технологий в самые низкоуровневые сферы социальной жизни, характеризующиеся требованием реализации заданных функций с использованием малых объемов ресурсов (памяти, логических элементов и т. п.). Видимо, проблема перехода, по крайней мере, в отдельных областях применения криптографической за-

щиты данных к более простым алгоритмам шифрования созрела настолько, что организации ISO и IEC очень быстро приняли упомянутый выше стандарт.

Алгоритм CLEFIA является симметричным блочным шифром и соответствует требованиям к шифру AES: размер блока 128 бит, поддерживаемая длина ключа – 128, 192 и 256 бит. Структура алгоритма представляет собой сеть Фейстеля с четырьмя ветвями при ключе 128 бит и восемью ветвями при ключах 192 и 256 бит соответственно. Число раундов зависит от длины ключа и равно 18, 22, 26. В зависимости от размера ключа создается массив 32-битовых раундовых ключей в количестве 36, 44, 52 ключа соответственно.

Поскольку алгоритм CLEFIA представлен как «легковесный», то естественно ожидать хороших объемно-временных характеристик при его аппаратной реализации. В данной работе проведено исследование характеристик самой простой версии алгоритма – CLEFIA-128 – при его реализации на широко используемых микросхемах типа FPGA.

Исследование показателей аппаратной реализации алгоритма производилось следующим образом: с помощью системы проектирования фирмы XILINX ISE разрабатывался проект в базисе микросхем типа FPGA, затем производилась имплементация проекта (этапы Synthesize, Translate, Map), в результате чего получены данные о затратах оборудования, необходимого для реализации алгоритма. С помощью моделирующей системы ModelSim выполнено логическое моделирование проекта, результаты которого позволили определить количество тактов, необходимых для шифрования одного блока информации, а также для выполнения отдельных этапов алгоритма. Логическое моделирование позволило также проверить правильность реализации алгоритма, для чего использовались тестовые примеры, приведенные в приложении к стандарту.

Результаты исследования характеристик алгоритма CLEFIA-128 представлены ниже. Для сравнения указаны также соответствующие значения для алгоритмов ГОСТ 28147-89, стандарта СТБ 34.101.31-2011 (Belt) и стандарта США (AES). В частности, при реализации на микросхеме Virtex 4 xc4vlx15 требуются следующие аппаратные ресурсы (в процентах от имеющихся в микросхеме):

Clefia-128 – 37 %,
ГОСТ 28147-89 – 9 %,
Belt – 14 %,
AES – 27 %.

Временные характеристики алгоритмов

Алгоритм	Размер блока данных, бит	Количество тактов на один блок данных	Количество тактов на блок данных размером 64 бита
Clefia-128	128	419	210
ГОСТ 28147-89	64	129	129
Belt	128	211	106
AES	128	98	49

Анализ представленных данных показывает, что «легковесный» алгоритм CLEFIA-128 как по объему затрат оборудования, так и по производительности имеет существенно худшие показатели, чем использованные для сравнения широко применяемые стандартные алгоритмы.

Исследование алгоритмов CLEFIA-192 и CLEFIA-256 не проводилось, поскольку их показатели заведомо будут хуже, чем у CLEFIA-128, в связи с увеличением количества раундов (22 и 26 соответственно вместо 18) и ветвей сети Фейстеля с четырех до восьми.

УДК 681.3

М.В. Пономарёв, А.В. Душкин

СПЕЦИАЛЬНЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ ЗАКЛАДОЧНЫХ УСТРОЙСТВ

Существует большое число специальных методов обнаружения закладочных устройств (ЗУ): радиосканирование; индикация электромагнитного поля; радиоперехват; анализ параметров линий связи и проводных коммуникаций; рефлектометрия линий связи; инфракрасное зондирование и т. д.

Методы радиосканирования, индикации электромагнитного поля и радиоперехвата используются для обнаружения радиоизлучающих ЗУ.

Метод радиосканирования заключается в узкополосном радиоприеме, в заданном частотном диапазоне, с последовательным передвижением по шкале частот. Идентификация источника радиосигнала производится, как правило, на слух. Радиосканирование может осуществляться в ручном и компьютерном режиме. Ручное радиосканирование в связи с большой трудоемкостью применяется для поиска ЗУ, частотный диапазон которого известен хотя бы приблизительно.

Одними из лучших портативных сканирующих приемников являются сканеры производства фирмы AOR (Япония), которые могут сканировать радиоэфир в широком диапазоне частот (AR-3000A – от 0,1 до 2036 МГц, AR-8000 – от 0,5 до 1900 МГц, AR-2700 – от 0,5 до 1300 МГц), а также реализуют режим автоматического выбора типа модуляции (AM, NFM, WFM, USB, LSB, CW). Новые модели сканеров (AR-3000A, AR-8000) реализуют режим работы с управлением от компьютера. Для целей радиосканирования можно использовать специализированный компьютерный комплекс, а также специализированные компьютерные программы («Смерш», «Седиф» и т. п.).

При осуществлении радиосканирования и некоторых других методов обнаружения закладочных устройств, как правило, применяется технология инициации ЗУ, которая заключается в провоцировании их работы путем генерации известного звукового сигнала (например, воспроизведение магнитофонной записи, компьютерная акустическая инициация и пр.).

Если частотный диапазон источника радиосигнала неизвестен, то используется широкополосный радиоприем. Этот метод заключается в приеме суперпозиции радиосигналов в широком частотном диапазоне с помощью специальных широкополосных приемников. Суммарный радиосигнал детектируется на головные телефоны. Прослушивание радиоэфира позволяет опытному оператору сделать вывод о наличии ЗУ, инициированного известным звуковым сигналом.

На качество и разборчивость сигнала в значительной степени влияет фоновый шум, поэтому уровень сигнала должен быть достаточным для его различения и идентификации. В связи с этим оператор должен находиться на достаточно близком расстоянии от источника радиосигнала, иначе обнаружение и контроль последнего будет невозможен.

Для широкополосного радиоприема используются индикаторы поля типа R-10, R-20 (OPTOELECTRONICS, США), имеющие частотный диапазон, соответственно, от 30 до 2000 МГц и от 0,5 до 2500 МГц, или профессиональный поисковый прибор CPM-700 (REI, США) с частотным диапазоном от 0,05 до 3000 МГц.

Метод радиоперехвата практикуется с недавнего времени благодаря появлению специализированных перехватчиков радиосигналов, принцип действия которых основан на автоматическом сравнении уровня сигнала от радиопередатчика и фонового уровня с последующей самонастройкой. Наиболее известным представителем данного класса устройств является радиоперехватчик Xplorer (OPTOELEC, США). Этот прибор позволяет осуществить радиоперехват FM-сигнала в диапазоне от 30 до 2000 МГц за время не более 1 с. Необходимое условие эффективности указанного метода – превышение уровня искомого сигнала над фоновым уровнем. Радиоперехватчик Xplorer (так же, как и прибор CPM-700) может использоваться в режиме «акустической завязки», который заключается в самовозбуждении прибора за счет положительной обратной связи, при этом уровень самовозбуждения зависит от направленности прибора на ЗУ.

Анализ параметров линий связи и проводных коммуникаций заключается в измерении электрических параметров этих коммуникаций и позволяет обнаруживать ЗУ, считывающих информацию с линий связи или передающих информацию по проводным линиям.

Например, в телефонных линиях связи контролируется напряжение, электрический ток, активное и реактивное сопротивление линии, наличие высокочастотных сигналов. На основании измерений делается вывод о факте несанкционированного подключении к линии. Существует широкий класс приборов для контроля телефонной линии, связи. Некоторые из них кроме анализа параметров линии осуществляют функцию подавления подключенных ЗУ.

Прибор для контроля и защиты телефонной линии КОМ-1 (Россия) предназначен для обнаружения параллельно подключенных, а также для подавления последовательно подключенных (в том числе индуктивных) подслушивающих устройств. Обнаружение и подавление производится непосредственно во время телефонного разговора. Этот прибор осуществляет проверку телефонной линии в автоматическом режиме каждые 2 мин и обнаруживает параллельно подключенные подслушивающие устройства на расстоянии до 150 м. Подавление последовательно подключенных подслушивающих устройств осуществляется на расстоянии до 1000 м посредством зашумления телефонной линии в речевом диапазоне частот с превышением уровня шума над уровнем сигнала не менее 10 дБ.

Анализатор телефонной линии «Скат» (Россия), выполненный в виде телефонной розетки, выявляет факт подключения к телефонной линии подслушивающих устройств, о чем сообщает светодиодной индикацией, а также защищает линию от прослушивания за счет микрофонного эффекта путем фильтрации сигналов.

Тест-комплект АТ-2 (Россия), выполненный в кейсе, предназначен для проверки проводных линий на наличие гальванического подключения к ним подслушивающих устройств. Проверка проводится зондирующим сигналом частотой 40 или 400 Гц, обеспечивающим дальность обнаружения до 5000 м (при сопротивлении изоляции 200 кОм).

Система защиты ПТЗ-003 «Прокруст» (Россия) предназначена для обнаружения и подавления телефонных закладок различных типов. Обнаружение проводится путем измерения напряжения в линии, по-

давление осуществляется путем: поднятия постоянного напряжения в линии до 35 В; генерации «белого шума» в линию 50 Гц–10 кГц напряжением до 10 В; генерации ВЧ-помехи амплитудой до 35 В.

Анализатор телефонной линии АТ-23 (Россия) предназначен для мониторинга состояния телефонной линии и сигнализации факта последовательного и параллельного подключения к ней подслушивающих устройств, а также снижения эффективности использования индуктивных датчиков. Прибор регистрирует последовательное подключение подслушивающего устройства с внутренним сопротивлением не менее 30 Ом и параллельное подключение устройства с внутренним сопротивлением не более 100 Ом. Снижение эффективности использования индуктивных датчиков производится за счет уменьшения отношения сигнал/шум в них в 3 раза.

Для обнаружения ЗУ с передачей акустической информации по естественным проводным каналам (телефонная линия, электросеть, цепи пожарно-охранной сигнализации и пр.) используется, также, метод идентификации известного звука «на слух». При такой технологии поиска ЗУ осуществляется прослушивание сигналов в проводной коммуникации с целью обнаружения известного звукового сигнала. Используемая аппаратура – универсальный прибор СРМ-700 со специальным сетевым фильтром VLF-700.

Рефлектометрия линий связи проводится с целью определения расстояния до подозрительного места в линии. Расстояние определяется по осциллографу, на котором фиксируется время задержки импульса, отраженного от неоднородностей линии (места подключения ЗУ к линии). Рассчитанное расстояние откладывается вдоль линии связи с учетом ее трассировки и определяется точное место подключения ЗУ. Метод позволяет обнаруживать ЗУ, считывающих информацию с линий связи или передающих информацию по проводным линиям.

Инфракрасное зондирование производится с помощью специального ИК-зонда и позволяет обнаруживать ЗУ, осуществляющие передачу информации по инфракрасному каналу связи. Наиболее распространен ИК-зонд IRP-700 (REI, США), подключаемый к прибору СРМ-700. При обнаружении ЗУ в головных телефонах прослушивается известный звуковой сигнал, который усиливается при ориентировке ИК-зонда на закладочное устройство.

Перечень специальных методов обнаружения закладочных устройств не исчерпывается описанными в данной статье. Кроме того, специалистами разрабатываются новые методы поиска, появляются новые более совершенные поисковые приборы.

УДК 621.3

О.В. Рыбальский, В.И. Соловьёв, В.В. Журавель

НОВОЕ СПЕЦИАЛИЗИРОВАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «ФРАКТАЛ» ДЛЯ ИДЕНТИФИКАЦИИ ЦИФРОВОЙ АППАРАТУРЫ ЗВУКОЗАПИСИ И ПРОВЕРКИ ОРИГИНАЛЬНОСТИ ЦИФРОВЫХ ФОНОГРАММ

Проверка подлинности и оригинальности фонограмм, проводимая при производстве фоноскопической экспертизы, является одним из аспектов информационной безопасности. В частности, такая проверка относится к защите правоохранительных органов и общественности от дезинформации, которая может быть предоставлена на поддельных фонограммах.

Появление и широкое использование цифровых методов записи требовало создания нового теоретического подхода и разработки инструментария для проведения такой экспертизы. Была разработана теория выявления следов цифровой обработки фонограмм, и на ее основе предложен фрактальный подход к созданию методов и средств экспертизы ЦАЗЗ и цифровых фонограмм.

Следствием этого стало создание нового специализированного программного обеспечения, предназначенного для проверки оригинальности цифровых фонограмм и идентификации цифровой аппаратуры звукозаписи (ЦАЗЗ). При этом следует отметить, что идентификация ЦАЗЗ до появления этого программного продукта не обеспечивалась никакими аппаратными и программными средствами.

Почему мы акцентируем внимание на идентификации аппаратуры записи? Дело в том, что проверка оригинальности фонограммы (казалось бы, диагностическая задача) является, по сути, идентификационной задачей аппаратуры записи. Это объясняется тем, что согласно теории криминалистической идентификации исследуемый объект может быть тождественен лишь самому себе. Поэтому, если идентификационные признаки, вносимые в фонограмму аппаратом записи, одинаковы в исследуемой (спорной) и образцовой (экспериментальной) фонограммах, то, во-первых, мы идентифицируем аппарат записи и, во-вторых, показываем, что обе записи сделаны на одной аппаратуре. А из этого следует вывод, что исследуемая фонограмма является оригиналом.

Программа и методика ее применения в экспертной практике разрабатывались и отрабатывались в течение двух лет при активном участии экспертных учреждений Украины. Наконец, отработанные версии про-

грамм ции в
практ ы.
Та дова-
лась жен-
ный ина-
листи го на
двух ; раз-
ными отой
дискр ю за-
писан , при
разны ым –
сравн зных
аппар атуре
запис ые на
одном точки
зрени двух
одина

Результаты этих исследований (рис. 1–5) свидетельствуют о пригодности программы и методики ее применения для экспертных исследований оригинальности фонограмм и идентификации цифровой аппаратур ровед
денны воз-
можн и без
сглаж

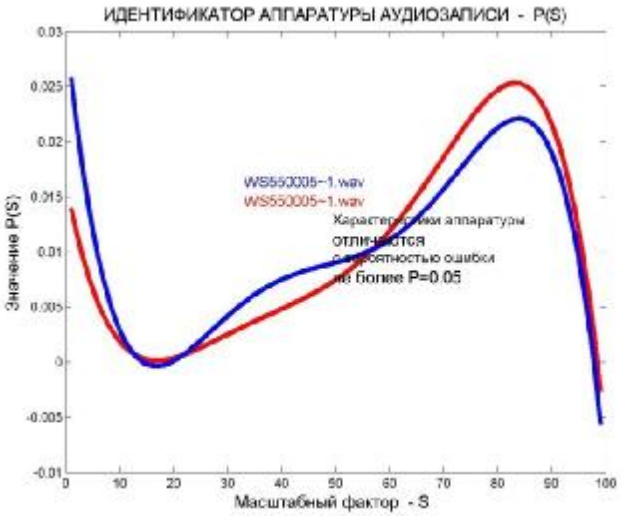


Рис. 1. Сравнение пары записей, сделанных на двух разных цифровых аппаратах с применением сглаживания кривых, представляющих результаты исследования

Рис. 2. Сравнение пары записей, сделанных на одном цифровом аппарате при представлении кривых без сглаживания

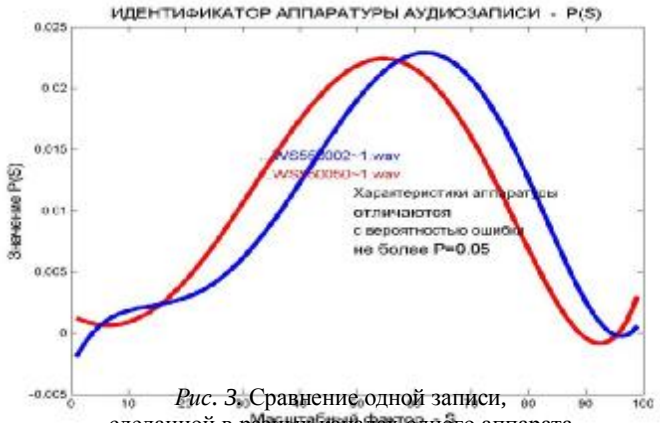


Рис. 3. Сравнение одной записи, сделанной в разных каналах одного аппарата

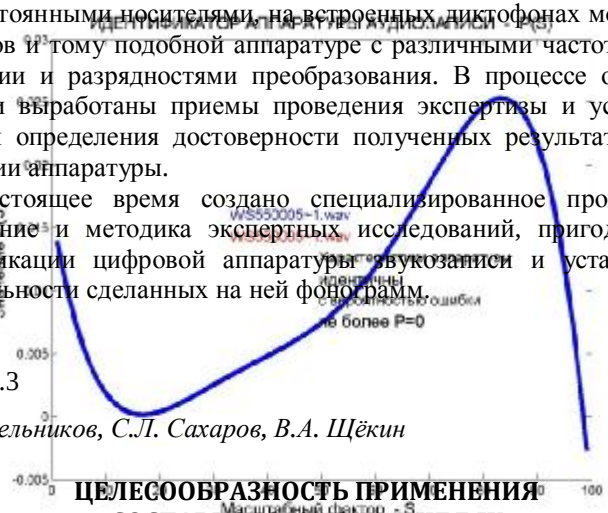
Рис. 4. Сравнение одной записи, сделанной в одном канале на одном аппарате как два разных файла

Рис. 5. Сравнение двух разных записей, сделанных на одном аппарате

Следует добавить, что отработка программы и методики проводилась на различных типах ЦАЗЗ, в том числе на диктофонах со сменны-

ми и постоянными носителями, на встроенных диктофонах мобильных телефонов и тому подобной аппаратуре с различными частотами дискретизации и разрядностями преобразования. В процессе отработки методики выработаны приемы проведения экспертизы и установлен критерий определения достоверности полученных результатов идентификации аппаратуры.

В настоящее время создано специализированное программное обеспечение и методика экспертных исследований, пригодные для идентификации цифровой аппаратуры звукозаписи и установления оригинальности сделанных на ней фонограмм.

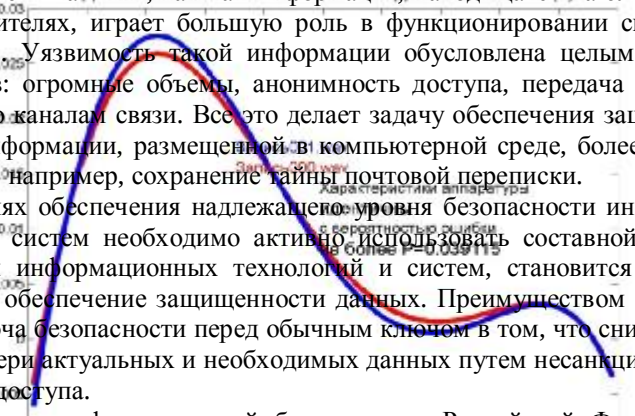


УДК 681.3

П.А. Сидельников, С.Л. Сахаров, В.А. Щёкин

ЦЕЛЕСООБРАЗНОСТЬ ПРИМЕНЕНИЯ СОСТАВНОГО КЛЮЧА В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Вопрос безопасности информации в информационных системах является очень важным, так как информация, находящаяся на электронных носителях, играет большую роль в функционировании силовых ведомств. Уязвимость такой информации обусловлена целым рядом факторов: огромные объемы, анонимность доступа, передача информации по каналам связи. Все это делает задачу обеспечения защищенности информации, размещенной в компьютерной среде, более сложной, чем, например, сохранение тайны почтовой переписки.



В целях обеспечения надлежащего уровня безопасности информационных систем необходимо активно использовать составной ключ. С ростом информационных технологий и систем, становится обязательным обеспечение защищенности данных. Преимуществом составного ключа безопасности перед обычным ключом в том, что снижается риск потери актуальных и необходимых данных путем несанкционированного доступа.

Доктрина информационной безопасности Российской Федерации определяет информационную безопасность как состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз.

Для решения проблем информационной безопасности необходима защита: находящейся в системе информации от дестабилизирующего

воздействия внешних и внутренних угроз информации; элементов системы от дестабилизирующего воздействия внешних и внутренних информационных угроз; внешней среды от информационных угроз со стороны рассматриваемой системы.

Необходимость использования составного пароля обусловливается в первую очередь тем, что технологии вскрытия паролей не стоят на месте. Сейчас опытному взломщику на вскрытие пароля из 8 или даже 10 символов требуется совсем немного времени. Взлом осуществляется одним из принципиальных способов: подбор пароля перебором, подбор пароля по словарю, фишинг, заражение компьютера вирусом «Троянский конь».

В первом способе пароль подбирается, проверяются все возможные комбинации. Рано или поздно одна из них по законам комбинаторики (учитывая, что скорость перебора составляет 100 000 паролей за одну секунду) найденная комбинация неизбежно совпадет с вашей. Время, необходимое взломщику для вскрытия вашего пароля, показано в таблице.

Количество знаков	Количество вариантов	Время перебора
1	36	менее 1 с
2	1 296	менее 1 с
3	46 656	менее 1 с
4	1 679 616	17 с
5	60 466 176	10 мин
6	2 176 782 336	6 ч
7	78 364 164 096	9 дней
8	2,821 109 910 12	11 мес.
9	1,015 599 510 14	32 г.
10	3,656 158 410 15	1 162 г.
11	1,316 217 010 17	41 823 г.
12	4,738 381 310 18	1 505 615 лет

Таким образом, для надежной защиты пароля от вскрытия таким способом нужно, чтобы его длина была минимум 8 символов. При создании пароля в 22 символа подбор будет нерентабелен.

Во втором же случае берется обычный словарь, дополненный некими частыми комбинациями цифр, вроде дат или просто красивых комбинаций символов и цифр (qwe или 123). Теперь собираем из них разные комбинации и проверяем. Именно по такому способу пароли типа «qwe123» вскрываются за доли секунды. Исходя из этого, нужно сделать пароль, в котором в явном виде целых слов не будет.

В третьем случае пользователю на почтовый ящик приходит письмо, в котором пользователю предлагают, перейдя по предоставленной ссылке, в целях обеспечения безопасности сменить на сайте свой пароль. На самом деле, такая ссылка ведет на сайт хакера со страницей, которая очень похожа на страницу необходимого сайта, и при попытке смены своего пароля он будет отправлен взломщику.

При заражении компьютера вирусом «Троянский конь» взломщик получает доступ к данным в зависимости от того, какую он поставил перед собой задачу. В свою очередь, пользовательские пароли не являются исключениями.

Исходя из этого, нам необходимо задуматься о составном пароле как о более надежном средстве обеспечения информационной безопасности.

При создании пароля необходимо чтобы пользовательский пароль был не менее чем из восьми символов, причем, чтобы в пароле в произвольном порядке были написаны буквы латиницей в разных регистрах, пароль содержал цифры и специальные символы. Если пароль создается для учетной записи, которая будет выполнять вход на сервер, то желательно создавать пароли, длина которых будет превышать 12 символов. Таким образом, можно обобщить рекомендации по созданию составных паролей в правила разработки составных ключей с целью обеспечения информационной безопасности.

1. Необходимо избегать коротких паролей. Сегодня практически все интернет-ресурсы сами не допускают регистрации, если пользователь ввел небезопасный пароль. Пароль не должен быть менее 8 символов, а лучше, чтобы и вовсе состоял из 10–12 знаков.

2. Обязательно, чтобы пароль состоял из букв и из цифр. Не стоит использовать повторяющиеся буквы и цифры. Можно использовать также знаки препинания или другие символы.

3. С помощью клавиши Shift можно сделать некоторые буквы пароля в верхнем регистре – это усилит его надежность.

4. Не стоит назначать пароль, внося туда личные данные или данные близких – имена, фамилии, даты рождения, прочие знаменательные даты.

5. Бессмысленность и нелогичность пароля – залог его надежности. Не стоит использовать слова, которые можно с легкостью отыскать в любом словаре, на любом языке.

6. При регистрации секретные вопросы для восстановления паролей необходимо составлять очень скрупулезно, чтобы нельзя было подобрать к ним ответ, опираясь на данные в социальных профилях или шаблонное мышление. Секретный вопрос должен быть оригинальным, в то же время вы сами должны будете вспомнить на него ответ.

Придерживаясь этих правил, каждый пользователь обеспечит безопасность своего компьютера и ценных данных, находящихся на нем. Однако кроме создания составного пароля нам необходимо задуматься еще и о его хранении. Сохранность пароля является важным вопросом в информационной безопасности, без решения этого вопроса даже сложный созданный нами пароль не станет помехой для взломщика. Как правило, пользователи хранят логины и пароли на своих компьютерах, планшетах или мобильных устройствах в отдельных текстовых файлах. Именно на такие файлы и охотятся программы-шпионы. Поэтому для хранения паролей необходимо либо использовать специальные программы – менеджеры хранения паролей, в которых применяется шифрование данных, либо грамотно оформлять текстовые файлы с паролями. Не стоит называть эти файлы именами, которые прямым текстом заявляют о своем назначении. Названия лучше подбирать неприметные, совершенно на иную тематику. Необходимо создать пароль к самому текстовому файлу, где хранятся пароли, но держать этот пароль уже придется в голове.

Таким образом, использование коротких и легких паролей недопустимо, чтобы обеспечить сохранность данных от взлома и хищения необходимо использовать составные пароли.

Из всего вышеперечисленного следует, что обеспечение информационной безопасности является комплексной задачей. Это обусловлено тем, что информационная среда является сложным многоплановым механизмом, в котором действуют многие компоненты. Для решения проблемы обеспечения информационной безопасности необходимо применение законодательных, организационных и программно-технических мер. Пренебрежение хотя бы одним из аспектов этой проблемы может привести к утрате или утечке информации, стоимость и роль которой в жизни современного общества приобретает все более важное значение.

УДК 004.056.53

А.В. Федорченко, А.А. Чечулин, И.В. Котенко

ИНТЕГРИРОВАННАЯ БАЗА ДАННЫХ УЯЗВИМОСТЕЙ

Одним из способов повышения защищенности компьютерных сетей является постоянное отслеживание используемых программно-аппаратных средств на наличие в них уязвимостей, нарушающих безопасность компьютерных систем. На данный момент существует ряд организаций, занимающихся мониторингом, классификацией и накоплением данных об уязвимостях. Данные организации предоставляют открытый доступ к своим базам уязвимостей, однако каждая такая база заполняется независимо от других и, что более важно, имеет свой формат представления данных.

Одной из областей применения баз уязвимостей являются системы оценки защищенности компьютерных сетей. Списки уязвимостей в этих системах используются как один из основных источников информации для оценки защищенности, так как описания уязвимостей содержат как предусловия, так и оценки, характеризующие результат атак, эксплуатирующих эти уязвимости, а также списки конкретных программно-аппаратных продуктов, содержащих данные уязвимости.

Предполагается, что объединение открытых баз данных уязвимостей приведет к увеличению количества уникальных записей об этих уязвимостях и расширению списка продуктов, в которых они могут иметь успешную реализацию, что позволит повысить вероятность обнаружения уязвимых программно-аппаратных средств, используемых в анализируемых компьютерных сетях, и, как следствие, повысит точность оценки защищенности этих сетей. Кроме того, использование структуры базы данных, оптимизированной для быстрого поиска уязвимостей, позволит применять ее в системах оценки защищенности компьютерных сетей, работающих на этапе эксплуатации, т. е. проводящих анализ безопасности сети в режиме, близком к реальному.

Основными задачами, решаемыми в данной работе, является создание модели процесса формирования интегрированной базы данных уязвимостей для повышения точности оценки защищенности компьютерных сетей; разработка реляционной модели формируемой базы для обеспечения необходимой оперативности при работе в составе системы оценки защищенности компьютерных сетей. Основным отличием разрабатываемой интегрированной базы данных уязвимостей является ее направленность на оперативное получение результатов поиска подходящих уязвимостей для программно-аппаратных конфигураций и совмещение в одной базе информации из разнородных открытых источников описаний уязвимостей.

В настоящее время базы данных уязвимостей широко применяются при решении задач обеспечения безопасности компьютерных систем. Они используются в сканерах уязвимостей, сканерах безопасности, системах обнаружения и предотвращения атак и т. д. Основной проблемой существующих баз является низкая скорость формирования результата поиска уязвимого программно-аппаратного обеспечения. Задача формирования такого результата усложняется сложной зависимостью между элементами программно-аппаратного обеспечения, необходимыми для реализации некоторой уязвимости. Учитывая тот факт, что базы данных уязвимостей наполняются преимущественно отдельно друг от друга, имеют различные форматы описания уязвимостей и продуктов и не используют единой методики поиска уязвимостей, их применение в системе оценки защищенности компьютерных сетей затруднено.

Для полноценного применения разрабатываемой интегрированной базы данных уязвимостей в системе оценки защищенности компьютерных сетей она должна содержать в себе: список уязвимостей; список продуктов; показатели, характеризующие уязвимости. В связи с тем, что данные в базу добавляются из разных источников, множество записей уязвимостей были помещены в интегрированный список уязвимостей, а записи продуктов – в интегрированный словарь продуктов.

Процесс интеграции уязвимостей был разделен на два этапа: установление соответствия по прямым ссылкам (идентификаторам) на уязвимости объединяемых баз; установление соответствия по ссылкам на неиспользуемые источники (например, другие базы данных уязвимостей) с условием, что данные ссылки являются уникальными для всех объединяемых баз.

Стоит отметить, что если идентификаторы в пределах одной базы ссылались на собственные записи уязвимостей, то такие уязвимости объединялись в одну запись интегрированного списка уязвимостей.

Процесс формирования интегрированного словаря продуктов заключается в объединении записей продуктов используемых баз данных уязвимостей с исключением дублирования. Однако на начальном этапе, данный словарь составляется путем добавления записей Общего перечисления платформ (Common Platform Enumeration, CPE). CPE – это структурированная схема именования для компьютерных систем и платформ, основанная на синтаксисе Универсальных идентификаторов ресурсов (Uniform Resource Identifiers, URI). Такое решение было принято в связи с тем, что данный словарь содержит большое количество записей продуктов, а реализация его записей имеет наилучшую на сегодня форму представления продуктов.

Несмотря на то, что в качестве основы для заполнения интегрированного словаря продуктов был использован словарь CPE, формат самих записей был изменен и приобрел следующий вид:

{тип}:{производитель}:{продукт}:{версия}:{модификация}:{редакция}.

Также следует отметить, что в качестве показателей, характеризующих уязвимости, выла выбрана Общая система оценки уязвимостей (Common Vulnerability Scoring System, CVSS), которая является одной из наиболее востребованных, по мнению экспертов.

Проектирование структуры интегрированной базы данных уязвимостей производилось по разработанной модели процесса формирования. Конечные данные были распределены по следующим реляционным таблицам: (1) производители; (2) продукты, (3) параметры продуктов (включает поля «тип», «версия», «модификация», «редакция»); (4) уязвимости и (5) уязвимые конфигурации (включает внешние ключи записей таблиц 4 и 3, а также поле «параметр зависимости»).

Параметр зависимости в реляционной таблице (5) является единственным признаком, определяющим связь между уязвимым программно-аппаратным обеспечением и продуктами, при которой данная зависимость может быть реализована. Таким образом, если указанный в качестве ключа продукт имеет уязвимость без такой зависимости, то поле «параметр зависимости» этой записи будет иметь значение 0. Если же данная уязвимость для данного продукта реализуется только в случае наличия другого продукта, то такая зависимость будет описана следующим образом:

пусть группа продуктов, имеющих положительную реализацию уязвимости в зависимости от наличия в системе любого из продуктов другой группы, является группой «A»;

тогда группа продуктов, влияющих на положительную реализацию уязвимости продуктов группы «A», является группой «B»;

значение поля «параметр зависимости» записи таблицы связывания для продуктов группы «A» будет нечетным, начиная со значения 1;

значение поля «параметр зависимости» записи таблицы связывания для продуктов группы «B» будет четным, начиная со значения 2.

В таблице уязвимостей поле «флаг зависимости» в случае наличия у данной записи уязвимости продуктов с зависимостями принимает значение 1, иначе – 0. Поле «дополнительная информация» включает в себя идентификаторы уязвимостей из оригинальных баз, а также текстовое описание, дату обнаружения, возможное решение, для преодоления уязвимости.

Описанная структура позволяет с помощью одного SQL-запроса к интегрированной базе данных уязвимостей осуществлять поиск уязви-

мостей, присущих некоторому комплексу программно-аппаратных продуктов (т. е. списку установленного программно-аппаратного обеспечения на отдельном хосте исследуемой сети).

В качестве практической реализации был разработан прототип интегрированной базы данных уязвимостей, для формирования которой были использованы следующие источники описания уязвимостей и продуктов: база CVE; база NVD; база OSVDB; словарь CPE.

В результате формирования интегрированной базы данных общее число уникальных записей уязвимостей по сравнению с используемыми источниками увеличилось, по меньшей мере, на 30 %, а количество записей интегрированного словаря продуктов – на 110 %. Представленный прототип интегрированной базы данных был использован как базовый компонент для построения автоматизированной системы моделирования атак и анализа защищенности компьютерных сетей.

Для проверки эффективности функционирования интегрированной базы данных была проведена серия экспериментов для моделирования различных сценариев атак.

В перспективе планируется дальнейшая разработка и модификация интегрированной базы данных уязвимостей за счет увеличения числа используемых открытых баз данных уязвимостей, присвоение источникам ссылок показателей доверия и расширенного анализа уникальности уязвимостей для обеспечения наиболее качественной интеграции. Для интегрированного словаря продуктов предполагается в качестве основы использовать также словарь CPE версии 2.3. Планируется разработка функции обновления для исключения необходимости полного переформирования интегрированной базы данных уязвимостей с течением времени, что повысит оперативность формирования базы.

УДК 004.056

А.А. Чечулин

АНАЛИЗ И КЛАССИФИКАЦИЯ ВОЗМОЖНЫХ ИЗМЕНЕНИЙ, ПРОИСХОДЯЩИХ В КОМПЬЮТЕРНОЙ СЕТИ, ИХ ВЛИЯНИЕ НА ДЕРЕВЬЯ АТАК

Защита информации в компьютерных сетях является важной задачей, решением которой занимаются многие научные и коммерческие коллективы. Для повышения уровня защиты необходимо не только

обнаруживать вредоносную активность, но и постоянно отслеживать как состояние различных средств защиты, так и изменения в архитектуре и составе защищаемой сети.

Одним из наиболее эффективных подходов к оценке защищенности является подход, основанный на моделировании атак, позволяющий учесть не только уязвимости, содержащиеся в отдельных хостах компьютерной сети, но и возможные последовательности действий нарушителя, которые могут привести к большему ущербу, нежели использование отдельных уязвимостей. Одним из представлений, описывающим возможные действия атакующего, являются деревья атак. Узлы дерева атак могут быть представлены как возможные атакующие действия, связанные между собой в соответствии с тем, в каком порядке их может выполнять нарушитель. Однако точность и адекватность построенного дерева атак полностью зависит от полноты исходных данных, т. е. модели исходной компьютерной сети.

В процессе эксплуатации компьютерная сеть представляет собой постоянно изменяющийся объект, т. е. ее структура и отдельные элементы (например, хосты) могут меняться со временем. Модель компьютерной сети и, как следствие, модели атак и результаты их оценки также должны изменяться в соответствии с изменениями в реальной сети. Особенностью этого процесса является то, что в большинстве существующих систем моделирования атак для его выполнения может потребоваться время и ресурсы, сравнимые с этапом проектирования сети, что приводит к невозможности использования моделирования.

Для повышения эффективности процесса обновления моделей в настоящей работе предлагается разработанная оригинальная классификация возможных изменений компьютерной сети, влияющих на общую защищенность. Данная классификация содержит следующие элементы: изменение топологии (добавление/удаление связей между хостами); изменение состава (добавление/изменение/удаление) хостов; изменение параметров (добавление/удаление) системы безопасности; добавление/изменение/удаление уязвимостей.

Для каждого типа изменения разработана схема, позволяющая минимизировать время, необходимое на обновление модели. Благодаря такому подходу удалось значительно снизить время, необходимое на модификацию исходных данных в соответствии с изменениями в реальной сети.

В рамках алгоритма модификации выделяются три класса изменений, сгруппированные по воздействию на дерево атак: (1) не влияющие

на дерево атак (например, изменения приводящие к появлению таких уязвимостей на хосте, что нарушитель не получает никаких новых возможностей по сравнению с теми, которыми он обладал до этого); (2) уменьшающие дерево атак (например, удаление элементов программно-аппаратной конфигурации одного из хостов или удаление связей); (3) расширяющие дерева атак (например, появление новых уязвимостей). Аналогично изменения группируются по влиянию на доступные нарушителю атакующие действия.

Рассмотрим возможные изменения более подробно.

1. Изменение топологии в части добавления новых связи в модель компьютерной сети. При этом выполняются следующие действия:

а) поиск хостов из дерева атак, участвующего в добавленной связи;

б) добавление в дерево атак новых хостов и связей.

2. Изменение топологии (удаление связи). При обработке данного изменения задействован только блок (3). При этом выполняются следующие действия:

а) удаление из дерева атак хостов, соединенных удаленной связью;

б) удаление части дерева, не связанной с корнем.

3. Изменение состава (добавление/удаление) хостов. При этом выполняются следующие действия:

а) добавление/удаление возможных атакующих действий и доступных нарушителям атакующих действий AAM для данного хоста;

б) в случае удаления хоста – удаление всех связей, в которых он был задействован (см. п. 2 алгоритма модификации);

в) добавление/удаление возможных переходов нарушителей между хостами в дерево атак.

4. Изменение программно-аппаратной конфигурации хоста или параметров системы безопасности, связанных с одним хостом. При этом выполняются следующие действия:

а) добавление/удаление возможных атакующих действий и доступных нарушителям атакующих действий для данного хоста;

б) добавление/удаление возможных переходов нарушителей между хостами в участках дерева атак, где был задействован изменяемый хост.

Изменение программно-аппаратной конфигурации хоста и/или параметров его системы безопасности приводит к появлению или удалению списков уязвимостей, присущих этому хосту и доступных нарушителям В том случае если изменение списка доступных уязвимостей не влияет на потенциальные возможности одной или нескольких моделей нарушителя, то для этих моделей модификация дерева не требуется.

5) Добавление/изменение/удаление. При этом выполняются действия, аналогичные изменению конфигурации хостов, где в качестве измененных выступают хосты, программно-аппаратная конфигурация которых допускает использование измененной уязвимости. В случае если изменение списка доступных уязвимостей не влияет на потенциальные возможности одной или нескольких моделей нарушителя, то для этих моделей модификация дерева не требуется.

Классификация возможных изменений в компьютерной сети и алгоритм обновления деревьев атак, предложенные в данном исследовании, отличаются от существующих аналогов направленностью на оперативное получение результата. Алгоритм обновления деревьев атак учитывает классификацию возможных изменений в моделях, что позволяет оперативно приводить модели атак в соответствие с изменениями или событиями, происходящими в реальной сети, за счет модификации только тех элементов деревьев атак, которые соответствуют измененным элементам компьютерной сети.

Работа выполняется при финансовой поддержке РФФИ (13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417), программы фундаментальных исследований ОНИТ РАН (контракт № 2.2) и проекта ENGENSEC программы Европейского сообщества TEMPUS.

РАЗДЕЛ 3

СОВРЕМЕННЫЕ ПРОБЛЕМЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 002:004.056

В.В. Бондуровский, Г.И. Перекопский

ПАРЛАМЕНТСКОЕ ИЗМЕРЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ СНГ И ОДКБ НА СОВРЕМЕННОМ ЭТАПЕ

Секретариаты Совета Межпарламентской ассамблеи государств – участников СНГ, Парламентской ассамблеи Организации Договора о коллективной безопасности, а также Координационный совет Международного союза юристов и профильных органов СНГ осуществляют сотрудничество высших законодательных органов государств СНГ и ОДКБ. В течение многих лет они обеспечивают разработку региональных стандартов регулирования отношений в информационной сфере и в обеспечении ее безопасности, что отразилось на становлении информационных национальных законодательств.

В то же время оказалось, что всего того, что было сделано в последние два десятилетия, недостаточно для системного и адекватного парирования существующих вызовов и угроз в стремительно развивающейся информационной сфере.

Несмотря на то что в СНГ и ОДКБ и до этого принимались межгосударственные документы, имеющие важнейшее значение для обеспечения информационной безопасности, следует признать, что в них отсутствовала инструментальная конкретика.

В результате мы запоздали с адекватным реагированием. Стало понятным, что в сложившейся ситуации необходимо что-то срочно делать.

Предпринятый в инициативном порядке нашими экспертами анализ ситуации с целью разрешения этого вопроса показал, что именно в данной области назрела масса проблем, на решение которых необходимо нацелить наши государства, но главное – успешно решить их в самые короткие сроки. В число этих экспертов вошли белорусские и российские ученые-практики.

В соответствии с Комплексным планом мероприятий по реализации Концепции сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности на период с 2008 по 2010 годы был определен круг конкретных мер для решения в первоочередном порядке.

Прежде всего подготовлен проект Рекомендаций по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности. В работе участвовали специалисты Института государства и права РАН, Санкт-Петербургского института информатики и автоматизации РАН, Института национальной безопасности и Академии МВД Республики Беларусь. Подходы к разработке этого концептуального по своему значению документа публиковались для широкого обсуждения на страницах ряда авторитетных периодических изданий. В 2012 г. работа над документом была успешно завершена.

Этот документ определил комплекс законодательных инициатив, отраженных в межгосударственных программах сотрудничества государств-участников в сфере безопасности на периоды 2014–2018 гг., которые 25 октября 2013 г. утвердил Совет глав государств СНГ.

С учетом того, что актуальность защиты секретов (и не только государственных) сегодня возрастает, немногим ранее в соответствии с решениями Совета коллективной безопасности ОДКБ были подготовлены Рекомендации по сближению и гармонизации законодательства государств – членов ОДКБ по защите государственных секретов и Глоссарий основных понятий в законодательстве о государственной тайне государств – членов ОДКБ.

В 2013 году, помимо этого, тем же научным коллективом полностью завершена подготовка еще одного специального в данной области документа – Рекомендаций по правовому регулированию эксплуатации открытых телекоммуникационных сетей для предупреждения их использования в террористических и иных противоправных целях. Подготовлен и ряд других нормативных правовых актов.

В соответствии с идеями и решениями, получившими статус межгосударственных, уже в текущем году разработаны проекты Стратегии обеспечения информационной безопасности государств – участников СНГ, модельного регламента административных процедур, осуществляемых уполномоченными органами в сфере обеспечения информационной безопасности государств – участников СНГ, модельный закон «О критически важных объектах информационно-коммуникационной инфраструктуры», изменений в модельный закон «Об информации, информатизации и защите информации». В ближайшее время указанные проекты пройдут комплексную экспертизу в государствах-участниках. В 2015–2016 гг. предстоит подготовить проекты измене-

ний и дополнений в модельный Уголовный кодекс для государств – участников СНГ по вопросам борьбы с преступлениями в информационной сфере, Комментария к модельному закону «О государственных секретах» и изменений к нему, модельного закона «О критически важных объектах информатизации»).

По самим названиям перечисленных документов можно судить о их новизне, их реализация в национальных правовых системах государств-участников будет служить добротным подспорьем в нормативно-правовом противодействии вызовам и угрозам информационной безопасности государств СНГ и ОДКБ.

Многое было сделано для того, чтобы соответствующие законодательные инициативы обрели политическую волю и стали межгосударственными решениями.

УДК 002:004.056

Г.В. Вусс

ДЕЯТЕЛЬНОСТЬ БАЗОВОЙ ОРГАНИЗАЦИИ ГОСУДАРСТВ – УЧАСТНИКОВ СНГ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Важнейшими основополагающими документами, определяющими сотрудничество государств – участников СНГ в области информационной безопасности, являются Концепция сотрудничества государств – участников Содружества Независимых Государств в сфере обеспечения информационной безопасности (далее – Концепция) и Комплексный план мероприятий по реализации Концепции сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности на период с 2008 по 2010 год (далее – Комплексный план). Данные документы были утверждены Советом глав государств СНГ 10 октября 2008 г.

Указанная Концепция представляет собой согласованную государствами – участниками СНГ совокупность официальных взглядов и положений о целях, принципах и основных направлениях межгосударственного сотрудничества в сфере обеспечения информационной безопасности.

Одним из мероприятий Комплексного плана было определение базовой организации государств – участников СНГ по методическому и организационно-техническому обеспечению работ в области информационной безопасности и подготовке специалистов в этой сфере (далее – Базовая организация).

Решением Совета глав правительств СНГ от 30 мая 2014 г. статус Базовой организации был придан ФГУП ВНИИПВТИ. Одновременно было утверждено Положение о базовой организации государств – участников Содружества Независимых Государств по подготовке, переподготовке и повышению квалификации руководящего состава для органов внутренних дел (полиции) (далее – Положение о Базовой организации).

На ФГУП ВНИИПВТИ возложены задачи по организационному и научно-методологическому обеспечению органов государственной (исполнительной) власти, осуществляющих функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий и информационной безопасности в государствах – участниках СНГ, а также учебно-методическому и кадровому обеспечению переподготовки и повышения квалификации специалистов в сфере информационной безопасности в государствах – участниках Содружества.

Согласно Положению о Базовой организации деятельность осуществляется в соответствии с ежегодным планом работ. План работы Базовой организации на 2013 г. утвержден совместным решением 47-го Совета глав АС РСС и 18-го Координационного совета государств – участников СНГ по информатизации при РСС от 5 ноября 2012 г.

Финансовое обеспечение направлений деятельности Базовой организации осуществляется из средств, формируемых в основном за счет оплаты заказчиками работ, выполняемых по договорам и контрактам, оплаты экспертиз и консультаций, а также оплаты целевой переподготовки и повышения квалификации кадров.

В марте 2013 г. институт стал победителем конкурсов, проводимых Региональным содружеством в области связи по темам: «Проведение анализа состояния выполнения национальных программ информатизации, проектов построения информационного общества и развития ИКТ, включая вопросы обеспечения информационной безопасности» (НИР) и «Создание пилотного проекта системы защищенного трансграничного юридически значимого информационного обмена в рамках СНГ» (НИОКР).

Тематика работ, определенных в технических заданиях на НИР и НИОКР, соответствовала задачам и направлениям деятельности Базовой организации.

В результате выполнения Плана работы Базовой организации на 2013 г. и требований технических заданий на НИР и НИОКР разработаны следующие документы:

проект доклада Совету глав правительств СНГ о выполненных мероприятиях Стратегии сотрудничества государств – участников СНГ в

построении и развитии информационного общества и плана действий по ее реализации на период до 2015 года;

предложения по совершенствованию сотрудничества государств – участников СНГ в области ИКТ;

аналитическая справка о состоянии выполнения национальных программ информатизации, проектов построения информационного общества и развития ИКТ в государствах – участниках СНГ, включая вопросы обеспечения информационной безопасности;

справка о состоянии развития нормативно-правовой базы государств – участников СНГ в области ИКТ;

предложения по исключению дублирования решаемых проблем в рамках национальных программ информатизации, проектов построения информационного общества и развития ИКТ в государствах – участниках СНГ, включая вопросы обеспечения информационной безопасности;

проект Плана совместных мероприятий по продвижению позиции государств – участников СНГ на международных форумах по вопросам интернационализации управления интернетом;

отчет об исследованиях в области формирования организационно-координирующей структуры для обеспечения создания трансграничного пространства доверия на основе сети Интернет в государствах – участниках СНГ (далее – ПД-Т) и в других международных форматах (Евразийская экономическая комиссия);

предложения по практической реализации модели ПД-Т и методологии ПД-Т.

В части подготовки предложений по гармонизации и унификации нормативно-правовой базы в области ИКТ и информационной безопасности со стороны института были выдвинуты предложения о разработке проектов модельных законов «Об электронном правительстве» и «О трансграничном информационном обмене электронными документами».

Данные предложения вошли в Перспективный план модельного законотворчества в СНГ на 2011–2015 годы (постановление Совета Межпарламентской ассамблеи государств – участников Содружества Независимых Государств от 27 марта 2012 г. № 6).

Секретариатом Совета МПА СНГ были проведены открытые конкурсы на право заключения договоров по разработке проектов модельных законов «Об электронном правительстве» и «О трансграничном информационном обмене электронными документами».

По результатам открытых конкурсов 17 января 2014 г. Комиссия по размещению заказов для нужд Секретариата Совета МПА СНГ приняла решение заключить договора с ФГУП ВНИИПВТИ на разработку

проектов модельных законов «Об электронном правительстве» и «О трансграничном информационном обмене электронными документами». Срок выполнения работ 2014–2016 гг.

На заседание Постоянной комиссии МПА СНГ по культуре, информации, туризму и спорту были одобрены в основном с учетом замечаний и предложений, высказанных на заседании комиссии, представленные ФГУП ВНИИПВТИ проекты концепции модельного закона «Об электронном правительстве» и «О трансграничном информационном обмене электронными документами» (11 марта 2014 г., Санкт-Петербург, Таврический дворец).

На очередном заседании Постоянной комиссии МПА СНГ по культуре, информации, туризму и спорту должны быть представлены проекты модельных законов «Об электронном правительстве» и «О трансграничном информационном обмене электронными документами».

В мае 2013 г. был сформирован Общественный совет Базовой организации, в состав которого вошли представители шесть государств – участников СНГ (Республика Армения, Республика Беларусь, Республика Казахстан, Кыргызская Республика, Республика Молдова, Российская Федерация) и Исполкома РСС.

На первом организационном заседании Общественного совета Базовой организации 16 мая 2013 г. были утверждены положение, регламент и план работы Общественного совета со 2-го квартала 2013 г. по 2-й квартал 2014 г.

На 2-м заседании Общественного совета Базовой организации 30 мая 2014 г. выработаны предложения и утвержден план работы, мероприятия которого направлены на объединение усилий специалистов стран Содружества в вопросах обеспечения информационной безопасности.

В целях предоставления оперативной информации о деятельности Базовой организации и ее Общественного совета на сайте ФГУП ВНИИПВТИ ведется соответствующий раздел.

В настоящий период деятельность Базовой организации осуществляется в соответствии с планом работы на 2014 г., в который включено мероприятие по содействию реализации Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности, подписанного в Санкт-Петербурге 20 ноября 2013 г.

УДК 002:004.056

М.А. Вус

ПОНЯТИЙНЫЙ АППАРАТ СФЕРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В НОРМАТИВНО-ПРАВОВОЙ БАЗЕ ОДКБ

Организация Договора о коллективной безопасности (ОДКБ) – международная организация военно-технического сотрудничества, созданная на постсоветском пространстве, объединяет в настоящее время шесть независимых государств: Республику Армения, Республику Беларусь, Республику Казахстан, Кыргызскую Республику, Российскую Федерацию и Республику Таджикистан. ОДКБ позиционирует себя как многофункциональная структура противодействия традиционным и новым вызовам и угрозам миру, безопасности и стабильности. Диапазон таких вызовов в последнее время не только не сужается, а, напротив, расширяется. Учитывая это обстоятельство, Президент Российской Федерации В.В. Путин особо подчеркнул, что «совместно с нашими союзниками мы должны укреплять возможности Организации Договора о коллективной безопасности».

В качестве одного из основных направлений создания системы коллективной безопасности государства – члены ОДКБ рассматривают сближение основных положений законодательных актов в области обороны и безопасности. Парламентская ассамблея ОДКБ (ПА ОДКБ), являющаяся органом межпарламентского сотрудничества государств – членов этой организации, обсуждает вопросы межгосударственного сотрудничества, принимает рекомендации по сближению законодательства этих государств в международной, военно-политической, правовой и иных областях. В области юрисдикции государств – членов ОДКБ как во внутригосударственной сфере, так и в международном пространстве большую роль играет выбор конкретных значений применяемых терминов и понятий, их легитимное толкование и применение в различных договорах, соглашениях и иных актах, прежде всего в актах, имеющих политическое, экономическое и юридическое значение.

Согласованная политика требует определенности и однозначности понятийного аппарата, который обусловлен характером регулируемых отношений в разных отраслях законодательства. Активно развивающаяся информационная сфера изобилуют специальными терминами. Юридические определения специальных терминов должны играть решающую роль при толковании норм законов и в правоприменительной практике, ибо «размытие» закрепленного законом толкования термина

чревато возникновением юридических конфликтов. Для информационной сферы это особенно актуально.

За два десятилетия существования СНГ на постсоветском пространстве разработано и принято большое число нормативных правовых актов, однако для большинства этих актов сегодня характерны терминологическое многообразие и слабая определенность используемого понятийного аппарата. Это относится и к массиву понятий и дефиниций, обслуживающих сферу информатики и информационной безопасности, который начал формироваться сравнительно недавно. В этой связи необходима определенность и унификация в нормативно-правовой базе государств – членов ОДКБ, прежде всего базовых терминов и понятий, используемых в процессе нормативно-правового регулирования и сотрудничества в области обеспечения информационной безопасности, а также их единообразная трактовка.

Последние десятилетия происходит становление теории информационной безопасности. Глобализация информационных процессов повлекла за собой возникновение целого спектра проблем безопасности. Уже сегодня само понятие «информационная безопасность» превратилось из узкотехнического в понятие общечеловеческого оборота. Информационная сфера – весьма чувствительный фактор жизнедеятельности общества, увеличивается число техногенных факторов, повышается связанная с этим уязвимость. Возрастание роли и значения информационной безопасности требует детальной проработки и углубленных исследований проблем ее обеспечения. Актуальными направлениями исследований при этом является как теоретическое осмысление содержания информационной безопасности, ее предмета, методов, так и формирование понятийно-категориального аппарата.

Коллективом специалистов СПИИРАН и ФСТЭК России был проведен анализ понятийного аппарата международных договоров и информационного законодательства государств – членов ОДКБ и предпринята попытка разработки словаря-справочника по информационной безопасности для рабочих органов ПА ОДКБ. Сложность задачи заключалась в необходимости сформировать фактически универсальную лексическую систему, включающую при всем многообразии лексики тематической группы «информационная безопасность» совокупность самых необходимых легитимных терминов, чтобы сделать этот документ удобным для практического использования.

Опираясь на трактовку системного подхода применительно к задаче формирования и структурирования понятийного аппарата, опубликованную ранее в журнале «Информатизация и связь» [1], представилось возможным сформировать русскоязычный словарь-справочник, включающий 163 группы терминов и легальных трактовок понятий, отно-

сящихся к сфере информационной безопасности. Выборка включает набор основных категорий, которые предлагается рассматривать как базовые для сферы информационной безопасности. В этот набор входят относящиеся к сфере информационной безопасности лексических единицы, получившие юридическое толкование и закрепление в международных и национальных правовых актах государств – членов ОДКБ, с указанием первоисточников.

Словарный материал представлен в табличной форме. Сформированная выборка понятийного аппарата не претендует на полноту, но может послужить ориентиром в правотворческой деятельности. Материал адресован парламентариям, членам экспертных групп и комиссий, работникам органов СНГ и рабочих органов Межпарламентской ассамблеи СНГ, Парламентской ассамблеи ОДКБ и иных интеграционных объединений государств постсоветского пространства. Представляется, что этот справочный материал окажется полезен в правотворческой и правоприменительной деятельности, а также в научных исследованиях и в учебном процессе [2].

1. Эскиз системного подхода к формированию понятийного аппарата информационной безопасности / М.А. Вус [и др.] // Информатизация и связь. 2012, № 9. С. 7–15.

2. Словарь-справочник по информационной безопасности для Парламентской Ассамблеи ОДКБ / под общ. ред. М.А. Вуса и М.М. Кучерявого. СПБ. : СПИИРАН [и др.], 2014. 96 с.

УДК 343.787.7

В.В. Клюс

АКТУАЛЬНЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ ЭНЕРГОИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УКРАИНЫ

Стратегия национальной безопасности Украины, согласно законодательству Украины, формулирует общие принципы, приоритетные цели, задачи и механизм защиты жизненно важных интересов личности, общества и государства от внутренних и внешних потенциальных и реальных угроз. Следует отметить, что современные угрозы безопасности государства, общества и личности все более концентрируются в духовной сфере. Именно духовная безопасность государства, общества, личности является основной преградой для построения нового глобального мироустройства.

Проанализировав научную литературу о духовной безопасности, мы выделяем ее основные составляющие религиозная безопасность; психологическая безопасность; информационно-психологическая безопасность; энергоинформационная безопасность.

Хотим обратить внимание на современные угрозы энергоинформационной безопасности Украины. Процессы глобализации неумолимо ведут к построению невиданной в истории человечества всемирной технотронной диктатуры во главе с единым политическим и религиозным лидером. Открыто строится глобальное сетевое информационно-сотовое общество. Усиливаются процессы изменения образа человека с помощью нанотехнологий, которые будут непосредственно присутствовать в организме человека и будут подключены к новым глобальным сетям. Также усиливаются процессы воздействия на личность и общество благодаря новым техническим средствам, которые используются при построении нового глобального информационно-сотового общества. Ряд современных потенциальных и реальных угроз энергоинформационной безопасности Украины мы попытаемся обозначить в условиях благоприятного построения нового глобального информационно-сотового общества в контексте обеспечения национальной безопасности Украины.

Действующим законом Украины от 9 января 2007 г. «Об Основных принципах развития информационного общества в Украине на 2007–2015 годы» декларируется создание информационно-сотового общества в Украине. Актуальным можно считать внедрение нанотехнологий в организм человека, благодаря которым некоторые идеологи построения нового миропорядка предлагают создать особые условия для жизнедеятельности человека. При этом они не раскрывают сущности последствий и угроз для личности и общества в новом глобальном информационно-сотовом обществе. Построение информационно-сотового общества невозможно без принятия соответствующих нормативно-правовых документов в Украине. На первом этапе архитекторы информационно-сотового общества собираются осуществлять контролирующие и управляющие функции с помощью электронных биометрических устройств, постоянно сопровождающих человека. Сегодня действующий закон Украины от 20 ноября 2012 г. «О Едином государственном демографическом реестре и документах, которые подтверждают гражданство Украины, удостоверяющих личность и ее специальный статус» регламентирует создание и деятельность Единого государственного демографического реестра и оформление документов с использованием этого реестра. Таким образом, речь идет о замене общегражданских бумажных документов на электронные биометрические устройства, информацию с которых можно считывать на расстоянии, а с

помощью новых технологий можно управлять социальной группой и поведением отдельных лиц, что является латентной угрозой энергоинформационной безопасности Украины. Так, ст. 21 вышеуказанного закона Украины регламентируется получение паспорта гражданина Украины, который содержит бесконтактный электронный носитель, а ст. 22 также предусматривает, что паспорт гражданина Украины для выезда за границу содержит бесконтактный электронный носитель.

Следующим этапом будет внедрение технических средств, неотделимых от тела человека. Следует напомнить, что соединение нанотехнологий с организмом человека является угрозой энергоинформационной безопасности личности, а в целом и общества, а также и государства.

Конечно, потребуется некоторое время для принятия ряда законов Верховным Советом Украины, в том числе некоторых нормативно-правовых документов, регламентирующих внедрение RFID-чипов под кожу человека, примером может служить распространение нанотехнологических средств в США, где получают широкое распространение в индивидуальном, «подкожном», пользовании среди людей. Производитель таких устройств – компания Applied Digital Solutions собиралась имплантировать в 2002 г. 10 тыс. своих VeriChip жителям Мексики. Эта маленькая капсула способна нести в себе индивидуальный номер человека, по которому можно определить его медицинскую историю, адрес, номер телефона и прочую информацию о личности.

В каждой стране мира создается электронное правительство, построенное по единым международным стандартам на единой информационной и программной платформе. Со временем электронные правительства отдельных стран должны составить единую всемирную систему. Локальное электронное правительство с его областными и другими центрами, будут подконтрольны наднациональным структурам, которые фактически будут обладать абсолютной властью над электронным населением. Несомненно, что электронное правительство Украины будет входить в единую глобальную архитектуру всемирного электронного правительства. В целом же совершенно очевидно, что реализация проектов, направленных на вступление Украины в глобальное информационно-сотовое общество по международным стандартам и правилам, необходимо расценивать как действия, ведущие к разрушению основ национальной безопасности Украины.

В контексте построения глобального информационно-сотового общества следует обратить внимание и на ст. 1, 2 закона Украины от 10 января 2007 г. «О ратификации Соглашения о сотрудничестве в гражданской глобальной навигационной спутниковой системы (ГНСС) между Украиной и Европейским содружеством, его государствами-членами». Из нормативно-правового акта следует, что совместная работа в сфере

гражданской спутниковой навигации «ГАЛИЛЕО» (автономная гражданская европейская глобальная спутниковая навигационная система) на данный момент проходит под гражданским контролем, но управление этой системой *может быть передано частному лицу*. Латентная угроза утратить контроль гражданского общества над спутниковой навигационной системой и универсальный компьютером в Страсбурге и передача его частному лицу может создать благоприятные условия для захвата управления системой «ГАЛЛИО» и базой персональных данных, куда передается информация для автоматизированной обработки в универсальном компьютерном центре в Страсбурге.

Следует также напомнить, что особое положение в контексте обеспечения энергоинформационной безопасности Украины в условиях развития информационно-сотового общества занимает психотронное оружие, обеспечивающее воздействие на этническую, религиозную и коллективную психологию граждан территории потенциального противника. Внешняя сила формирует модель поведения через манипуляцию социальными группами. Негативные воздействие обусловлено манипуляцией психики (сознания и подсознания) человека, сопровождающееся неадекватным восприятием им реальной действительности. Такое воздействие может представлять угрозы для различных видов безопасности личности и общества, государства. Одной из разновидностей является психофизическое (энергоинформационное) воздействие физических факторов информационной или энергетической природы на психику человека.

Развитие научно-технического прогресса влияет на новые современные потенциальные угрозы энергоинформационной безопасности, например воздействие на человека психотронным оружием. Так, коллектив ученых, возглавляемый академиком Российской академии естественных наук И.В. Смирновым, является автором научного труда по поведению и состоянию человека в информационной среде обитания и практических приемов их коррекции. Можно сказать, что западные специалисты в вышеуказанной сфере считают И.В. Смирнова отцом психотронного оружия. Подобные исследования проводились не только в России, но и в США, где в 1993 г. была создана американская компания Psychotechnologies Corp. В это же время появился и стал развиваться Институт психоэкологии РАЕН. В 1997 г. в Российском университете дружбы народов начала работать кафедра психоэкологии, в 1998 г. – русско-корейская компания «KRTechnologies» и др.

Основными направлениями исследований психоэкологии с применением компьютерных психотехнологий являются психозондирование и психокоррекция.

Психокоррекция позволяет управлять состоянием и поведением человека.

Разработаны следующие методы психокоррекции:

акустическая, или аудиопсихокоррекция – закодированные слова, целые фразы закладываются в аудиоряд, который человек прослушивает;

видеопсихокоррекция – закодированные образы, сюжетные картинки и слова закладываются в видеоряд, который он просматривает.

К новейшим угрозам энергоинформационной безопасности Украины можно отнести программу активного высокочастотного исследования авроральной области HAARP (High Frequency Active Auroral Research Program), которая находиться в США. Система HAARP способна создавать вибрации волн, проникающие в мозг людей и животных; вибрации волн могут проникать через толщу Земли и обнаруживать скрытые бункеры и т. д.

В то же время в США есть нормативный правовой акт от 2 октября 2001 г. № HR 2977 IH «О сохранении космоса», представленного палатой представителей США, который запрещает размещение оружия в космосе, а именно в ст. 7 к экзотическим системам оружия относят: электронное, психотронное, или информационное оружие; высотные сверхнизкочастотные системы оружия и др. Согласно вышеуказанному нормативно-правовому акту США термин «оружие» и «система вооружения» называет устройство, способное направить источник энергии (включая молекулярную или атомную энергию, лучи субатомных частиц, электромагнитное излучение, плазму или излучение сверхнизкой частоты (ELF) или ультранизкой частоты (ULF); причинить смерть или ранения, или повреждение, или разрушение человека с помощью наземного, морского базирования или космических систем, используя электромагнитную, психотронную, звуковую, лазерную или другие энергии, направленные на отдельных людей или население с целью информационной войны, управления настроением или сознанием.

К сожалению, подобные нормативно-правовые документы, которые могли бы создать благоприятные условия для обеспечения энергоинформационной безопасности Украины, на данный момент Верховным Советом Украины не рассматриваются.

Исходя из вышесказанного, отметим, что знания даже общих положений, соединенных с позитивным практическим опытом своевременной нейтрализации потенциальных и реальных угроз энергоинформационной безопасности в значительной мере может способствовать более рациональной организации деятельности государственных органов с целью повышения эффективности обеспечения энергоинформационной безопасности и национальной безопасности Украины в целом.

УДК 004.056

В.О. Морар, И.О. Морар

ОРГАНИЗОВАННЫЕ ПРЕСТУПНЫЕ ФОРМИРОВАНИЯ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

По статистике 50 % пользователей старше 18 лет становятся жертвами кибератак или неприятных ситуаций в интернете: более 1 млн пострадавших в день или 12 жертв в секунду, 113 млрд долларов – общая сумма прямых убытков всего за 12 месяцев. Рост объема среднего ущерба от кибератаки на одного среднестатистического пользователя в 2011 г. – 197 долларов США, в 2013 г. – 298 долларов США. Каждый пятый человек старше 18 лет становился жертвой кибератаки либо в социальных сетях, либо через мобильные устройства.

Несмотря на то что проблемы киберпреступности присущи множеству государств, количество киберпреступлений среди пользователей разнится (см. таблицу) также, как и общий ущерб от кибератак (рис. 1).

Страны, где больше всего жертв киберпреступности среди пользователей

Страна	Процент от числа населения
Россия	85
Китай	77
Южная Африка	73
Мексика	71
ОАЭ	71
Новая Зеландия	69
Канада	68
Индия	65
Колумбия	64
США	63
Турция	63
Саудовская Аравия	62
Сингапур	61
Австралия	60
Бразилия	60
Польша	60
Объединенное Королевство	58
Италия	56
Швеция	56
Германия	53

Дания	50
Нидерланды	50
Франция	45
Япония	19

* Во всех случаях учитывались те, кто оказывался жертвой хотя бы раз в жизни (в опросе приняли участие 13 033 респондента в возрасте от 18 до 64 лет из 24 стран).

Рис. 1. Общий ущерб от кибератак в мире (млрд долларов)

Увеличивается разнообразие и доступность технических средств, в том числе разной бытовой техники с подключением к интернету (телевизоры, холодильники и пр.). Ориентация государства в сторону развития и популяризации безналичных расчетов, сопровождающееся увеличением количества устройств, осуществляющих финансовые транзакции, ростом числа пользователей всевозможных электронных платежных систем и развитие интернет-торговли привели к тому, что уже 87 % респондентов осуществляют операции с электронными деньгами, используя настольный или портативный компьютер, 22 % и 27 % – с помощью планшетов и смартфонов соответственно. При этом отвечая на вопрос: «Сталкивались ли вы с киберпреступностью?» – 68 % российских респондентов дали положительный ответ.

Совершенно очевидно, что эта сфера жизнедеятельности общества не могла остаться без внимания со стороны организованных преступных формирований (ОПФ), в том числе и транснационального характера (ТОПФ) В качестве примера киберпреступности с иностранным субъектом можно привести знаменитую пирамиду МММ-2012 в Республике Беларусь, когда преступник нарушал законы государства без физического нахождения на его территории.

Актуальность проблемы кибербезопасности, сохраняющаяся на протяжении нескольких лет, связана не только с несовершенством нормативно-правовой базой Российской Федерации, которая развивается. Другими составляющими информационной сферы, требующими к себе внимания, являются: информационно-техническое и информационно-психологическое направления (рис. 2).

И если первое направление наименее подвержено прямому влиянию со стороны ОПФ (коррупция и лоббирование интересов, в том числе в законодательных органах, имеет место быть, т. е. их нельзя не учитывать), то информационно-техническое и информационно-психологическое направление наиболее интересны организованным преступным формированиям. В этой связи даже возникли и существуют как кибер ОПФ (например, Anonymous, Cuber, Hidden Lynx и др.), специализирующиеся исключительно на преступлениях в информационной сфере, так и классические формирования, одним из направлений деятельности которых является совершение киберпреступлений.

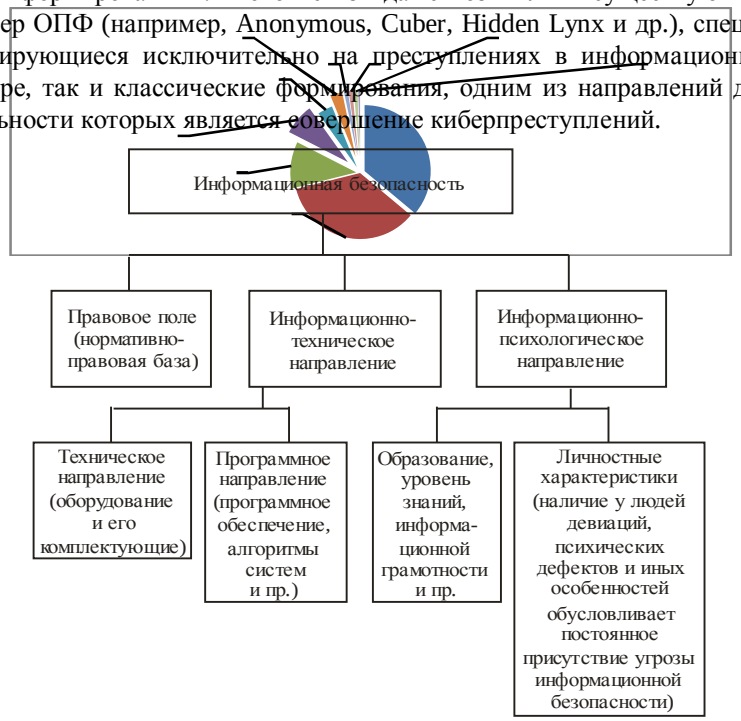


Рис. 2. Типовая схема направлений обязательных для развития и совершенствования информационной безопасности

В этой связи возникают и формируются разные рынки.

Рынок купли-продажи уязвимостей («багов», «слойтов») как легальный, так и криминальный. И если на легальном варианте данного рынка компании (например, iDefense, SnoSoft, VUPEN, Google, Facebook и др.) платят энтузиастам за обнаруженные уязвимости («баги», «сплойты») с целью своевременного их исправления и поддержания уровня информационной безопасности на достаточном уровне, то на криминальном цель обнаружения уязвимостей иная.

Рынок вредоносного программного обеспечения. Так, например, вредоносная программа CRYPTOLOCKER, парализующая работу технического средства и требующая от жертвы плату (300 долларов США) за возобновление работоспособности, и другие вредоносные программы. Например, вредоносная программа «Careto» или «Маска», обнаруженная специалистами «Лаборатории Касперского», считается серьезной шпионской угрозой. Ее атаки точечны и тщательно продуманы. По данным Kaspersky, вредоносная программа еще с 2007 г. собирает конфиденциальную информацию: считывает нажатие клавиш, записывает содержание разговоров Skype, ключи шифрования и другие данные. «Careto» заражает как Windows и OS X, так iOS и Android. Всего через несколько часов после обнаружения вредоносной программы «Лабораторией Касперского» вся информации и все сервера «Careto» исчезли.

Кибератаки, например финансовые, которые хотя и являются сложной и дорогой в реализации атакой по сравнению с другими (DDos-атака, рассылка спама и прочее), является наиболее прибыльным видом киберпреступления, так как в случае успеха предоставляет прямой доступ к деньгам жертвы.

Вместе с тем угрозы информационной безопасности эволюционируют, возникают новые. Реальность угрозы не ослабевает, а уровень информационной грамотности остается на достаточно низком уровне Например, сбой в январе 2014 г. государственного файрвола Китая «Золотой Щит». Это была не просто диверсия, направленная на обрушение файрвола подконтрольного государству, а демонстрация силы со стороны организованного преступного формирования. Так, всех граждан в период инцидента перенаправляли на страницу содержащей информацию с описанием алгоритма по обходу файрвола Китая «Золотой Щит». Ежегодный рейтинг худших паролей, публикуемый Splash-Data и формируемый с учетом списка украденных паролей и попавших в интернет, возглавляет «123456», включая такие, как «password», «11111» и др. И все это является благодатной почвой для приложения криминальных талантов ОПФ, не только использующей данные угрозы информационной безопасности в своих интересах. Они также принимают активное участие по формированию причин и условий для возникновения возможностей осуществления киберпреступлений, в том числе посредством деятельности в следующих направлениях: информационно-техническое, информационно-психологическое и правовое поле. Несмотря на то что первое направление, наименее подвержено прямому влиянию со стороны ОПФ, коррупция и лоббирование интересов, в том числе в законодательных органах, имеет место быть, т. е. их нельзя не учитывать.

Таким образом, информационная безопасность является одной из основных составляющих системы обеспечения национальной безопасности Российской Федерации в целом. Для ее обеспечения необходим комплексный подход, включающий работу над системой законодательных актов и в техническом и психологическом направлениях. А также наличие понимания того, что борьба с ОПФ в информационной сфере, должна стать одной из основополагающих задач для обеспечения кибербезопасности личности, организаций и государства.

УДК 341.4:004.9

Н.О. Мороз

МЕЖДУНАРОДНО-ПРАВОВАЯ КВАЛИФИКАЦИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Выявление международно-правовой сущности преступлений в сфере высоких технологий имеет большое теоретико-прикладное значение. Международно-правовая квалификация преступлений в сфере высоких технологий позволяет устанавливать адекватные правовые средства противодействия таким преступлениям в зависимости от их принадлежности к международным преступлениям, или преступлениям международного характера. Этим обусловлена актуальность темы настоящего исследования.

Международные преступления в науке принято определять на основании критерия объекта посягательства. В связи с этим полагаем, что из всех составов преступлений в сфере высоких технологий, закрепленных в международных соглашениях, к международному преступлению относится использование информационных и коммуникационных технологий для совершения актов терроризма, кибертерроризм (ст. 15 Арабской конвенции по борьбе с преступлениями в сфере информационных технологий от 21 декабря 2010 г.).

Полагаем, что совершение международного терроризма при помощи информационных и коммуникационных технологий является международным преступлением, поскольку:

1. Международный терроризм является международным преступлением ввиду объекта его посягательства, средств и методов совершения. В ряде резолюций Совета Безопасности ООН указывается, что международный терроризм представляет собой угрозу миру и безопасности человечества и является вызовом всем государствам и человече-

ству. Более того, для привлечения к уголовной ответственности за совершение отдельных актов терроризма был создан Специальный трибунал по Ливану.

2. Кибертерроризм рассматривается в качестве угрозы информационной безопасности в Соглашении между Правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения информационной безопасности от 16 июня 2009 г. Использование информационных и коммуникационных технологий в террористических целях запрещено Резолюцией Генеральной Ассамблеи Интерпола от 22 сентября 2005 г. № 10, а также ст. 1, 58 закона о терроризме Великобритании 2000 г., п. 2. ст. 421-1 Уголовного кодекса Франции, § 278c (126a), 278f Уголовного кодекса Австрии, § 237 Уголовного кодекса Эстонии.

3. Мнение о возможности использования информационных технологий для совершения международных преступлений (например, агрессии) высказывалось в науке, а также получило реализацию в проекте конвенции ООН «Об обеспечении международной информационной безопасности», разработанном в Российской Федерации.

В настоящее время не существует специальных международных соглашений для противодействия кибертерроризму. Лишь в одном международном договоре (Арабской конвенции по борьбе с преступлениями в сфере информационных технологий) закреплена обязанность государств-участников предусмотреть в своем уголовном законодательстве соответствующий состав преступления.

Учитывая общественную опасность кибертерроризма, существующие международно-правовые меры по борьбе с ним нельзя считать адекватными. В связи с этим считаем обоснованным заключение универсального международного договора для противодействия кибертерроризму, а также использованию информационных технологий для совершения деяний против международного мира и безопасности.

Международную природу преступлений в сфере высоких технологий подчеркивали многие ученые. На 11-м конгрессе ООН по предупреждению преступности и обращению с правонарушителями заявлялось о международной природе таких преступлений и о появлении новой тенденции – использовании компьютерных технологий преступными группами. Проведенный анализ региональных международных соглашений, универсальных международных договоров общего характера позволил выделить 21 состав преступлений в сфере высоких технологий, которые, по нашему мнению, являются преступлениями международного характера.

Преступления в сфере высоких технологий совершаются физическими лицами и вне связи с политикой, проводимой конкретным государством. Это следует из норм Факультативного протокола к Конвенции о правах ребенка, касающегося торговли детьми, детской проституции и порнографии от 25 мая 2000 г., Конвенции Совета Европы о киберпреступности от 23 ноября 2001 г., дополнительного Протокола к Конвенции Совета Европы о киберпреступности относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных сетей от 21 января 2003 г., Соглашения о сотрудничестве государств СНГ в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г., Арабской конвенции по борьбе с преступлениями в сфере информационных технологий от 21 декабря 2010 г.

Вместе с тем п. 1 ст. 12 Конвенции Совета Европы о киберпреступности предусматривает обязанность государства-участника обеспечить возможность привлечения юридических лиц к ответственности за уголовное преступление, которое совершается в его пользу физическим лицом.

Действующие международные соглашения не предусматривают возможности создания международного судебного органа для уголовного преследования лиц, совершивших преступления в сфере высоких технологий.

Также отметим, что в целях координации международного сотрудничества в борьбе с преступностью в сфере высоких технологий были приняты четыре специальных международных договора.

Полагаем, что правоотношения по поводу использования глобальных информационных сетей являются международными, поскольку интернациональными являются как данные сети, так и субъекты, отношения между которыми возникают относительно их правового регулирования и эксплуатации. Таким образом, в том случае, глобальные информационные системы и сети являются предметом или средством совершения преступления или если средством их совершения являются иные технические средства удаленного получения данных, объектом таких преступлений, на наш взгляд, следует считать международные отношения по сотрудничеству в области использования телекоммуникационных, компьютерных систем или сетей.

Итак, преступления в сфере высоких технологий международного характера – это запрещенные международными договорами деяния, посягающие на международное сотрудничество в области использования телекоммуникационных, компьютерных систем или сетей, совершаемые физическими или юридическими лицами, которые несут за них уголовную ответственность по национальному праву.

УДК 341.23 + 342.9

Д.В. Перевалов

ОСНОВНЫЕ НАПРАВЛЕНИЯ СОТРУДНИЧЕСТВА ГОСУДАРСТВ – УЧАСТНИКОВ СНГ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ

Современное общество характеризуется переходом к качественно новому состоянию – информационному обществу, в котором отмечается возрастающее влияние новых информационно-коммуникационных технологий на все сферы общественной жизни, обусловленное лавинообразным развитием систем передачи данных. Разработка новейших технологий, которые призваны обеспечить потребности личности и общества в информации, влечет за собой поступательное развитие новых средств коммуникации, рост их производства и модификации.

Вместе с тем трансформация общества в условиях информационно-коммуникационной революции формирует новые угрозы информационной безопасности как отдельных государств, так и конкретных регионов, в том числе для безопасности критически важных объектов информационно-коммуникационной инфраструктуры (КВО). Актуальной данная проблема является и для государств – участников СНГ.

В современный период сотрудничество государств – участников СНГ по вопросам обеспечения безопасности КВО требует совершенствования в первую очередь в вопросах гармонизации законодательств в рассматриваемой области. В соответствии с общепризнанными принципами и нормами международного права в качестве приоритетных целесообразно рассматривать следующие направления гармонизации законодательств государств – участников СНГ в области обеспечения безопасности КВО.

1. Определение понятийно-категориального аппарата, используемого при правовом регулировании обеспечения безопасности КВО.

При развитии понятийно-категориального аппарата в рассматриваемой области представляется необходимым принимать во внимание основные формы и характер проявления угроз безопасности КВО на территориях государств – участников СНГ, особенности создания и функционирования систем обеспечения безопасности таких объектов. В дальнейшем при разработке конкретных международных и национальных нормативных правовых актов необходимо обеспечить ориентацию всех участников на использование единого понятийно-категориального аппарата.

2. Закрепление основных направлений правового регулирования обеспечения безопасности КВО в государствах – участниках СНГ.

В качестве таких направлений, носящих приоритетный характер и подлежащих закреплению в национальном законодательстве государств СНГ, следует отнести: определение источников угроз, их характера, разработку классификации угроз в рассматриваемой сфере; определение деяний, признаваемых правонарушениями в рассматриваемой сфере; регламентацию деятельности по выявлению и последующему устранению причин и условий, способствующих формированию и реализации угроз безопасности КВО; определение мер, направленных на недопущение нанесения ущерба критическим элементам КВО; установление мероприятий, направленных на выявление и пресечение противоправной деятельности, нарушающей или прекращающей функционирование КВО.

Одним из важнейших аспектов является уточнение закрепляемых в национальном законодательстве государств СНГ положений, предусматривающих перечни правонарушений в области обеспечения безопасности КВО. Соответствующую разработку и доработку законодательных актов в данной сфере целесообразно осуществлять с учетом отличительных признаков конкретных действий, позволяющих идентифицировать их и выделить из спектра сходных по объективной стороне преступлений и правонарушений, которые будут рассматриваться как угрозы безопасности КВО.

Требуют разработки и закрепления в специализированных нормативных правовых актах или в отдельных правовых нормах наиболее важные направления деятельности компетентных государственных органов в области обеспечения безопасности КВО: создание национальной системы обеспечения безопасности КВО; формирование и использование сил и средств обеспечения безопасности КВО; деятельность по идентификации угроз безопасности КВО, предупреждению, выявлению и пресечению правонарушений в данной области; характер и пределы реализации мер, направленных на пресечение указанных правонарушений; определение объема полномочий и ответственности между компетентными государственными органами, эксплуатирующими КВО, осуществляющими контроль их эксплуатации, определяющими правоохранительную деятельность в области обеспечения безопасности КВО.

3. Нормативное закрепление основных направлений международного сотрудничества в сфере правового регулирования обеспечения безопасности КВО.

В качестве таких направлений следует рассматривать: проведение согласованной политики по гармонизации национального законода-

тельства в рассматриваемой области; совместная работа по предотвращению и устранению причин и условий, способствующих формированию угроз безопасности КВО; обмен информацией по вопросам предупреждения и пресечения правонарушений, создающих в области безопасности КВО; оказание взаимной правовой, методической, технической и иной помощи; проведение совместных процессуальных, оперативных и иных мероприятий по документированию и пресечению правонарушений в рассматриваемой области и т. д.

4. Обеспечение введения мер ответственности за подготовку и совершение деяний, которые будут отнесены к правонарушениям в области обеспечения безопасности КВО.

За совершение правонарушений в области обеспечения безопасности КВО физические лица в соответствии с национальным законодательством должны нести уголовную, административную и иную ответственность в зависимости от общественной опасности деяния или наступивших последствий.

Для повышения эффективности деятельности компетентных государственных органов и системы мер, направленных на предупреждение и пресечение правонарушений в области обеспечения безопасности КВО, представляется необходимым обеспечить согласование правовых норм в рамках специальных законов, в том числе соответствующих норм уголовного законодательства стран СНГ.

К первоочередным целесообразно относить следующие меры по совершенствованию правового регулирования обеспечения безопасности КВО.

1. Определение уровней правового регулирования обеспечения безопасности КВО государств – участников СНГ: межгосударственный, национальный.

При этом необходимо учитывать, что при осуществлении правового регулирования рассматриваемой области возникает ряд проблем, основной из которых является сопряжение технических аспектов эксплуатации КВО и закономерностей правовой регламентации деятельности компетентных государственных органов по обеспечению их безопасности.

2. Совершенствование межгосударственного уровня правового регулирования обеспечения безопасности КВО.

Представляется, что в рамках СНГ будет обоснованной разработка модельного закона «О критически важных объектах информационно-коммуникационной инфраструктуры», который должен предусматривать: основные термины и их определения; основные направления государственной политики в области обеспечения безопасности КВО;

положения, определяющие общие критерии и порядок отнесения объектов социально-экономической инфраструктуры к КВО; категории КВО; общие положения ведения государственного реестра КВО; порядок организации безопасного функционирования КВО; требования к безопасному функционированию КВО; особенности осуществления внутреннего и внешнего контроля функционирования КВО; содержание деятельности по обеспечению безопасности КВО, ее основные задачи и принципы; систему обеспечения безопасности КВО (объекты, субъекты, задачи, угрозы, содержание правовых, организационных, инженерно-технических, программно-аппаратных и специальных мер); порядок реагирования на инциденты безопасности; порядок функционирования государственной системы реагирования на инциденты безопасности КВО; особенности реагирования на инциденты безопасности КВО; основания и порядок исключения объектов социально-экономической инфраструктуры из числа КВО; общие положения исключения указанных объектов из государственного реестра КВО; субъекты и порядок государственного контроля и надзора в области обеспечения безопасности КВО; полномочия государственного органа в области обеспечения безопасности КВО.

3. Совершенствование национального уровня государств – участников СНГ по обеспечению безопасности КВО.

На национальном уровне государств – участников СНГ требуется принятие специальных нормативных правовых актов (закона, указа президента, постановления правительства), непосредственно регламентирующих обеспечение безопасности КВО.

Одновременно необходимо создание системы правовых норм в административном, уголовном, трудовом и гражданском законодательствах, определяющих компетенцию и ответственность заинтересованных юридических и физических лиц в данной сфере.

УДК 343.985

А.А. Смирнов

ПРОТИВОДЕЙСТВИЕ ИСПОЛЬЗОВАНИЮ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ДЕСТАБИЛИЗАЦИИ ОБЩЕСТВЕННО-ПОЛИТИЧЕСКОЙ ОБСТАНОВКИ В ГОСУДАРСТВЕ

Информационно-коммуникационные технологии (ИКТ) оказывают все более значительное влияние на обеспечение национальной и меж-

дународной безопасности, которое носит разноплановый характер и включает в себя такие аспекты, как трансформация традиционных и возникновение новых угроз безопасности информационного характера, использование ИКТ в деятельности субъектов обеспечения безопасности и др. Генеральная Ассамблея ООН приняла, начиная с 1998 г., целый ряд резолюций под названием «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности», в которых выражается озабоченность тем, что информационные технологии и средства потенциально могут быть использованы в целях, несовместимых с задачами обеспечения международной стабильности и безопасности. Одной из таких деструктивных целей является дестабилизация общественно-политической обстановки в государстве.

Источниками такой дестабилизации выступают внутренние субъекты (террористические и экстремистские организации) и (или) иностранные государства. В последнем случае правомерно говорить о вмешательстве во внутренние дела государства. Между внешними и внутренними субъектами дестабилизации в большинстве случаев имеет место взаимосвязь, степень выраженности которой может варьироваться в зависимости от обстоятельств.

Использование подрывных операций в качестве инструмента борьбы между государствами насчитывает не одно тысячелетие. Так, они достаточно подробно описаны в древнекитайских трактатах по военному искусству [1, 2]. Например, перечень 36 китайских стратагем включает такие, как «убить чужим ножом» (№ 3), «тайно подкладывать хворост под котел другого» (№ 19), «стратагема сеяния раздора» (№ 33).

Однако именно в XX в. подрывные операции были поставлены на твердую теоретическую основу и стали своеобразной универсальной технологией борьбы с государствами-противниками. Произошел качественный переход от единичных стратегических операций специальных служб, планирование и проведение которых занимало многие десятилетия, к некой конвейерной процедуре свержения неугодных режимов, запускавшейся операторами в нужный момент времени при достаточно сжатой предварительной работе.

В последние десятилетия наиболее распространенной формой таких подрывных операций стали так называемые «цветные революции». Их можно определить как форму свержения политических режимов, осуществляемого разнородной коалицией протестных сил сетевого типа при активной внешней поддержке международных акторов с преимущественным применением методов ненасильственного сопротивления.

Основными формами использования ИКТ для дестабилизации общественно-политической обстановки в государстве выступают:

ведение внешней и внутренней враждебной пропаганды через СМИ и интернет-ресурсы;

распространение информационной продукции, провоцирующей дестабилизацию социально-политической обстановки в стране;

подстрекательство в социальных сетях к проведению протестных акций, мятежей или террористических атак, организации незаконных вооруженных формирований;

использование электронных платежных систем для финансирования террористических и экстремистских организаций, незаконных вооруженных формирований;

кибератаки на критически важные объекты информационной инфраструктуры.

Среди ключевых информационных ресурсов, которые используются для дестабилизации общественно-политической обстановки, следует выделить, прежде всего, средства массовой информации и ресурсы глобальной информационной сети Интернет. К последним относятся интернет-сайты, видеохостинги, социальные сети, блоги и т. п. В интересах специальных служб разрабатываются специализированные программно-технические инструменты ведения психологических операций в интернете.

В ходе революционных событий на Украине в начале 2014 г. использовался такой инструмент сетевого противоборства, как Twitter-шторм. Активисты Евромайдана запустили в Twitter флешмоб #DigitalMaidan Twitter Storm с целью привлечь внимание иностранных СМИ и общественных деятелей к событиям в Украине. Организаторы акции предлагали пользователям принять участие в Twitter-шторме, для чего необходимо было в определенное время отправить поток твитов, таргетированных на аккаунты ключевых журналистов, политиков и лидеров мнений по всему миру. При этом на сайте уже было заготовлено более сотни коротких сообщений (твитов) с призывами предотвратить новые жертвы среди протестующих и поддержать украинцев в борьбе за демократию. Присоединиться к Twitter-шторму можно на сайте или в группе инициативы на Facebook. Чтобы отправить твиты, достаточно лишь нажать на соответствующую кнопку на сайте напротив выбранного сообщения. При этом ресурс нацеливал именно на синхронную массовую рассылку таких сообщений, которая стартовала в определенное время, создавая тем самым мощный поток сообщений (шторм).

Серия революций в странах Ближнего Востока и Северной Африки («Арабская весна»), протестные акции в России и Республике Беларусь, государственный переворот в Украине – эти и другие международные события 2010–2014 гг. продемонстрировали возможности успешного применения ИКТ для дестабилизации общественно-политической обстановки в государстве. Безусловно, неправильно видеть в

самих ИКТ причину такой дестабилизации, однако они выступают достаточно мощными инструментами ее осуществления, в связи с чем требуется выработка мер противодействия их применению в деструктивных целях.

Считаем, что к числу основных групп мер информационного противодействия использованию ИКТ для дестабилизации общественно-политической обстановки в государстве следует отнести следующие меры:

а) поискового и информационно-аналитического характера – направлены на обнаружение, сбор и анализ данных об информационной деятельности субъектов дестабилизации, выявление их замыслов и направлений деструктивной активности;

б) информационной изоляции и подавления – применяются для подавления или блокирования каналов коммуникации, используемых для дестабилизации, а также ограничения распространения через них деструктивной информации либо доступа к ней пользователей;

в) информационного реагирования и контрпропаганды – направлены на нейтрализацию враждебной пропаганды, разоблачение и дискредитацию в общественном сознании субъектов дестабилизации, на донесение до общества информации об истинном положении дел;

г) информационно-пропагандистского, обучающего и воспитательного воздействия – имеют долговременный характер и направлены на формирование «информационного иммунитета» населения к враждебной пропаганде и подрывным действиям в области массового сознания.

На наш взгляд, сам термин «противодействие» не должен ориентировать только на ответную реакцию государственных институтов на возникшую угрозу дестабилизации общественно-политической обстановки в стране. Полагаем, что основой стратегии деятельности государства в борьбе с данной угрозой должны быть наступательность и действия на опережение. Только так можно избежать стремительного развития событий по негативному сценарию в новом цифровом мире с присущими ему сверхвысокими скоростями передачи и распространения массовой информации.

1. Сунь-цзы. Искусство стратегии. М. : Эксмо ; Спб. : Мирград, 2007. 528 с.

2. Зенгер Х. фон. Стратагемы. О китайском искусстве жить и выживать : в 2 т. М. : Эксмо, 2006. 1024 с.

3. Яровая М. Цифровой Майдан: активисты запускают Twitter-шторм, нацеленный на мировую общественность [Электронный ресурс] // AIN.UA. 27.01.2014. URL: http://ain.ua/2014/01/27/510280 (дата обращения: 24.03.2014).

4. Сундиев И.Ю., Смирнов А.А. Обитаемый остров 2.0 [Электронный ресурс] // Сайт С.П. Курдюмова. URL: http://spkuryumov.ru/networks/obitaemyj-ostrov-2.0 (дата обращения: 26.03.2014).

УДК.343.985

А.Н. Тукало, Е.В. Трахимович

НЕКОТОРЫЕ АКТУАЛЬНЫЕ АСПЕКТЫ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСТНОСТИ СО СТОРОНЫ СОЦИАЛЬНЫХ СЕТЕЙ

В настоящее время социальные сети вытеснили традиционные средства массовой информации с информационного поля. Данный факт давно был осознан владельцами традиционных средств массовой информации и обусловлен тем, что охват одного поста в сообществе, например в социальной сети «ВКонтакте», может превышать совокупный охват аудитории телевидения, радио, газет и пр. (под охватом следует понимать число пользователей, которые увидели записи сообщества. Различают охват подписчиков и полный охват. Полный охват отражает число всех пользователей социальной сети, которые видели записи конкретного сообщества за определенный промежуток времени).

Опасность воздействия социальных сетей возрастает благодаря эффекту спящего (англ. sleepereffect, понятие заимствовано из области шпионажа). Данный эффект был открыт психологом Карлом Ховландом, который возглавлял исследования для американского военного министерства. Суть его – знание об источнике разрушается быстрее, чем приведенные аргументы. Иными словами, мозг относительно быстро забывает о том, откуда поступили сведения (из социальных сетей), но саму по себе информацию так быстро он не забывает. Поэтому информация из недостоверного источника со временем приобретает все бóльшую достоверность. Обесцененный элемент улетучивается из памяти прежде, чем содержание послания начнет забываться. Таким образом, социальные сети превращаются в мощный инструмент пропаганды, а с учетом того, что присутствие государственных органов и средств массовой информации в социальных сетях в Республике Беларусь носит формальный характер, то представляет серьезную угрозу не только информационной безопасности государства, но и его суверенитету. Достаточно вспомнить порядок использования социальных сетей во время событий Евромайдана в Украине, а также то, как они используются сейчас во время боевых действий на территории самопровозглашенной Донецкой Народной Республики. Для этого целесообразно взглянуть на сообщества двух лагерей: так называемого «Правого сектора» и «Сторонников федерализации» или «Антимайдана».

Использование приемов социальной инженерии, а также инструментов социального медиамаркетинга в социальных сетях, позволяет с минимальными материальными и временными затратами удаленно создавать сообщества лиц с отклоняющимся поведением, а также оказывать на них должное информационное воздействие, а в случае необходимости координировать их действия.

Правилами социальных сетей запрещено распространение информации, а также создание сообществ, целью которых является разжигание войны, пропаганда насилия, расового неравенства и т. п. Поэтому открытое продвижение таких сообществ невозможно либо затруднено. Однако возможны иные способы:

1. Деятельность под видом оппозиционных сообществ, которая позволяет осуществлять, с одной стороны, необходимую пропаганду, а с другой стороны, использовать внутренние инструменты социальной сети для расширения аудитории и распространения своих взглядов (таргетинг, ретаргетинг, реклама в сообществах, обмены и т. п.).

2. Продвижение неофициальными («серыми», «черными» методами). Это способ расширения своей целевой аудитории посредством спама в социальных сетях, массовых приглашений в конкретное сообщество, взлома страниц. Цены на данные услуги невелики: за тысячу участников придется выложить от 50 до 150 долларов США (цены зависят от применяемых методов, а также от критериев самой аудитории: страна, город, возраст, пол, интересы и т. п.). С другой стороны, данные операции можно осуществить самостоятельно, приобретая специальное программное обеспечение.

3. Парсинг данных пользователей социальной сети по интересующим критериям с целью привлечения в тематическую группу, а также получения интересующих данных, например номеров телефонов граждан, состоящих в определенном сообществе (возможно, для рассылки через зарубежные сервисы sms-спама, содержащего либо угрозы, либо призывы участвовать в массовых мероприятиях).

Кроме того, в целях информационной пропаганды используется не одно сообщество, а несколько (как правило, не меньше трех). Связано это с тем, что чтобы заставить человека поверить в конкретную информацию, необходимо, чтобы он столкнулся с данной информацией не менее трех раз, причем информация должна быть воспринята субъектом, на которого оказывается воздействие, из разных источников.

УДК 34:002

В.К. Фисенко, В.А. Дмитриев,
А.Б. Степанян, Е.П. Максимович

ОСОБЕННОСТИ НОВЫХ ВЕРСИЙ МЕЖДУНАРОДНЫХ СТАНДАРТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Введением в действие новых версий базовых международных стандартов в области оценки информационной безопасности: ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008, ISO/IEC 15408-3:2008 и сопутствующих им документов ISO/IEC 18045:2008, ISO/IEC TR 15446:2009 требует адекватного обновления соответствующих национальных стандартов и делает актуальными работы в этом направлении. В докладе обсуждаются основные изменения в этих версиях и их влияние на методологию оценки безопасности информационных технологий.

Общая концепция – оценка безопасности информационных технологий (ИТ) путем проведения активного исследования объекта информационных технологий с целью независимой и достоверной оценки его фактических свойств безопасности сохранилась. Однако методы исследования претерпели ряд существенных изменений и стали более гибкими и предоставляют разработчику и эксперту бóльшую свободу действий.

Концептуальные изменения новой версии ISO/IEC 15408-1,2,3 состоят в следующем:

1) изменился объект оценки (ОО) – теперь это только продукты ИТ (ранее в качестве ОО рассматривались и продукты и системы ИТ. Теперь для продуктов и систем ИТ предполагается использовать разные стандарты);

2) появился новый вид деятельности – оценка составных ОО;

3) изменился подход к оценке таких важных аспектов безопасности, как разбиение на области, самозащита и невозможность обхода политики безопасности;

4) исключены анализ скрытых каналов и оценка стойкости средств безопасности;

5) допускается использование упрощенных профилей защиты (ПЗ) и заданий по безопасности (ЗБ), разработанных по первому уровню гарантии оценки, для которого по сравнению с обычным ЗБ: не требуется приводить описание проблемы безопасности и соответственно определения угроз, политики безопасности, предположений; не обязательно излагать задачи безопасности для ОО, но при этом задачи безопасности для среды функционирования должны быть изложены;

не требуется обосновывать задачи безопасности, поскольку в ЗБ не приводится описание проблемы безопасности; в обосновании требований безопасности необходимо аргументировать только обоснование неудовлетворения зависимостей, поскольку в ЗБ не приводятся задачи безопасности для ОО.

Выделение двух типов объектов оценки – простых (однокомпонентных) и составных обусловлено потребностью в использовании принципиально разных подходов к их оценке. Составной объект предполагает выбор двух или более объектов ИТ, уже прошедших успешную оценку безопасности в соответствии с ISO/IEC 15408-3 и объединение их в новый объект без какой-либо дальнейшей доработки каждого из составляющих компонентов. В составном ОО один компонент обычно опирается на сервисы, предоставленные другим компонентом. Компонент, которому необходимы сервисы, называется зависимым, а компонент предоставляющий сервисы – базовым. Введение простых и составных ОО обусловлено потребностью в использовании принципиально разных подходов к их оценке. Для составных объектов предметом исследования являются интерфейсы между составляющими их компонентами. Для поддержки разных уровней гарантии оценки составных объектов дополнительно введены три иерархических составных пакета гарантии, применяемые к объектам, состоящим из компонентов, которые прошли предварительную покомпонентную оценку. Увеличение гарантии от одного составного пакета к другому достигается подстановкой иерархически более высокого компонента гарантии из того же семейства гарантии и/или добавлением новых компонентов из других семейств.

В новой версии стандартов ISO/IEC 15408-1,2,3 признана неэффективность используемого ранее подхода к оценке таких свойств безопасности, как разбиение на области, самозащита и невозможность обхода политики безопасности. Как показала практика, по сравнению с проверкой других функциональных возможностей безопасности эти свойства трудно проверяемы и требуют особого многоаспектного и сложного анализа функциональных возможностей на уровне архитектуры комплекса средств безопасности и проекта ОО. Вследствие этого соответствующие функциональные требования безопасности исключены из ISO/IEC 15408-2. Вопросы проверки указанных свойств рассматриваются в новых семействах ADV_ARC «Архитектура безопасности» и ADV_INT «Внутренняя структура КСБО» класса гарантии ADV «Разработка» стандарта ISO/IEC 15408-3:2008.

Изменен подход к структурированию руководящих документов: вместо прежнего деления на документы типа «Руководство пользователя» и «Руководство администратора» в ISO/IEC 15408-3:2008 руководящие документы делятся на руководства по подготовке доставленного объекта оценки к работе (семейство AGD_PRE: «Подготовительные процедуры») и руководства по эксплуатации (семейство AGD_OPE «Руководство пользователя»). Такой подход отражает два важных этапа жизненного цикла объекта оценки (установка и эксплуатация) и позволяет более четко и полно учесть и отразить в документации возникающие на каждом из них проблемы безопасности – обеспечение безопасности на этапе установки объекта и обеспечение безопасности объекта на этапе его эксплуатации.

Усовершенствована структура уровней гарантии оценки, хотя, как и прежде, общее их количество осталось прежним (семь). В частности, во все уровни гарантии включены компоненты класса ASE «Оценка задания по безопасности», что представляется совершенно оправданным, так как процессы испытания и аттестации объекта базируется на проверке требований задания по безопасности и допущенные при его написании упущения и ошибки могут свести на нет эффективность данных процессов.

Изменения в стандартах ISO/IEC 15408-1,2,3 привели к существенному изменению сопутствующих документов ISO/IEC 18045 и ISO/IEC TR 15446.

В ISO/IEC 18045 представлен набор видов деятельности, касающихся экспертной оценки профилей защиты, заданий по безопасности, проектной документации на разных уровнях ее детализации (архитектуры безопасности, функциональной спецификации, представления реализации), моделирования политики безопасности, тестирования, анализа уязвимостей, эксплуатационной документации, безопасности составного ОО. В отличие от предыдущих версий разные виды деятельности эксперта сгруппированы по типам проводимой оценки, а не по действиям эксперта для оценки на соответствие отдельным уровням гарантии. Для ряда высокоуровневых гарантийных компонентов действия эксперта не определены ввиду отсутствия общесогласованных рекомендаций по проверке их выполнения. На уровне конкретных видов и подвидов деятельности изменения в ISO/IEC 18045 являются весьма значительными и определяются изменениями на уровне классов и компонентов гарантии из ISO/IEC 15408-3, что обусловлено наличием соответствующих связей между структурными единицами этих стандартов. Например, появление в ISO/IEC 15408-3 нового класса гарантийных требований ACO «Составной объект» привело к появлению в ISO/IEC 18045 нового вида деятельности, цель которой состоит в том, чтобы определить, были ли компоненты составного ОО интегри-

рованы безопасным способом в соответствии с ЗБ для составного ОО. Это достигается посредством анализа и тестирования интерфейсов между компонентами, поддерживаемыми анализом проекта компонентов и проведением анализа уязвимостей. В частности, при оценке качества тестирования требуется проверить, правильно ли разработчик выполнил и документировал тесты для каждого из интерфейсов базового компонента, на которые опирается зависимый компонент. Эксперт должен выполнить тестирование функциональных требований безопасности составного ОО с использованием интерфейсов составного ОО и интерфейсов базового компонента, используемых зависимым компонентом с целью проверки того, что они работают в соответствии о спецификацией. При выборке тестов нужно учитывать возможное влияние изменений на конфигурацию/использование базового компонента при применении его в составном ОО.

Документ ISO/IEC TR 15446 представляет собой руководство по разработке ПЗ и ЗБ в соответствии с требованиями стандартов ISO/IEC 15408-1,2,3.

ISO/IEC 15408-1,2,3 содержит описание состава ПЗ и ЗБ, но по-прежнему не дает никаких рекомендаций относительно способов их разработки, практического использования при определении, проектировании или разработке систем защиты информации. ISO/IEC TR 15446:2008 призван восполнить этот пробел. Он включает рекомендации и методики, разработанные в соответствии с требованиями из ISO/IEC 15408-1,2,3 и обобщающие коллективный опыт, накопленный в области оценки и обеспечения безопасности продуктов ИТ.

Указанные международные документы уже практически подготовлены для ввода в действие в Республике Беларусь как национальные стандарты.

УДК 34:002

А.А. Шугай

ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ

Информация о человеке неизбежно циркулирует в обществе, объективно существуя как в виде документов, так и в сознании других людей, а оборот ее часто осуществляется независимо от воли индивида.

В информации о гражданах в силу объективных причин нуждается и государство. Информация всегда была и остается важнейшим атрибутом государственного управления. С древнейших времен светская власть собирала информацию о населении с помощью фискальных органов. Церковные книги, где отмечались факты рождений, смертей, венчаний, были источником сведений о прихожанах для духовных правителей.

В свете вышеперечисленных факторов возникла объективная потребность в гармонизации интересов личности и государства в области оборота информации личного характера, что и обусловило появление в правовой науке специальной юридической категории – института персональных данных личности.

Мировое сообщество давно уже осознало проблему необходимости защиты персональных данных граждан, результатом чего стало принятие ряда международных документов, направленных на их защиту.

Юридические основы прав на защиту личной тайны и персональных данных были заложены в двух основополагающих международных документах – Всеобщей декларации прав человека, принятой Генеральной Ассамблеей ООН в 1948 г. и Европейской конвенции о защите прав человека и основных свобод 1950 г.

Согласно ст. 12 Всеобщей декларации прав человека никто не может подвергаться произвольному вмешательству в его личную жизнь, произвольным посягательствам на неприкосновенность жилища, тайну корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту от такого вмешательства или таких посягательств.

Европейская конвенция о защите прав человека и основных свобод, принятая 4 ноября 1950 г., в ст. 8 устанавливает, что каждый человек имеет право на уважение его личной и семейной жизни, корреспонденции.

Особой вехой в развитии законодательства о защите персональных данных в мировом сообществе стало принятие 28 января 1981 г. в Страсбурге Конвенции о защите частных лиц в отношении автоматизированной обработки данных личного характера СЕД № 108 (далее – Конвенция), целью которой стало обеспечение на территории каждой из сторон договора уважения прав и основных свобод каждого человека, особенно его права на неприкосновенность личной жизни в связи с использованием и обработкой его персональных данных.

На сегодняшний день Конвенцию подписали и ратифицировали более 40 стран, среди которых и ближайшие соседи Республики Беларусь (Латвия, Литва, Польша, Украина и Россия). Из государств Европы Конвенцию не подписали и не ратифицировали только Азербайджан, Армения, Сан-Марино и, к сожалению, Республика Беларусь.

В нашей стране на сегодняшний день отсутствует базовый нормативный акт в сфере защиты персональных данных, что, несомненно, негативно влияет на обеспечение защиты персональных данных граждан.

Так же в Республике Беларусь на данный момент отсутствует независимый орган по защите персональных данных. Практика создания

таких институтов по всему миру доказала, что они играют важную роль по контролю за соблюдением законодательства о персональных данных, интерпретации и развитию положений законодательства. Создание в Беларуси специализированного органа может привести к улучшению ситуации по защите персональных данных.

Очевидно, что существуют значительные расхождения белорусского законодательства со стандартами, закрепленными в основополагающих международных документах по защите персональных данных. Для Республики Беларусь принципиально важно как можно быстрее имплементировать положения Конвенции для полноценной реализации права на неприкосновенность частной жизни своих граждан.

Кроме того, не подписав Конвенцию, Республика Беларусь может остаться в информационной изоляции, так как Конвенция запрещает передачу персональных данных тем государствам или организациям, которые не могут обеспечить должный уровень защиты данных. Такой уровень может быть признан более «слабым», чем в других государствах, и для передачи персональных данных в Республику Беларусь могут потребоваться дополнительные разрешения. Таким образом, Беларусь может остаться в стороне от развития современного информационного общества.

В связи с этим считаем необходимым подписать и ратифицировать Республикой Беларусь Конвенцию о защите частных лиц в отношении автоматизированной обработки данных личного характера, после чего приступить к созданию национальной системы защиты персональных данных (разработать закон Республики Беларусь «О персональных данных», базовый законодательный акт в сфере защиты персональных данных; создать уполномоченный независимый орган по защите персональных данных граждан; привести в соответствие действующее законодательство с международными стандартами в сфере защиты персональных данных).

УДК 004.413.4

В.М. Шишкин

МОДЕЛИРОВАНИЕ ДИНАМИКИ ИНФОРМАЦИОННОЙ БОРЬБЫ

Последние годы демонстрируют отчетливую тенденцию того, что обеспечение информационной безопасности (ИБ) на различных ее уровнях приобретает черты противоборства и становится непрерывным процессом. Его сложность и динамика дает основания полагать,

что проблемы международной информационной безопасности (МИБ) должны исследоваться не только на вербальном уровне.

Учитывая реалии, особенно новейшие, и явное нежелание доминирующей в информационной сфере стороны терять свое превосходство МИБ полезно сделать предметом исследований теми средствами, которые позволят в значительной мере исключить субъективизм мнений. Необходимы инструменты объективного анализа и прогноза, а именно средства математического моделирования. Связав в систему динамического взаимодействия некоторый набор существенных в определенном контексте факторов, расчетным путем можно будет обеспечить возможность оценки развития ситуации при альтернативных сценариях, проигрывать различные варианты поведения сторон, оценивать эффективность управляющих воздействий и т. д.

В первом приближении, поскольку многие системы, изменение состояния которых согласовано с законами сохранения, могут быть описаны на языке обыкновенных дифференциальных уравнений [1], это может быть простейшая система таких уравнений. Опыт применения подобного рода динамических моделей в различных предметных областях, в том числе плохо формализуемых, имеет уже достаточно давнюю историю, показав их, по крайней мере, познавательную и прогностическую полезность. Поэтому естественно попытаться применить этот аппарат для моделирования и анализа динамики информационной борьбы, причем как в макромасштабе (например, государственной политики), так и на технологическом уровне.

Прежде всего при этом необходимо определить фазовое пространство, что является непростой и неоднозначно решаемой задачей. Тем не менее некоторые из фазовых переменных, скорее всего, должны быть в их составе. Трудно, например, обойтись при макромоделировании без учета уровня информатизации, развития информационно-коммуникационных технологий (ИКТ). Они инкорпорированы во все системы жизнеобеспечения и управления государства, регионов, производственные процессы, в большинство видов технических устройств и технологического оборудования, вошли в повседневный быт значительной части населения. Очевидно также, что информатизация сопровождается нарастанием и усложнением плохо решаемых, как показывает практика, проблем ИБ разного масштаба: от индивидуального до глобального. ИБ стала не просто структурной составляющей национальной безопасности (НБ), но неотъемлемо присутствует во всех ее аспектах. Поэтому переменная, выражающая уровень НБ, также должна присутствовать в модели.

Важность объективного анализа различных сценариев развития ситуации обусловлена ко всему прочему еще и тем, что существуют прак-

тически взаимоисключающие взгляды на стратегию развития ИКТ, а следовательно и на проблематику ИБ в России, хотя в последнее время оппозиционные декларируемой государственной политике позиции стали менее заметны. С одной стороны, прилагаются усилия по воссозданию импортозамещающего производства отечественной компонентной базы СВТ, коммуникационного оборудования, разработке ОС, без чего трудно говорить о поддержании приемлемого уровня НБ, во всяком случае в сфере государственного управления, обороны, функционирования критически важных систем и объектов, а с другой – утверждается неэф- ... мер при перенасыщенном глобальном рынке ...

правлений развития науки, технологий и техники в Российской Федерации направление «Информационно-телекоммуникационные системы», парадоксально мотивированные тем, что «Россия ... отстает от развитых стран по уровню научных исследований в области информационно-коммуникационных технологий». Причем все эти инициативы исходили от околоправительственных структур.

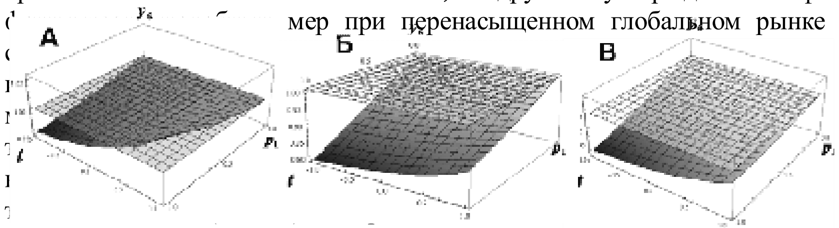
В первоначальной версии нашей модели [2], еще не включавшей процессы противоборства, в качестве содержательной основы была использована структурная схема [3], иллюстрирующая взаимодействие развития ИКТ и обеспечения НБ через систему других взаимообусловленно действующих факторов. Даже в образном виде она позволила видеть, что при отсутствии сбалансированности составляющих процесса, недооценке угроз, учитывая опосредованные обратные связи, национальной безопасности и в целом социально-экономическому развитию может быть нанесен ущерб. Для начала модель была представлена системой семи обыкновенных дифференциальных уравнений первого порядка следующего вида:

$$\dot{y} = P^T y + Q^T \dot{y},$$

где y – вектор фазовых переменных, в качестве которых выступают элементы указанной структурной схемы, в том числе уровни НБ, развития ИКТ, угроз НБ, социально-экономического развития; P, Q – матрицы коэффициентов, знак которых определяется направленностью действия факторов, в числе которых p_{ii} – диагональные элементы P, представляющие собственные потенциалы i-х факторов.

Для упрощения поиска области устойчивости значения коэффициентов фиксировались соответственно разным сценариям развития ситуации, а для проверки устойчивости использовался критерий Гурвица. Тестовые расчеты показали правдоподобное поведение модели в автономном режиме, что позволяет исследовать ее при различных сценариях управлений и более содержательном назначении коэффициентов.

На рисунке показаны некоторые результаты моделирования в виде трех диаграмм, где t – время, p_1 – потенциал развития ИКТ и y_6 – уровень НБ.



На диаграмме А представлен благоприятный вариант развития ситуации (положительный потенциал системы обеспечения НБ, $p_7>0$). Как видим, тогда уровень НБ (y_6) монотонно растет при достаточных потенциалах развития ИКТ (p_1) и системы обеспечения НБ.

Диаграмма Б – неблагоприятное развития ситуации (отрицательный потенциал системы обеспечения НБ, $p_7<0$) – показывает очевидное: любой вариант развития ИКТ при деградации системы обеспечения НБ приводит к резкому снижению уровня безопасности.

На диаграмме В – промежуточный вариант развития ситуации (нулевой потенциал системы обеспечения НБ). Стагнация системы обеспечения НБ, как и ее деградация (Б), в любом случае ведет не к фиксации, а к снижению уровня национальной безопасности.

Таким образом, построенная модель, несмотря на предельную простоту, дала правдоподобные результаты, показав возможность применения дифференциальных моделей для решения задач, подобных рассмотренной. Разумеется, интерпретация результатов почти очевидна и без расчетов на модели, но объективный инструмент всегда убедительнее вербальных доводов и подкрепляет их.

В последней версии данная модель существенно модифицирована, размерность фазового пространства в ней снижена, смысловое содержание переменных несколько переформулировано, введены ресурсы как источник управляющих воздействий, подключена симметричная система противника. В таком виде она позволит анализировать развитие ситуации для различных сценариев противоборства и находить оптимальные управления (выбор противодействий) как в режиме ис-

следования или прогноза, так и для выработки решений в реальном масштабе времени и способна послужить основой имитационной модели информационной борьбы.

Для целей моделирования информационной борьбы нами исследуются и другие типы моделей динамических систем, в частности с использованием физических аналогий, моделей популяционной динамики и др. Продолжается поиск наиболее подходящих для разных ситуаций вариантов фазового пространства борьбы в инфосфере и критериев управления.

1. Моисеев Н.Н. Универсум. Информация. Общество. М. : Устойчивый мир, 2011. 200 с.

2. Шишкин В.М., Абросимов И.К. Динамическая модель системы взаимодействия развития ИКТ и обеспечения национальной безопасности : материалы VIII С.-Петерб. межрегион. конф., Санкт-Петербург, 23–25 окт. 2013 г. СПб., 2013. С. 25.

3. Юсупов Р.М., Шишкин В.М. Информационно-коммуникационные технологии и национальная безопасность – противоречивая реальность // Информатизация и связь. № 1, 2010. С. 27–35.

РАЗДЕЛ 4

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

УДК 004.056.5

О.К. Барановский

ВЫБОР МЕР ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Объекты информатизации, отнесенные к критически важным, обеспечивают функционирование экологически опасных и (или) социально значимых производств и (или) технологических процессов, выполняют функции информационных систем и обеспечивают предоставление значительного объема информационных услуг в различных сферах национальной безопасности.

Вопросы обеспечения безопасности критически важных объектов информатизации (КВОИ) регулируются указами Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации», от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» и другими законодательными актами. Основным техническим нормативным правовым актом, регламентирующим порядок обеспечения безопасности, является ТКП 483-2013 (01019) «Информационные технологи и безопасность. Безопасная эксплуатация и надежное функционирование критически важных объектов информатизации. Общие требования».

Безопасность КВОИ обеспечивается реализацией комплекса мер технической и криптографической защиты информации, по обеспечению функциональной (технологической) безопасности и мер физической безопасности.

На современном этапе информатизации внедрение информационных технологий на КВОИ сопровождается объединением информационных сетей, сетей управления и мониторинга. Поэтому задача обеспечения безопасности КВОИ, заключающаяся в создании условий, при которых технологическая и информационная инфраструктура и информационные процессы защищены от максимально возможного числа

угроз и воздействий с нежелательными последствиям, становится еще более актуальной.

Внедряются новые подходы к обеспечению безопасности информации от угроз несанкционированного доступа с применением объектов информационных технологий. В результате создается не статичная система защиты информации, а запускается управляемый процесс постоянного анализа защищенности КВОИ и обрабатываемой информации, пересмотра и корректирования мер защиты. При этом необходимо использовать базовые наборы мер защиты информации, адаптируемые под конкретные объекты и изменяющийся ландшафт угроз.

Требования ТКП 483-2013 (01019) соответствуют зарубежным и международным методологическим подходам к обеспечению безопасности информации на объектах информатизации, обрабатывающих информацию, распространение и (или) предоставление которой ограничено, а также обеспечивающих функционирование государственных информационных систем и автоматизированных систем управления производственными и технологическими процессами (например, ISO/IEC 27001, проект приказа ФСТЭК России «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»).

Эффективность обеспечения безопасности информации основывается на адекватности модели угроз конкретного КВОИ и выбранной методологии оценки рисков от их реализации.

В связи с тем, что единая базовая модель угроз КВОИ в Республике Беларусь отсутствует, перед владельцем КВОИ и разработчиком системы защиты информации (системы безопасности в целом) стоит задача выбора и обоснования необходимого и достаточного комплекса мер защиты информации.

Базовые требования технической и криптографической защиты информации содержатся в комплексе предварительных стандартов, устанавливающих классификацию КВОИ (СТБ П 34.101.52-2012), соответствующие профили защиты (СТБ П 34.101.53,54,55,56,57,58-2012) и рекомендации по разработке задания по безопасности (СТБ П 34.101.59-2012). Срок действия предварительных стандартов – с 1 июня 2012 г. по 1 июня 2014 г.

Очевидно, что назначение и условия эксплуатации конкретных КВОИ могут определять невозможность или нецелесообразность реализации тех или иных мер защиты информации, в этом случае необходимо реализовывать компенсирующие меры безопасности. От компетентности владельца КВОИ и разработчика системы защиты информации (системы безопасности в целом) зависит учет всего спектра факторов, влияющих на реализацию угроз КВОИ.

Очевидно, что модель угроз КВОИ должна учитывать модель злоумышленника (его компетентность, техническую оснащенность). В условиях отсутствия такой информации эксперту практически невозможно определить, достаточно ли для реализации компенсирующих мер использовать обычные средства защиты информации в информационных системах, либо специально разрабатывать новые средства защиты информации, либо предпринимать дополнительные меры защиты.

На сегодня достаточно четкие указания по применению средств защиты информации установлены в части криптографической защиты информации (указ Президента Республики Беларусь от 16 апреля 2013 г. № 196, приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62 «О некоторых вопросах технической и криптографической защиты информации»). Не устанавливаются дополнительные требования к средствам технической защиты информации, применяемым на КВОИ.

Согласно ТКП 483-2013 (01019) решение о реализации тех или иных мер защиты принимается в результате применения методологии оценки рисков (СТБ ISO/IEC 27001-2011). В ходе выполнения данной процедуры оценивается риск причинения ущерба в результате реализации угроз активам КВОИ, важным для осуществления деятельности организации.

Предложен подход по оценке рисков на основе учета ценности (критичности) активов КВОИ для выполнения КВОИ функций его назначения. Оценка рисков может быть проведена в двух вариантах: с применением высокоуровнего или детального подхода. Сам процесс состоит из следующих этапов: идентификация активов КВОИ, идентификация угроз КВОИ, идентификация уязвимостей активов КВОИ, идентификация мер защиты, оценка вероятности реализации угроз, оценка влияния реализации угроз на выполнение КВОИ его функций, расчет и оценка рисков.

На основе предложенного подхода разработан и готовится к введению в действие проект государственного стандарта Республики Беларусь «Информационные технологии. Методы и средства безопасности. Методика оценки риска информационной безопасности в информационных системах».

Одновременно все еще актуальны вопросы, связанные с определением вероятностей угроз и оценкой их влияния на активы КВОИ.

В связи с вышеизложенным, учитывая особый статус КВОИ, наряду с такими объектами защиты, как объекты информатизации, предназначенные для обработки государственных секретов, для реализации единых подходов в обеспечении безопасности необходимо разработать и внедрить ряд документов, устанавливающих: базовую модель угроз безопасности КВОИ; базовый набор мер защиты информации; руководящие указания по выбору мер защиты информации.

УДК 519.876

Н.М. Бобович

ИСПОЛЬЗОВАНИЕ МЕТОДОВ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ПРИ ОЦЕНКЕ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Нормативные правовые акты, принятые на национальном уровне Республики Беларусь в последние годы, требуют осуществления таких мер обеспечения безопасности критически важных объектов информатизации (КВОИ), которые бы до минимума снижали как величину риска при воздействии на них дестабилизирующих воздействий, так и величину возможного ущерба [1, 2]. Одним из методов снижения риска до приемлемого уровня является управление риском (риск-менеджментом), по которым понимают процесс принятия и исполнения решений, направленных на снижение вероятности неблагоприятного результата и минимизацию возможных потерь. Начальным этапом такого управления является проведение экспертной оценки возможного риска, при которой вероятны ошибки или недостаточно полный учет отдельных факторов. Чтобы избежать ситуации, когда один и тот же эксперт осуществляет оценку и несет ответственность за принимаемые решения, оценка должна проводиться разными структурными подразделениями.

Устранение перечисленных недостатков возможно за счет оценки рисков путем проверки соответствия текущего состояния безопасности требованиям международных стандартов и национальных руководящих документов.

Однако на практике КВОИ функционируют в условиях различных случайных воздействий и возмущений, поэтому система защиты КВОИ может быть описана только стохастически, а воздействие дестабилизирующих воздействий можно описать только с некоторой вероятностью. Сами КВОИ являются достаточно сложными, и их исследование осуществляется с помощью системного подхода, который во многом базируется на моделировании реальных процессов, происходящих в системе.

Используются три основных вида моделей: эвристические, натурные и математические.

Эвристические модели представляют собой образы, которые возникают в сознании исследователя (например, при формировании требований к безопасности КВОИ на этапе проектирования).

Натурные модели – подобные реальные объекты в материальном смысле слова, отличаются по размерам, материалу элементов, внешних условий и т. д. (примером могут служить исследования электромагнитных излучений технических средств КВОИ в лабораторных условиях).

Математические модели представляют собой эквивалент объекта, отражающий в математической форме важнейшие его свойства – законы, которым он подчиняется, связи, присущие составляющим его частям, и т. д. [3].

Одним из частных случаев математического моделирования является имитационное моделирование, которое успешно используется в следующих случаях: отсутствует возможность построения аналитической модели; дорого или невозможно экспериментировать на реальном объекте; требуется сымитировать поведение системы во времени.

При имитационном моделировании различают две основные разновидности данного метода: метод имитационного моделирования (статистическое моделирование); метод Монте-Карло (статистическое испытание).

Наиболее распространенной программой имитационного моделирования является GPSS (General Purpose Simulation System – система моделирования общего назначения), которая появилась в 1961 г. [4]. Программа предназначена для моделирования систем массового обслуживания. Известными версиями являются – GPSS World (1993) и Micro-GPSS (2) (1996). Основным недостатком GPSS является плохая графическая интерпретация, что снижает наглядность создаваемой модели.

Другая известная программа MATLAB, по существу, представляет собой высокопроизводительный язык, используемый для технических расчетов, причем он используется для моделирования и в тех случаях, когда задачи выражаются в форме, близкой к математической. Приложение к MATLAB – пакет Simulink позволяет пользователю на экране монитора из библиотеки стандартных блоков и модулей создавать с помощью графических связей модель устройства или процесса, т. е. имитировать работу реального объекта. При этом пользователю достаточно общих знаний при работе на компьютере и знание той предметной области, к которой принадлежит моделируемый объект.

При разработке систем измерений, испытаний и управления достаточно эффективной является среда графического программирования LabView, которая программно совместима с MATLAB и Simulink и позволяет включать в имитационную модель различные датчики, созданные в среде LabView.

Язык программирования Visim предназначен для имитационного моделирования. Он сочетает в себе характерный для Windows интерфейс, позволяет создавать блочные диаграммы и мощное моделирующее ядро [5].

Перспективным методом имитационного моделирования является программный продукт AnyLogic, первая версия которого появилась в 2000 г. AnyLogic использует универсальный объектно-ориентированный подход (язык Java), а интерфейс разработан на визуальном подходе. Поэтому платформа поддерживает все способы моделирования систем: агентное моделирование, дискретно-событийное моделирование и системную динамику [6]. AnyLogic позволяет решать разнообразные задачи в области производства, образования, здравоохранения, финансов, управления рисками и т. п.

Имитационное моделирование КВОИ и его элементов может быть осуществлено с помощью системы имитационного моделирования Arena, которая включает следующие основные подсистемы: источники (Create); стоки (Dispose); процессы (Process); очереди (Quene). От источников в модель поступают данные (объекты) со скоростью, которая задается статистической функцией. Данные (объекты) после прохождения модели поступают в сток. В очереди данные (объекты) ожидают обработки перед тем, как попасть в некоторый процесс. Время обработки (производительность процесса) может быть разной и случайной. В итоге перед некоторыми процессами образуется очередь (из данных или объектов). Как правило, Arena используется для минимизации количества данных (объектов) в очереди, причем тип очереди может быть либо последовательным (первые пришедшие в очередь первыми идут в обработку), либо стековым (последние пришедшие в очередь первыми идут в обработку).

В имитационном моделировании для решения задач теории массового обслуживания эффективно используется метод Монте-Карло (ММК) [7], который основан на получении большого числа реализаций стохастического (случайного) процесса и формируется таким образом, чтобы его вероятностные характеристики совпадали с аналогичными величинами решаемой задачи. Прямое моделирование с помощью ММК какого-либо физического процесса подразумевает моделирование поведения отдельных частей исследуемой физической системы. Поэтому, например, ММК можно использовать для моделирования устойчивости функционирования элементов КВОИ за какой-то период.

При этом следует учитывать, что в таких случаях неизвестны (или известно приближенно) средние значения каких-то параметров моделируемого устройства, а также обычно неизвестны и законы распределения этих параметров. Поэтому при ММК делаются допущения, что закон распределения либо равномерен, либо нормален.

Проведенный выше анализ показывает, что универсального метода моделирования КВОИ для оценки текущего состояния их безопасности не существует. Поэтому целесообразно моделировать подсистемы КВОИ в отдельности, используя различные программные продукты по отдельности или в их комбинации.

1. О некоторых мерах по обеспечению безопасности критически важных объектов информатизации [Электронный ресурс] : указ Президента Республики Беларусь от 25 окт. 2011 г. № 486 // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. Минск, 2014.

2. О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации [Электронный ресурс] : постановление Совета Министров Республики Беларусь от 30 марта 2012 г. № 293 // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. Минск, 2014.

3. Самарский А.А., Михайлов А.П. Математическое моделирование. Идеи. Методы. Примеры : 2-е изд., испр. М. : Физматлит, 2002.

4. Томашевский В.Н., Жданова Е.Г. Имитационное моделирование в среде GPSS. М. : Бестселлер, 2003.

5. Дьяконов В.П. Визуальное математическое программирование VisSim+ Mathcad+ MATLAB. М. : Солон-Пресс, 2009.

6. Карпов Ю.Г. Имитационное моделирование систем. Введение в моделирование с AnyLogic СПб. : БХВ-Петербург, 2009.

7. Ермаков С.М. Метод Монте-Карло в вычислительной математике (Вводный курс). СПб. : Невский Диалект ; М. : БИНОМ. Лаб. знаний, 2009.

УДК 004.056

А.С. Дубровин, С.Ю. Хабибулина

МЕТОДОЛОГИЧЕСКИЙ ПОДХОД К ПРОБЛЕМЕ КОМПЛЕКСНОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ НА ОСНОВЕ ИХ ЭТАЛОННОГО МОДЕЛИРОВАНИЯ

Современный подход к решению проблемы комплексного обеспечения безопасности объектов информатизации поддерживается в Российской Федерации группой стандартов ГОСТ Р ИСО/МЭК 15408-2008 «Информационная технология. Методы и средства обеспечения безо-

пасности. Критерии оценки безопасности информационных технологий». Согласно этому подходу безопасный объект информатизации успешно противодействует заданным угрозам защищенности при заданных условиях его функционирования. Это приводит к постоянному совершенствованию как способов и средств защиты объектов информатизации, так и способов и средств реализации угроз их защищенности, в результате чего возникновение новых средств защиты приводит к появлению обходящих их угроз. Описанный современный подход в целом удовлетворителен для многих видов объектов информатизации. Однако его нельзя считать удовлетворительным для критически важных объектов информатизации (КВОИ). Безопасность таких объектов приоритетнее их функциональности.

Такое положение вещей приводит к необходимости новой трактовки понятия «безопасность КВОИ», под которой следует понимать отсутствие уязвимостей этих объектов, при наличии которых возможна реализация различных угроз защищенности. Это позволяет устранить ряд противоречий в определении противостояния средств защиты и угроз защищенности. При этом безопасность КВОИ должна характеризоваться их соответствием некоторым подлежащим стандартизации эталонным моделям безопасной (неуязвимой) обработки и передачи (циркуляции) информации. В связи с этим существует практическая проблема, состоящая в том, что подобное положение вещей лишь частично реализуется на практике и не находит прямого отражения в соответствующих стандартах на унифицированные архитектурные решения, удовлетворяющие общепринятым эталонным моделям циркуляции информации.

Причина лежит в принципиальных теоретических трудностях моделирования технологий комплексного обеспечения безопасности КВОИ, возникающих при попытке соединить перспективный подход к комплексному обеспечению безопасности КВОИ с гибкостью защитных механизмов. Природа этих трудностей в самом общем виде сводится к проблемной ситуации при моделировании процессов безопасной обработки информации в КВОИ, влияющих на защиту информации, которая может быть определена как противоречие между динамическим, локальным и дискретным рассмотрением при моделировании неуязвимости КВОИ и статическим, глобальным и непрерывным – при моделировании гибкости защитных механизмов.

Разрешение проблемной ситуации означает обеспечение на уровне моделей как недопущения уязвимостей информации в процессе ее обработки на КВОИ, так и применение гибких защитных механизмов. Это невозможно в рамках традиционной «аналитической» общенаучной парадигмы. Предлагаемый методологический подход предусматривает для этого системную интеграцию математических моделей обработки и

защиты информации, соединяющую неуязвимость и гибкость по каждому из трех аспектов комплексного обеспечения безопасности информации (конфиденциальность, доступность и целостность) в КВОИ на основе конструктивной унификации указанных противоречий.

В плане конфиденциальности и доступности информации гибкость защитных механизмов означает гибкость разграничения доступа к информации, а уязвимости кроются в модели используемой политики безопасности (ПБ) и в ее практической реализации. Единственной подлинно гибкой является дискреционная модель ПБ, которая неизбежно порождает уязвимости. С другой стороны, единственным неуязвимым является класс моделей конечных состояний, берущий свое начало от мандатного метода контроля доступа. Однако возможности применения существующих моделей конечных состояний весьма ограничены ввиду их принципиальной негибкости. Этот недостаток данного класса моделей можно устранить, сблизив его с дискреционной моделью. Но этому мешает естественное для «аналитической» общенаучной парадигмы традиционно независимое рассмотрение процессов защиты информации от процессов обработки информации, а отход от этого принципа требует масштабных и глубоких научных исследований, начало которым было положено в рамках созданного нами научного направления, получившего название «Эталонная модель защищенной автоматизированной системы (ЭМЗАС)».

В соответствии с используемым нами системным подходом к комплексному обеспечению безопасности КВОИ ЭМЗАС как идеализированная модель КВОИ реализует технологию неуязвимой обработки и передачи информации. Такая модель обеспечивает возможность стандартизации унифицированного архитектурного облика различных классов КВОИ путем разработки и регистрации по регламентации ГОСТ Р ИСО/МЭК 15408-2008 необходимого набора профилей защиты, полное соответствие КВОИ которым означает их эталонность в смысле ЭМЗАС.

Регламентируемые ЭМЗАС модели комплексов ПБ, соединяя существо моделей конечных состояний с дискреционной формой, предусматривают, что любой дискреционный доступ в КВОИ может реализовываться только однозначно определяемой последовательностью переходов между конечными состояниями, для которой можно гарантировать неуязвимость КВОИ. Методологические принципы достижения этого следующие: обеспечение необходимого разделения информационных процессов, реализующих различные дискреционные доступы, для устранения их взаимовлияния; обеспечение контролируемой однозначной реализации каждого отдельно взятого дискреционного доступа.

Данные принципы реализуются за счет представления произвольного дискреционного доступа, имеющего многоуровневый характер. При этом ограничения глобальной ПБ задаются согласно обычной дискреционной модели, а ограничения локальной ПБ – как полномочия доступа данной авторизации между субъектами соседних уровней в направлении сверху вниз. Иерархическая структуризация информационных ресурсов КВОИ, обеспечивающая единство рассмотрения глобальной и локальной ПБ ЭМЗАС, предусматривает 15 уровней как расширение известной 7-уровневой модели OSI в направлении декомпозиции ее прикладного уровня. Нижние шесть уровней ЭМЗАС одноименны нижним шести уровням OSI, а остальные уровни ЭМЗАС следующие: информационный (7), менеджерский (8), прикладной (9), серверный (10), навигационный (11), диспетчерский (12), интеграционный (13), идентификационный (14) и административный (15).

Теоретической базой реализации монитора обращений в эталонной КВОИ служит известная концепция изолированной программной среды (ИПС). Она является дальнейшим развитием классической общепризнанной концепции ядра безопасности, основанной на субъектно-объектной модели КВОИ, в направлении учета порождений субъектов. Если концепция ядра безопасности направлена на решение задачи реализации произвольно заданной ПБ, то концепция ИПС – на решение задачи гарантирования произвольно заданной ПБ.

Концепция эталонной КВОИ в смысле ЭМЗАС развивает концепцию ИПС в направлении регламентации комплекса ПБ ЭМЗАС. Назначением концепции эталонной КВОИ является реализация заданной локальной ПБ ЭМЗАС, что обеспечивает единство рассмотрения динамического и статического доступа к информации. Способом реализации данной концепции является организация в КВОИ ИПС, отвечающей специальному перечню требований к ее субъектному наполнению. Такой перечень из восьми требований сформирован и обоснован на основе разработанного принципиального облика комплекса ПБ ЭМЗАС, позволяющего гарантировать глобальную ПБ посредством реализации индуцирующей ее локальной ПБ. Построена концепция организации субъектного наполнения эталонной объектно-реляционной СУБД с детализацией данных требований, позволяющая использовать объектно-реляционные технологии в эталонных КВОИ.

Основными средствами реализации концепции эталонной КВОИ являются уровневые комплексы сервисов безопасности (КСБ). Уровневый КСБ включает уровневые: объект управления; сервис контроля целостности информации; монитор безопасности, состоящий из монитора безопасности объектов и монитора безопасности субъектов. Уровневый контроль целостности информации применяется ко всем

объектам-источникам для информационного процесса данного уровня с использованием объекта, хранящего эталонное состояние этих объектов-источников.

Эталонная КВОИ представляет собой подобие слоеного пирога, где информационные процессы, организованные в соседние функциональные уровни иерархической структуризации ресурсов ЭМЗАС, разделяются соответствующими уровневыми КСБ, которые являются контролирующими посредниками при взаимодействии информационных процессов, относящихся к соседним уровням ЭМЗАС. Создание нормативной базы реализации концепции эталонной КВОИ требует такого подхода к стандартизации унифицированного архитектурного облика различных классов эталонных КВОИ, который предусматривает стандартизацию их уровневых интерфейсов в форме стандартизации интерфейсов сопряжения информационных процессов данного уровня ЭМЗАС с соседними с ними уровневыми КСБ. При таком подходе к стандартизации КВОИ могут строиться из отдельных программных блоков, гарантированно «плотно прилегающих» друг к другу без образования уязвимостей. Их можно комплектовать в постепенно расширяемую библиотеку ЭМЗАС-классов наподобие базовой библиотеки классов технологии dot net.

УДК 342.951

А.В. Калиберов

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТАМОЖЕННЫХ ОРГАНОВ РЕСПУБЛИКИ БЕЛАРУСЬ В УСЛОВИЯХ ТАМОЖЕННОГО СОЮЗА

Условия, в которых приходится и придется работать таможне в ближайшее десятилетие, характеризуются в документах Всемирной таможенной организации комбинацией ряда факторов: стремительно развивающиеся информационные и коммуникационные технологии, новые технологии доставки товаров и либерализация торговли, растущая угроза международного терроризма, появление новых схем коммерческого мошенничества.

Таможенный кодекс Таможенного союза – основной правоустанавливающий документ, обеспечивающий таможенное регулирование в Таможенном союзе и непосредственно влияющий на внешнюю торговлю и другие формы внешнеэкономической деятельности государств – членов Таможенного союза заработал 6 июля 2010 г. После вступления в силу данного кодекса принципиально изменилась система законода-

тельства, регулирующего таможенные правоотношения в республике: теперь ее основу составляют международные договоры государств – членов Таможенного союза и решения Комиссии Таможенного союза, таможенное законодательство Республики Беларусь применяется только в части, отнесенной к его компетенции Таможенным кодексом Таможенного союза и международными договорами, а также в части, не урегулированной таможенным законодательством Таможенного союза.

На сегодня функционирование Таможенного союза невозможно без эффективного использования общих информационных ресурсов, свободного доступа к ним таможенных служб государств – членов Таможенного союза, надежного информационно-технического обеспечения общих таможенных процессов. Перспективным направлением развития становится участие в интеграции национальных информационных систем в рамках Таможенного союза.

В качестве основных причин, обусловливающих актуальность вопросов обеспечения информационной безопасности на единой таможенной территории Таможенного союза, их научной проработки, являются:

объединение в единое информационное пространство деятельности таможенных органов государств – участников Таможенного союза, включая сопряжение их информационных систем;

динамичное развитие информационных технологий в таможенном деле, которые требуют новых адаптированных к ним подходов по обеспечению безопасности информации;

специфика закрытости технологий и средств защиты конфиденциальной информации таможенных органов, включая национальную государственную тайну;

особенности финансирования деятельности по обеспечению безопасности информации в условиях Таможенного союза.

Анализ подходов государств – участников Таможенного союза в решении задач по обеспечению безопасности информации показал, что они имеют в целом одни и те же взгляды на эту сферу деятельности. В Таможенном кодексе Таможенного союза отражены положения по регулированию деятельности таможенных органов в сфере обеспечения безопасности информации, в частности этим вопросам посвящена гл. 4 «Информационные системы и информационные технологии», ст. 8, 16, 21, 47, 57, 101, 102, 134, 136.

Однако при реализации указанных положений необходимо решение некоторых вопросов. Объединение в Таможенный союз таможенных органов создало новую обстановку, в которой появляются общие сферы деятельности, требующие согласования друг с другом, в том числе

в информационной сфере, для которой также необходимо обеспечить информационную безопасность.

В структуре законодательства, регулирующего вопросы обеспечения информационной безопасности, особое значение имеют концептуальные политические документы, в Республики Беларусь к важнейшим из которых надо отнести Концепцию национальной безопасности Республики Беларусь (утверждена указом Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь»).

В деятельности таможенных органов Республики Беларусь таким правовым актом является Концепция информационной безопасности таможенных органов Республики Беларусь, утвержденная в 2006 г. решением Коллегии Государственного таможенного комитета Республики Беларусь.

Концепция определила систему взглядов на проблему обеспечения информационной безопасности прежде всего в автоматизированных информационных системах, составляющих Единую автоматизированную информационную систему таможенных органов Республики Беларусь, а также в таможенных органах в целом.

Однако вступление в силу ряда правовых актов, таких как Договор о Таможенном кодексе Таможенного союза (подписан в Минске 27 ноября 2009 г.), Протокол о внесении изменений и дополнений в Договор о Таможенном кодексе Таможенного союза от 27 ноября 2009 г. (подписан в Москве 16 апреля 2010 г.), принятие закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации», подписание Президентом Республики Беларусь указа № 575 от 9 ноября 2010 г. «Об утверждении Концепции национальной безопасности Республики Беларусь», требует координальной переработки положений Концепции информационной безопасности таможенных органов Республики Беларусь с учетом изменений национального законодательства, положений Таможенного кодекса Таможенного союза, а также с учетом соглашений, договоров, протоколов, заключенных в рамках Таможенного союза, решений Межгосударственного Совета Евразийского экономического сообщества, решений Комиссии Таможенного союза.

Концепция должна стать методологической основой для формирования и проведения единой политики в области обеспечения безопасности таможенных органов в условиях Таможенного союза; разработки практических мер по воплощению политики безопасности информации и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации.

УДК 681.586

А.Н. Коваленко

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ПРИБОРОВ КОНТРОЛЯ МИКРОДВИЖЕНИЙ В ОХРАНЕ ОБЪЕКТОВ

К приборам контроля микродвижений относится широкий класс специализированной радиоизмерительной аппаратуры, применяемой во многих областях мировой промышленности для контроля микровибрации, микросейсм, отдельных параметров механического движения, характеризующих состояние сооружений, машин, исследовательского и технологического оборудования, подземных масс, биологических и других объектов. В настоящее время в нашей стране серийно выпускаются измерительные преобразователи, усилительная и анализирующая аппаратура, контрольно-сигнальные приборы, средства метрологические обеспечения.

Известно довольно большое число физических явлений, которые предлагаются для измерительного преобразования параметров движения. Примером использования некоторых из них могут служить технические средства охраны, которые применяются для обнаружения нарушителя путем неконтактного контроля его движений:

емкостные, принцип действия которых основан на изменении электрической емкости чувствительного элемента при движении объекта обнаружения;

радиолокационные, основанные на модуляции движущимся объектом высокочастотного электромагнитного поля;

ультразвуковые, которые построены на использовании принципа изменения структуры ультразвукового поля, названного появлением объекта;

инфракрасные, использующие принцип прерывания узконаправленного инфракрасного луча телом нарушителя;

вибрационные, принцип действия которых основан на восприятии колебаний упругой среды, вызванных перемещениями объекта.

Выбор конкретных средств для контроля движений во многом зависит от диапазона изменения контролируемого параметра как по амплитуде, так и по частоте.

Микродвижения определяются предельно малыми значениями параметров, которые сведены в таблицу.

Значения параметров микродвижений

Параметр	Диапазон значений
Поступательное перемещение, мкм	10^{-2}–10^{3}
Поступательная скорость, м/с	10^{-9}–10^{-4}
Поступательное ускорение, м/с^2	10^{-6}–10^{-2}
Угловое перемещение, рад	10^{-6}–10^{-4}
Угловая скорость, рад/с	10^{-5}–10^{-3}
Угловое ускорение, рад/с^2	10^{-4}–10^{-2}

Для оценки приборов неконтактного контроля микродвижений особое значение имеют показатели эффективности преобразования очень малых значений параметров при наличии помех. Основным критерием эффективности первичных измерительных преобразователей следует считать порог чувствительности. Этот показатель, отражая отношение полезного сигнала к помехам, наилучшим образом характеризует способность прибора правильно осуществлять контроль микродвижений.

Емкостные преобразователи являются высокочувствительными преобразователями малых перемещений. Они позволяют проводить технический контроль поступательных перемещений – порядка десятых долей минуты.

Рассчитано, что при условии защиты емкостного преобразователя от помех и подавлении шумов генератора минимальное контролируемое перемещение в полосе частот 1Гц может составить 10^{-12}м.

К числу других достоинств емкостных преобразователей относятся простота, малые габариты и масса, малая инерционность и незначительное обратное воздействие на объект контроля.

Исключительная возможность модификации чувствительного элемента емкостных преобразователей, в качестве которого может использоваться любое электропроводящее тело, простота создания объемной зоны чувствительности весьма больших размеров и заданной конфигурации делают особенно целесообразными разработки преобразователей с неэкранированным чувствительным элементом для контроля микродвижений активным методом в открытой среде и в труднодоступных местах.

На основе емкостного принципа преобразования микродвижений в нашей стране и за рубежом непрерывно развиваются технические средства охраны, устанавливаемые как внутри помещений, так и на периметрах охраняемых объектов. При этом большое внимание уделяется вопросам повышения устойчивости емкостных устройств, размещаемых на открытом пространстве и подвергающихся воздействию электрических помех и различных климатических факторов. В частности, осадки или увеличение влажности воздуха могут оказывать боль-

шое влияние на места крепления проводов чувствительного элемента, снижая чувствительность емкостного преобразователя и вызывая ложные сигналы тревоги в системе охраны. Электромагнитные поля от посторонних источников воздействуют на приемный электрод неэкранированного чувствительного элемента как на приемную радиоантенну, вызывая паразитную модуляцию электрического сигнала, индуцируемого генераторным электродом.

УДК 351.74(477):(004.7)

В.А. Кудинов

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНОГО ОБЪЕКТА ИНФОРМАТИЗАЦИИ – ИНТЕГРИРОВАННОЙ ИНФОРМАЦИОННО-ПОИСКОВОЙ СИСТЕМЫ ОРГАНОВ ВНУТРЕННИХ ДЕЛ УКРАИНЫ

С начала процесса информатизации органов и подразделений внутренних дел Украины прошло уже более 40 лет. За это время накоплен большой опыт использования различных информационных и информационно-телекоммуникационных систем оперативно-розыскного и информационно-справочного назначения, в которых неоднократно происходили изменения информационных процессов в связи с периодическим обновлением средств оргтехники и информационных технологий.

С целью выполнения указа Президента Украины от 20 октября 2005 г. № 1497 «О первоочередных задачах по внедрению новейших информационных технологий» в Министерстве внутренних дел Украины в последние годы принимаются меры по созданию и внедрению различных интегрированных информационно-аналитических систем. В настоящее время наиболее применяемой в Украине является Интегрированная информационно-поисковая система (ИИПС) ОВД, которая функционирует с 2009 г. Положение о ИИПС ОВД Украины было утверждено приказом МВД Украины от 12 октября 2009 г. № 436. В системе авторизации ИИПС на сегодня зарегистрировано более 27 тыс. пользователей – работников ОВД.

Целью создания данной системы является объединение существующих в ОВД Украины информационных ресурсов в единый информационно-аналитический комплекс с использованием современных информационных технологий, компьютерного и телекоммуникационного оборудования для поддержки оперативно-служебной деятельности ОВД, существенного укрепления их способности противодействия и профилактики преступности.

Интегрированная информационно-поисковая система ОВД Украины – это совокупность организационно-распорядительных мероприятий, программно-технических и информационно-телекоммуникационных средств, которые обеспечивают формирование и ведение информационно-справочных, оперативно-розыскных учетов, авторизованный доступ к информационным ресурсам ИИПС. Информационные массивы системы составляют более 15 баз данных (например, «Факт»; «Преступление»; «Лицо»; «Розыск»; «Мигрант»; «Административное правонарушение»; «Коррупционное правонарушение»; «Угон»; «Криминальное оружие»; «Зарегистрированное оружие»; «Вещи», «Потерянные документы»; «Электронный рапорт»), которые содержат значительные объемы информации и обеспечивают оперативно-служебную деятельность всех органов внутренних дел Украины.

Известно, что в рамках работ в области критически важных объектов, которые проводятся в Республике Беларусь, был подписан указ Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации». Указом утверждено Положение об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации. В соответствии с этим положением к критически важным объектам информатизации относятся также такие объекты, которые осуществляют функции информационной системы, нарушение штатного режима которой может привести к значительным негативным последствиям для национальной безопасности в разных сферах (в том числе информационной); обеспечивают предоставление значительного объема информационных услуг, частичное или полное прекращение оказания которых может привести к значительным негативным последствиям для национальной безопасности в разных сферах (в том числе информационной). Так как нормальное функционирование ИИПС ОВД обеспечивает государственную, общественную и информационную безопасность, которые входят в структуру национальной безопасности, ее также необходимо отнести к критически важным объектам.

А защита критически важных объектов представляет собой одну из наиболее важных задач обеспечения национальной безопасности любой страны. При этом защита критически важных объектов включает проведение мероприятий, которые должны обеспечить их сохранение в случае различных внутренних и внешних воздействий.

Структура ИИПС ОВД построена по 3-уровневой иерархической модели, соответствующей организационной структуре МВД Украины. Внедрение этой системы позволило в режиме реального времени получать доступ к информационным ресурсам ОВД Украины, осуществлять обработку информации непосредственно в горрайлинорганах, форми-

ровать обобщенные информационные ресурсы на областном и центральном уровнях МВД Украины. Обмен информацией между территориально удаленными структурными подразделениями ОВД и доступ пользователей к ИИПС обеспечивается средствами единой цифровой телекоммуникационной сети МВД Украины и локальных вычислительных сетей ОВД.

Таким образом, комплексная система защиты информации (КСЗИ) должна обеспечить на каждом уровне ИИПС ОВД Украины действие информационных систем класса 2, а функционирование ИИПС ОВД Украины в целом – как информационной системы класса 3, т. е. КСЗИ в ИИПС ОВД должны объединить в единую систему все необходимые меры и средства защиты от различных угроз безопасности информации на всех этапах ее жизненного цикла.

На сегодняшний день в состав территориальных узлов ИИПС ОВД входят автоматизированные рабочие места (АРМ), которые обеспечивают авторизованный доступ пользователей ИИПС горрайлинорганов к формированию и использованию информационных ресурсов регионального узла ИИПС ОВД. При этом в ИИПС для пользователей устанавливаются четыре уровня доступа к информационным ресурсам системы и один уровень для внесения информации в соответствующие базы данных системы.

А в состав центрального и региональных узлов ИИПС входят: АРМ администратора узла ИИПС, который является составной частью КСЗИ узла и предназначенный для мониторинга системных журналов регистрации работы программно-технических средств, анализа нарушений в работе системы, настройки параметров, которые необходимы для обеспечения стабильной работы программно-технических средств узла; АРМ администратора безопасности, которые являются составной частью КСЗИ узла и предназначены для реализации технологии предоставления пользователям доступа к информации в ИИПС (в соответствии с предоставленными распорядителем ИИПС правами доступа), мониторинга системных журналов регистрации работы пользователей и программных средств; АРМ криптографической защиты, которые являются составной частью КСЗИ узлов системы и предназначены для реализации технологии электронной цифровой подписи в ИИПС; АРМ, которые обеспечивают авторизованный доступ пользователей ИИПС к информационным ресурсам узлов ИИПС.

Для дальнейшего совершенствования обеспечения безопасности информационных ресурсов ИИПС ОВД можно выделить ряд первоочередных организационных и программно-аппаратных мероприятий:

1. Постоянное проведение комплекса мероприятий для поддержания нормального функционирования программно-аппаратных средств ИИПС ОВД.

2. Создание действенного резерва программно-аппаратных средств ИИПС ОВД.

3. Обеспечение надежного хранения резервных копий информационных массивов ИИПС ОВД.

4. Ограничение доступа посторонних лиц к информационным ресурсам путем построения ряда зон защиты, в которых функционируют соответствующие средства охраны.

5. Обеспечение постоянного мониторинга действий пользователей ИИПС ОВД, что позволит своевременно выявлять нарушения во время их работы с объектами защиты.

6. Повышение требований к подбору персонала ИИПС ОВД.

7. Ограничение возможности ознакомления посторонних лиц с работой и документацией объектов защиты ИИПС ОВД.

8. Принятие мер дисциплинарного воздействия к пользователям ИИПС ОВД, которые предоставляют свои логины и пароли другим лицам (в частности, своим подчиненным).

9. Периодическое повышение квалификации персонала ИИПС ОВД, проведение практических тренингов с пользователями системы по работе с объектами защиты (особенно после программно-аппаратного обновления системы) и другие мероприятия.

УДК 327.37

А.М. Кузьмицкий

ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМЕ ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ ИСПОЛЬЗОВАНИЯ АТОМНОЙ ЭНЕРГИИ

На этапе строительства Белорусской атомной электростанции представляется целесообразным предложить отдельные аспекты по защите информации в системе ее физической защиты (СФЗ). Попытки несакционированного доступа при этом могут осуществляться, например, к пунктам управления СФЗ и другим жизненно-важным объектам информатизации или субъектам, эксплуатирующим СФЗ. Непосредственной угрозе могут подвергаться такие виды информации, как речь, побочные электромагнитные излучения, визуальное изображение.

В целях обеспечения комплексной безопасности информации физической защите подлежат жизненно-важные объекты информатизации:

центральный пункт управления (ЦПУ) СФЗ;

локальные пункты управления (ЛПУ) СФЗ;

помещения, в которых хранятся носители информации (хранилища);

узлы связи;

оконечные терминальные устройства и автономные средства, использующие микропроцессорную технику и реализующие отдельные элементы подсистем СФЗ;

коммуникации СФЗ и системы электропитания (трансформаторные подстанции, автономные источники).

Помещения ЦПУ и его «серверной» размещаются в зонах ограниченного доступа, находящихся в пределах внутренней или особо важной зон. Доступ в эти помещения должен регулироваться автоматизированной системой контроля управления и доступом (СКУД) и быть строго дифференцирован по выполняемым функциям персонала.

Помещение «серверной», не требующее постоянного присутствия обслуживающего персонала, в дополнение к оконечным устройствам СКУД оборудуется техническими средствами охраны в соответствии с высшей категорией охраняемых объектов и высшей степенью секретности обрабатываемой и хранимой информации, но не менее чем двумя рубежами охранной сигнализации с разными физическими принципами действия. Информация баз данных СФЗ дублируется, и одна из копий должна быть помещена в хранилище носителей информации, обслуживающее ЦПУ.

Помещения ЛПУ должны размещаться в специально приспособленных для этого зонах ограниченного доступа, находящихся в пределах защищенной или одной из внутренних зон в зависимости от зоны обслуживания или функционального назначения локальной АС.

Вход и выход из этих помещений должен регулироваться автоматизированной СКУД. Обслуживание ЛПУ и его «серверной» обеспечивается персоналом охраны АЭС, назначаемым для каждой конкретной зоны обслуживания совместно со специалистами подразделений, обеспечивающих бесперебойное функционирование средств вычислительной техники, связи, электропитания, кондиционирования и т. п.

Узлы связи, коммутаторы оперативной связи или АТС малой емкости, сети телефонной и радиосвязи СФЗ, распределительное и коммуникационное оборудование также размещаются в пределах защищенной зоны в зонах ограниченного доступа, оборудованных автономными средствами или оконечными терминальными устройствами подсистемы управления и контроля доступа или защищенных от несанкционированного вскрытия техническими средствами охраны.

Коммуникации СФЗ (информационные кабели, кабельные колодцы и распределительные шкафы) выполняются в защищенном исполнении, в том числе с использованием сигнализации на вскрытие.

Эффективность защиты речевой информации, составляющей государственную тайну, должна соответствовать действующим нормам

безопасности информации в зависимости от установленной категории помещений пунктов управления СФЗ, в которых устанавливаются только системы телефонной связи, радиотрансляции, оповещения, сигнализации и электрочасофикации, сертифицированные по требованиям безопасности информации. Должна быть проведена проверка эффективности защиты этих устройств в реальных условиях их размещения, по результатам определяется необходимость применения дополнительных мер защиты.

Оконечные устройства этих систем, имеющие выход за пределы защищенной зоны АЭС, должны быть защищены от утечки информации за счет электроакустических преобразований. Средства защиты также должны быть сертифицированы.

Звукоизоляционные характеристики ограждающих конструкций и технологического оборудования защищаемого помещения должны соответствовать установленным нормам акустической защиты речевой информации.

Необходимо исключить передачу по незащищенным каналам проводной и радиосвязи информации, составляющей государственную и служебную тайну. Это осуществляется за счет жесткой регламентации характера и содержания передаваемых сообщений. Такого рода информация должна передаваться только по защищенным каналам связи либо с использованием средств криптографического преобразования.

Для обработки информации, составляющей государственную тайну, должны применяться средства вычислительной техники (СВТ), сертифицированные по требованиям безопасности информации, либо образцы техники, прошедшие проверку эффективности защиты информации в реальных условиях их размещения.

Размещение и монтаж технических средств, предназначенных для вывода защищаемой информации (печатающие устройства, видеотерминалы, графопостроители и т. п.), необходимо проводить с учетом максимального затруднения визуального просмотра информации посторонними лицами, а также принимать дополнительные меры, исключающие подобный просмотр (шторы на окнах, жалюзи, непрозрачные экраны и т. п.).

Прокладку соединительных линий средств оптико-электронного наблюдения (СОЭН) и оценки ситуации необходимо выполнять экранированным, надлежащим образом заземленным кабелем с учетом исключения возможности гальванического подключения к ним.

В случае если в состав СОЭН включены устройства вычислительной техники, обрабатывающие информацию в цифровом виде, их защита должна осуществляться в соответствии с требованиями по защите информации, обрабатываемой СВТ.

При использовании маскируемого оборудования или его элементов в рубежах охраны СФЗ, скрытии принципов функционирования инженерно-технических средств системы должны быть обеспечены меры их защиты от фотографических и оптико-электронных средств разведки.

Эффективность принимаемых мер защиты должна соответствовать действующим нормативным документам по противодействию фотографическим и оптико-электронным средствам разведки.

Основными мероприятиями по защите информации в СФЗ от таких средств являются: использование маскирующих свойств местности, условий ограниченной видимости; применение ложных сооружений и маскировочных конструкций; пространственные ограничения, направленные на исключение контакта между средствами разведки и защищаемым объектом.

Все вышеперечисленные мероприятия используются на различных этапах жизненного цикла системы физической защиты АЭС.

УДК 34:002

А.Н. Лепёхин, Д.В. Перевалов

НОРМАТИВНОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

В рамках регулирования информационных правоотношений, в частности правовой регламентации функционирования критически важных объектов информатизации, авторским коллективом разрабатывается целостный пакет проектов нормативных правовых актов в данной сфере. Предполагается, что принятие и реализация актов законодательства, направленных на регулирование информационных правоотношений, обеспечит повышение качества принимаемых нормативных правовых актов в сфере информационной безопасности, защищенность информационных интересов граждан, общества и государства придаст адресность государственной информационной политике, что, в свою очередь, повысит эффективность ее реализации.

Основу указанного пакета нормативных правовых актов составляет проект модельного закона «О критически важных объектах информационно-коммуникационной инфраструктуры» (далее – законопроект), который разрабатывается в соответствии с Межгосударственной программой совместных мер борьбы с преступностью на 2014–2018 годы, утвержденной решением Совета глав государств СНГ 25 октября 2013 г.

Законопроект непосредственно основывается на Модельном информационном кодексе для государств – участников СНГ, модельных

законах «Об информации, информатизации и защите информации» и «О международном информационном обмене», Рекомендациях по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности, а также учитывает положения нормативных правовых актов государств – участников СНГ: закона Азербайджанской Республики от 3 апреля 1998 г. № 460-IQ «Об информации, информатизации и защите информации»; закона Республики Армения от 17 февраля 1998 г. «О телекоммуникации»; закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»; закона Республики Казахстан от 5 июля 2004 г. № 567-II «О связи»; законов Республики Молдова от 22 июня 2000 г. «Об информатике» и от 3 февраля 2009 г. «О предупреждении и борьбе с преступностью в сфере компьютерной информации»; федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации», законов Украины от 5 июля 1994 г. № 80/94-ВР «О защите информации в информационно-телекоммуникационных системах» и от 18 ноября 2003 г. № 1280-IV «О телекоммуникациях»; указа Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации»; указа Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

Необходимость разработки законопроекта обусловлена, во-первых, увеличением числа критически важных объектов в системе объектов информационно-коммуникационной инфраструктуры государств – участников СНГ; во-вторых, повышением уровня опасности последствий для государства, общества и отдельных лиц в случае нарушения (прекращения) нормального функционирования критически важных объектов информационно-коммуникационной инфраструктуры; в-третьих, расширением спектра угроз безопасности таких объектов, изменением их характера и интенсивности, в-четвертых, отсутствием в большинстве государств – участников СНГ нормативно закрепленных основ деятельности по обеспечению нормального функционирования критически важных объектам информационно-коммуникационной инфраструктуры, а также по предупреждению, выявлению и локализации угроз их безопасности.

Основной целью подготовки законопроекта является выработка новой согласованной политики на пространстве СНГ в сфере информационной безопасности, гармонизация законодательных решений государств – участников СНГ в области обеспечения безопасности крити-

чески важных объектов информационно-коммуникационной инфраструктуры. Основными задачами при этом являются:

установление единых (общих) основных положений законодательства в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры, обеспечивающих регулятивную мобильность уполномоченных государственных органов государств – участников СНГ;

определение общих положений правового статуса субъектов обеспечения безопасности таких объектов;

выработка механизма установления эквивалентности и взаимного согласования систем обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры в государствах – участниках СНГ;

формирование единой, скоординированной и сопряженной системы правовых, организационных, инженерно-технических, программно-аппаратных и специальных мер обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры в государствах – участниках СНГ.

Таким образом, принятие законопроекта позволит создать эффективные организационно-правовые механизмы, обеспечивающие формирование и развитие системы обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры. Кроме того, данное действие позволит обеспечить комплексную реализацию положений Стратегии сотрудничества государств – участников СНГ в построении и развитии информационного общества, а также предусмотреть действенную систему мер интеграционного сотрудничества государств – участников СНГ в рамках сближения законодательства в сфере обеспечения информационной безопасности.

УДК 681.51

А.А. Матвеев

ПРОБЛЕМНЫЕ ВОПРОСЫ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Повсеместное внедрение широкого спектра информационных технологий в системы управления производственными и технологическими процессами обеспечивает развитие всех сфер государственной и экономической жизни страны. В то же время безопасность коммуникационных сетей и информационных систем, особенно их работоспособность и отказоустойчивость, стала крайне актуальной темой для общества. Эта тревога объясняется риском появления проблем в критически важных информационных системах, которые могут возникнуть из-за их сложности, а также из-за атак на инфраструктуры, предоставляющие критические сервисы. В четверку наиболее опасных и подверженных угрозам отраслей входят энергетика, нефтегазовая сфера, транспорт и водоснабжение. на безопасность критически важных объектов информатизации (КВОИ) являются:

интеграция в единые комплексы автоматизированных систем управления (АСУ) информационных систем, используемых в управлении производственными и транспортными структурами, административными и финансовыми ресурсами;

рост числа противоправных деяний с использованием информационных и коммуникационных технологий;

постоянное усложнение программного обеспечения и оборудования, используемых в АСУ;

вынужденная технологическая зависимость от иностранных компаний-производителей и поставщиков программно-аппаратных средств обработки, хранения и передачи информации, привлекаемых к созданию АСУ КВОИ;

стремление организаций – разработчиков программного обеспечения АС к снижению издержек и, как следствие, к использованию типовых решений и заимствованного программного обеспечения;

отсутствие достаточного нормативно-правового регулирования процессов обеспечения безопасности АСУ КВОИ, в том числе в части определения уровня их реальной защищенности и ответственности за нарушение требований по обеспечению безопасности КВОИ.

Кроме того, требования нормативных правовых актов предоставляют право владельцам объектов информатизации отнесения их к критически важным на основе отраслевых критериев. Это связано с тем, что в каждой отрасли существует своя специфика задач обеспечения безопасности. В то же время анализ сведений об имеющихся в структуре государственных органов и иных организаций объектах информатизации показывает, что значительную часть данных объектов не представляется возможным отнести к критически важным в соответствии с существующей процедурой, хотя они оказывают существенное влияние на отдельные отрасли Республики Беларусь (системы управления технологическими процессами банковской сферы, транспортной системы и др.). Владелец такого объекта нередко просто не понимает, что его система критически важная, а иногда старается самоустраниться по причине нежелания вкладывать средства в обеспечение необходимого уровня защищенности.

Учитывая изложенное, требуется совершенствование законодательства в сфере обеспечения безопасности критической инфраструктуры Республики Беларусь.

Также хотелось бы отметить, что направление безопасности КВОИ развивается на предприятиях медленнее, чем совершенствуются применяемые информационные системы. В первую очередь это связано с дополнительными расходами на защиту систем управления, а также с уровнем квалификации работников, ответственных за безопасность. Как пример этого – отсутствие отдельных подразделений (сотрудников), которые обеспечивают безопасность КВОИ, а также то, что ответственные специалисты часто просто не умеют определить потенциальный ущерб от нарушения информационной безопасности и обосновать перед руководством необходимость внедрения системы информационной безопасности. Для предприятий, где приоритетом является экономическая выгода, это наиболее серьезная проблема.

Оценивая уязвимость автоматизированных систем управления технологическими процессами (АСУ ТП), составляющих в большинстве основу КВОИ, необходимо учитывать и длительный срок их эксплуатации – десятки лет. При этом до середины 2000-х годов даже термина «уязвимость в программном обеспечении» еще не существовало и такие проблемы безопасности при разработке систем просто не принимались во внимание. Большинство АСУ ТП, которые в настоящее время работают в промышленности, создано без учета возможности кибератак. Например, большинство протоколов обмена данными, используемых SCADA и PLC, вообще не подразумевают никакой аутентификации и авторизации. Это приводит к тому, что любое появившееся в технологической сети устройство способно и получать, и выдавать управляющие команды на любое другое устройство.

Еще одна серьезная проблема заключается в том, что при столь длительном жизненном цикле АСУ ТП обновление и установка нового программного обеспечения в системе либо запрещены нормативной документацией, либо связаны со значительными административными и технологическими трудностями. В течение многих лет обновлением программного обеспечения АСУ ТП практически не занимались. При этом в открытом доступе есть довольно много информации по уязвимостям контроллеров и SCADA-систем, операционных систем, СУБД и даже интеллектуальных датчиков. Учитывая нарастающие темпы модернизации производства, централизации и информатизации функций управления производственными процессами, задачи информационной безопасности АСУ ТП будут становиться все более актуальными.

Необходимо обратить внимание и на проблему доступа ряда систем управления КВОИ к сетям общего пользования. Несмотря на существующее мнение, что сегмент сети систем управления изолирован, на самом деле современные системы управления имеют множество точек интеграции с другими системами предприятия. Служба автоматизации оценивает устойчивость системы относительно сбоев и отказов, тогда как необходимо учитывать возможность управляемой некорректной работы компонента, например, вследствие умышленного вредоносного воздействия, которое по статистике является наиболее распространенным инцидентом.

Исходя из сказанного, можно утверждать, что компоненты современных АСУ ТП могут оказаться взломаны, заражены, работать неправильно и привести к выходу из строя оборудования, неверно информировать оператора и спровоцировать его принять ошибочные решения, что, в свою очередь, может привести к аварийной ситуации.

Таким образом, решение проблем в области построения системы защиты КВОИ является комплексной задачей, требующей продолжения работ по совершенствованию нормативных правовых документов, формированию методической базы с учетом мирового опыта, развитию технологий информационной защиты на основе актуальных угроз в сфере информационной безопасности.

УДК 34:002

В.А. Насонова, П.Н. Жукова

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ МЕТОДИКИ ОЦЕНКИ УЯЗВИМОСТИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО РЕСУРСА

Согласно терминологии MITRE CVE (Common Vulnerabilities and Exposures) уязвимость – это состояние вычислительной системы (или нескольких систем), которое позволяет исполнять команды от имени другого пользователя; получать доступ к информации, закрытой для данного пользователя; показывать себя как иного пользователя или ресурс; производить атаку типа «отказ в обслуживании».

К основным характеристикам защищенности информационной системы (ИС) учреждения относятся: конфиденциальность информационной сферы системы; целостность ИС; доступность системы; подотчетность системы.

Отметим также, что уязвимости ИС могут иметь место на двух этапах жизненного цикла системы – на технологическом и эксплуатационном.

В условиях воздействия внешних и внутренних угроз ИС учреждения становится уязвимой вследствии нарушения равноправия в обслуживании пользователей; снижения пропускной способности систем обработки информации ниже минимально заданного допустимого уровня; отказа сервисных служб обслуживать запросы пользователей системы; зацикливания процесса функционирования, в частности процесса передачи и обработки информации, из-за нарушения целостности передаваемой и обрабатываемой информации.

В соответствии с классификацией информационного ресурса можно выделить источники возникновения уязвимости защищаемого ресурса. Наиболее вероятными являются обслуживающий персонал, средства вычислительной техники, информационные ресурсы, системное и прикладное программное обеспечение.

Практическая задача оценки угроз уязвимостей состоит в разработке модели представления системы информационной безопасности (ИБ), которая на основе научно-методического аппарата позволяла бы решать задачи оценки уязвимостей информационного ресурса, использования и оценки эффективности системы защиты информационного ресурса учреждения.

Основной целью модели является представление процесса создания системы ИБ с учетом правильности оценки уязвимостей параметров информационного ресурса, эффективности принимаемых решений и выбора рационального варианта технической реализации системы.

Специфическими особенностями решения данной задачи является: неполнота и неопределенность исходной информации о составе информационного ресурса и характерных угрозах; многокритериальность задачи, связанная с учетом большого числа частных показателей в системе защиты информации; наличие как количественных, так и качественных показателей, учитывающихся при решении задач разработки и внедрения модели оценки уязвимости ИС; невозможность применения классических методов оптимизации.

Проектирование системы безопасности сводится к математической модели. При этом необходимо учитывать ценность ресурсов системы, выраженную, например, в стоимостных показателях (характеристиках).

Широко известны табличные методы, учитывающие стоимостные характеристики ресурсов. В методах данного типа показатели информационных ресурсов оцениваются с точки зрения стоимости их замены или восстановления работоспособности, существующие или предполагаемы программные ресурсы оцениваются тем же способом, что и информационные.

Показатели, описывающие свойства защищаемых ресурсов и средств защиты, должны быть выражены количественно. Для преобра-

зования качественных показателей в количественны чаще всего используются экспертные оценки. При этом учитывается ценность информации для ее владельца, степень критичности информации и другие ее характеристики, например уровни секретности.

Рассматривается также задача рационального выбора метода определения с использованием весовых коэффициентов параметров уязвимости системы защиты информационного ресурса.

При наличии повышенных требований к безопасности информационного ресурса должен быть проведен так называемый полный вариант оценки уязвимостей системы, в рамках которого в дополнение к базовым должны рассматриваться следующие аспекты: определение ценности информационных ресурсов; расширение набора угроз, определенного на базовом информационном уровне ИБ; оценка вероятности угроз; определение уязвимостей информационных ресурсов.

При выборе дополнительных средств защиты учитываются не только сами угрозы, но и источники их возникновения. После идентификации выделяются уровни угроз (вероятность их реализации) и уровни уязвимости.

Основными факторами, определяющие выбор метода оценки весовых коэффициентов, являются: физическая сущность параметров и отношение между ними (параметры определяются исходя из цели); сложность проведения экспертизы и трудоемкость получения экспертной информации; степень согласованности мнений экспертов. Степень согласованности в первую очередь зависит от количества привлекаемых экспертов и уровня их квалификации, в то же время на нее будет влиять выбранный метод оценки весов, трудоемкость обработки экспертных данных. Этот фактор не является главным при современном уровне развития вычислительной техники.

Очевидно, что наиболее простыми методами с этой точки зрения являются ранговые, балльные методы. Учет вышеприведенных факторов позволяет выбрать метод оценки весовых коэффициентов системы защиты информационного ресурса учреждения. В качестве метода предлагается метод парных сравнений (метод Т. Саати).

Исходной информацией для построения функций принадлежности являются экспертные парные сравнения. Для каждой пары элементов универсального множества эксперт оценивает преимущество уязвимости одного элемента над другими по отношению к свойству нечетного множества $u_1 \quad u_2 \ \ldots \quad u_n$ – параметры экспертной оценки уязвимости системы защиты информационного ресурса:

$$A = \begin{matrix} u_1 \\ u_2 \\ \dots \\ u_n \end{matrix} \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & & a_{nn} \end{bmatrix},$$

где a_{ij} – уровень преимущества элемента u_i над u_j ($i, j = \overline{1,n}$), определяемый по 9-балльной шкале Саати.

Отношения весов представляются в виде сравнительных суждений из шкалы относительной важности. Далее, для матрицы парных сравнений A, состоящей из элементов a_{ij}, $i, j = 1,2,\dots,n$ (размерность матрицы определяется количеством параметров), должно выполняться условия $a_{ij} = \frac{1}{a_{ij}}$.

Предположим, что результаты попарного сравнения параметров уязвимости системы защиты информационного ресурса описываются отношениями их весов, т. е. можем представить в виде матрицы A (матрицы Саати).

Для нахождения вектора весов $\overline{\Lambda}$ необходимо решить уравнение, учитывая, что ранг матрицы равен 1, то n – единственное собственное число этой матрицы и, следовательно, имеется ненулевое решение. Более того, оно единственное, обладающее свойством:

$$\sum_{i=1}^{n} l_i = 1$$

Это решение – искомый вектор относительных весов параметров – вектор Саати.

A1	A2	A3	A4
1	a	a	a
a	1	a	a
a	a	1	a
a	a	a	1

Оценочная шкала экспертов: A1 – законодательная, научно-методическая и научная база защиты информационного ресурса; где A2 – структура органов, осуществляющих защиту информационного ресурса; A3 – политика информационной безопасности информационного ресурса; A4 – методы, способы и средства защиты информационного ресурса.

Определяя относительную важность четырех параметров (относительной важности уязвимостей информационного ресурса), необходимо решить задачу нахождения собственных значений $(A - lE) * W = 0$, где W – собственный вектор, а l – собственное значение матрицы.

Определение весовых коэффициентов с помощью нахождения вектора W матрицы парных сравнений является довольно трудоемкой задачей, но вполне приемлемой для оценки уязвимости информационного ресурса.

Уязвимость информационного ресурса можно рассчитать по формуле, используя оценки параметров системы защиты информационного ресурса:

$$U_{унив} = U_1 w_1 + U_2 w_2 + U_3 w_3 + U_4 w_4,$$

где U_1 – оценка законодательной, нормативно-методической и научной базы; U_2 – оценка структуры органа осуществляющей защиту информационного ресурса; U_3 – оценка политики информационной безопасности информационного ресурса; U_4 – оценка методов, способов и средств информационного ресурса; w_1, w_2, w_3, w_4 – веса оценок. Уязвимость отдельного параметра, информационного ресурса рассчитывается по формуле:

$$U^k = \sum_{i=1}^{n} u_i^k w_i$$

где U_k – показатель уязвимости k-типа информационного показателя; u_i^k – значения i-й характеристики параметра уязвимости элемента защиты информационного ресурса; w_i – весовой коэффициент i-й характеристики оценочного параметра информационного ресурса; n – количество рассматриваемых параметров.

Обобщенный критериальный показатель уязвимости k-типа информационного показателя качества информационными ресурса учреждения можно вычислить по формуле: $U^k = \sqrt[N]{U^1 \times U^2 \dots \times U^N}$

Показатель уязвимости является безразмерной величиной и имеет тенденцию к увеличению при повышении количества оцениваемых

параметров уязвимости информационного ресурса. Оценки уязвимости информационного ресурса разных организаций существенно отличаются, однако при наличии общих оценок и количества оцениваемых параметров их можно сопоставлять.

УДК 004.056

И.Б. Саенко, И.В. Котенко

ОСНОВЫ ПОСТРОЕНИЯ ПЕРСПЕКТИВНЫХ СИСТЕМ МОНИТОРИНГА И УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ДЛЯ ЗАЩИТЫ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

В условиях интенсивного развития и внедрения информационных и телекоммуникационных технологий ведущими государствами мира уделяется особое внимание вопросам обеспечения безопасности критически важных объектов информатизации (КВОИ). Для успешной реализации мероприятий защиты КВОИ необходимо решение ряда задач, основная из которых связана с созданием системы мониторинга и управления безопасностью. Цель ее создания – снижение до минимального уровня риска воздействия на объекты КВОИ и минимизация возникающего ущерба.

Современные системы мониторинга и управления безопасностью используют технологию управления событиями и информацией безопасности (Security Information and Events Management, SIEM). Эта технология является новым и достаточно бурно развивающимся направлением в области информационной безопасности, обладающим достаточно большим потенциалом по обнаружению угроз и выработке контрмер по обеспечению требуемого уровня безопасности информационной инфраструктуры. SIEM-системы в настоящее время имеют достаточно большое количество коммерческих реализаций, выполненных ведущими разработчиками и интеграторами средств и систем защиты информации. Однако область применения таких SIEM-систем первого поколения не выходит за рамки информационных процессов, протекающих в компьютерной сети. В то же время при мониторинге безопасности КВОИ становится все более актуальной задача выявления атак и прочих злонамеренных воздействий не только на основе анализа событий безопасности, зафиксированных в журналах сетевых

инфраструктурных элементов, но и на уровне бизнес-процессов, а также на уровне физических датчиков. Кроме того, известные коммерческие SIEM-системы испытывают значительные затруднения при обеспечении безопасности компьютерных сетей большой размерности. Все это обусловливает необходимость разработки и использования в КВОИ перспективных SIEM-систем, свободных от этих недостатков и определяемых как системы нового поколения.

В качестве основных требований, предъявляемых к перспективным системам мониторинга и управления безопасностью, следует указать возможность реализации следующего перечня новых функциональных возможностей:

1) межуровневой корреляции событий безопасности, поступающих из неоднородных источников;

2) адаптивной и высокомасштабируемой обработки событий, обеспечивающей управление большими объемами данных о безопасности в реальном или близком к реальному масштабе времени;

3) прогностического анализа безопасности, осуществляющего проактивное обнаружение и предотвращение дальнейших атак путем принятия соответствующих контрмер;

4) высокой доступности и отказоустойчивости сбора данных о событиях безопасности в условиях территориально-распределенного характера построения информационной инфраструктуры и активного вредоносного и (или) непреднамеренного воздействия на телекоммуникации.

В обобщенной архитектуре перспективной системы мониторинга и управления безопасностью КВОИ можно выделить уровень сети, уровень данных, уровень событий и уровень приложений. Уровень сети является внешним и охватывает сетевые элементы, являющиеся источниками данных о событиях безопасности. На уровне данных происходит предварительная обработка поступивших сведений, выделение из них событий безопасности и преобразование их в единый внутренний формат. На следующем уровне осуществляется обмен событиями между всеми компонентами системы. На уровне приложений производится хранение и аналитическая обработка событий.

Основными компонентами перспективной системы мониторинга и управления безопасностью КВОИ являются:

коллектор, под которым понимаются источники данных о событиях безопасности, такие, как сетевые устройства, серверы, рабочие станции, базы данных, межсетевые экраны, антивирусы, датчики, сенсоры и т. д.;

универсальный транслятор событий, формирующий уровень данных и предназначенный для первичной обработки данных о событиях безопасности, поступающих в систему;

высоконадежная шина событий, которая предназначена для распространения данных о событиях безопасности и их гарантированной доставки требуемым компонентам системы (уровень событий);

масштабируемый процессор событий, обеспечивающий адаптивную поддержку всех задач по их обработке и решению в реальном времени (уровень приложений);

репозиторий (хранилище) данных о безопасности;

система принятия решений и реагирования, предназначенная для централизованной верификации и управления политиками безопасности, обеспечивающими защиту инфраструктурных элементов (уровень приложений);

компонент моделирования атак и анализа защищенности (КМААЗ), обеспечивающий дополнительные аналитические возможности системы за счет реализации функций моделирования атак и анализа защищенности (уровень приложений);

прогностический анализатор безопасности, обеспечивающий расширенные возможности мониторинга безопасности, заключающиеся в моделировании состояния элементов информационной инфраструктуры в ближайшей перспективе и предсказании возможных нарушений безопасности (уровень приложений);

система визуализации, предназначенная для представления информации о безопасности в графическом виде, обеспечивающем ее наибольшую степень восприятия и визуального анализа (уровень приложений).

Средством кросс-платформенной интеграции компонентов системы мониторинга и управления безопасностью является репозиторий. В качестве основы для его реализации положена сервисно-ориентированная архитектура. Архитектура репозитория разделяется на два уровня: уровень хранения и уровень веб-сервисов. Уровень хранения включает в себя реляционную базу данных, базу XML-данных и базу данных в формате RDF, называемых триплетами, так как они отражают отношения «субъект – предикат – объект». Тем самым обеспечивается гибридный подход к хранению данных о событиях безопасности, сочетающий в себе достоинства всех базовых моделей представления данных и обеспечивающий, с одной стороны, задание моделей предметной области в виде онтологий, а с другой – использование логического вывода для выработки решений.

Из остальных компонентов более подробно охарактеризуем компонент КМААЗ. Он способен генерировать графы атак, вычислять метрики защищенности, оценивать защищенность сети посредством анализа графов атак, генерировать отчеты с рекомендациями по повышению безопасности и анализировать события безопасности для обнаружения атакующих действий, что позволяет распознавать модели поведения возможного злоумышленника и его последующие шаги.

Входными данными для КМААЗ являются: конфигурация компьютерной сети (системы); политики безопасности, определяемые множеством полномочий или правил доступа; формируемые предупреждения; внешние базы данных уязвимостей, атак, платформ и т. д.; профили нарушителей; требуемые значения метрик безопасности.

Основными результатами работы компонента КМААЗ являются: обнаруженные уязвимости; возможные маршруты (графы) атак и целей атак; зависимости между сервисами; «узкие места» в безопасности компьютерной сети; скорректированные деревья атак, основанные на изменениях, произошедших в сети; предсказания дальнейших шагов нарушителя; метрики безопасности, которые могут использоваться для оценки общего уровня безопасности; последствия атак и контрмер; предложения по увеличению уровня безопасности; решения, основанные на мерах, политиках и инструментарии безопасности.

В качестве примеров КВОИ, демонстрирующих преимущества перспективной системы мониторинга и управления безопасностью, были выбраны и проанализированы следующие сценарии:

компьютерная инфраструктура высокой производительности, применяющаяся для поддержки проведения Олимпийских игр, в которой циркулируют потоки, равные сотням тысяч/миллионам событий в секунду;

распределенная компьютерная инфраструктура, в которой доставка данных о событиях безопасности от периферии к центру и передача решений по применению контрмер от центра к периферии осуществляется через коммуникационную среду, подвергающуюся многочисленным воздействиям;

критическая инфраструктура (например, дамба), в которой необходимо проведение совместной обработки данных, поступающих как от традиционных для SIEM-систем источников событий, так и от инфраструктурных датчиков (сенсоров), фиксирующих параметры состояния элементов инфраструктуры;

информационная инфраструктура для проведения мобильных денежных платежей, в которой угрозы информационной безопасности коррелируются с угрозами финансового мошенничества.

Работа выполняется при финансовой поддержке РФФИ (13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417), программы фундаментальных исследований ОНИТ РАН (контракт № 2.2) и проекта ENGENSEC программы Европейского сообщества TEMPUS.

УДК 004.056

С.Ю. Стецюк

ПРОБЛЕМНЫЕ ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБЕСПЕЧНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

В последние годы мировым сообществом специалистов в сфере безопасности особое внимание уделяется важным для жизнедеятельности государства объектам инфраструктутры и возможным последствиям воздействий на подобные объекты для экологической, социальной, экономической и других сфер национальной безопасности. Очевидно, что инфраструктуры стран содержат множество критически важных объектов, таких, например, как электростанции, нефтепроводы, экологически опасные производства, транспортные узлы, выведение которых из строя может привести к катастрофическим последствиям.

В связи с этим в большинстве развитых стран мира (США, Австралия, Израиль, Франция, Германия и др.) были проведены исследования по выявлению объектов, которые могут представлять угрозу для нормальной жизнедеятельности стран в случае нарушения штатного функционирования (в результате террористических (диверсионных) актов, техногенных катастроф, стихийных бедствий). В первую очередь обращалось внимание на объекты, выход которых из строя может оказать существенное влияние на транспортную, энергетическую, кредитно-финансовую и другие критичные для обеспечения жизнедеятельности в масштабах государства или отдельных крупных районов системы.

По результатам исследования на территории США и Канады выделено около 2300 подобных объектов, в Германии – более 650, Франции – около 500, Японии – до 700. При этом отмечается, что они обладают относительно низкой защищенностью и имеют большое количество уязвимых точек несанкционированного доступа, воздействие на которые может привести фактически к полному параличу систем жизнедеятельности государства.

Защита критически важных объектов (КВО) как в отдельности, так и в их совокупности, которую принято называть критически важной инфраструктурой, или критической инфраструктурой, представляет собой одну из наиболее важных задач обеспечения национальной безопасности любой страны. Защита КВО включает проведение мероприятий, которые должны обеспечить их сохранение в случае различных воздействий природного или техногенного характера.

В последнее время вопросы безопасности критических инфраструктур активно поднимаются во всем мире. В рамках работ, проводимых в

этой области в Республике Беларусь, 25 октября 2011 г. подписан указ Президента Республики Беларусь № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации», которым утверждается Положение об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации.

В настоящее время в Республике Беларусь действует ряд нормативных правовых актов, регулирующих правовые отношения, возникающие при обеспечении безопасной эксплуатации и надежного функционирования критически важных объектов информатизации (КВОИ):

указ Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации»;

указ Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации»;

постановление Совета Министров Республики Беларусь от 30 марта 2012 г. № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации»;

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 декабря 2011 г. № 96 «О некоторых мерах по реализации указа Президента Республики Беларусь от 25 октября 2011 г. № 486»;

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 апреля 2012 г. № 42 «Об утверждении Инструкции о порядке проведения внешнего контроля критически важных объектов информатизации».

Кроме того, приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 17 июля 2013 г. № 47 утвержден и введен в действие технический кодекс установившейся практики «Информационные технологии и безопасность. Безопасная эксплуатация и надежное функционирование критически важных объектов информатизации. Общие требования», который определяет основные технические требования к обеспечению безопасности КВОИ.

Однако, несмотря на обширную область регулирования, которую затрагивают указанные нормативные правовые акты, остаются отдельные нерешенные вопросы, оказывающие значительное влияние на состояние защищенности КВОИ. Прежде всего, необходимо отметить отсутствие четких и однозначно трактуемых критериев для идентификации КВОИ, что дает возможность не относить значимые для национальной безопасности Республики Беларусь объекты инфраструктуры к критически важным. Кроме того, данной тенденции способствует и

факт отсутствия ответственности за нарушения в сфере обеспечения безопасности КВОИ (в том числе и за бездействие). Обращает на себя внимание и тот факт, что на сегодняшний день требования к системам безопасности КВОИ носят общий характер и не учитывают специфики функционирования объектов информатизации.

В связи с изложенным целесообразно:

определить понятные и однозначно трактуемые критерии отнесения объектов информатизации к критически важным;

закрепить ответственность за нарушения в сфере обеспечения безопасности КВОИ;

создать иерархию технических нормативных правовых актов, а также методических документов, которые учитывали бы особенности функционирования специфических КВОИ и оказывали бы существенную помощь владельцам таких объектов в построении систем безопасности.

Таким образом, устранение проблемных вопросов в обеспечении безопасности КВОИ требует комплексного, системного и нетривиального подхода к их решению. Не последнюю роль в данном процессе должен играть передовой опыт государств, которые уделяют повышенное внимание обеспечению безопасности критических инфраструктур.

УДК 004.7.056:004.41:629.7

А.И. Трубей, Г.Н. Науменко

ТЕОРЕТИЧЕСКИЕ И ПРИКЛАДНЫЕ ПРОБЛЕМЫ БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

При создании и эксплуатации критически важных объектов информатизации (КВОИ) надежность и безопасность являются вопросами первостепенной важности. Влияние программного обеспечении (ПО) на надежность и безопасность любых систем является ключевым фактором. Это обусловливает актуальность применения соответствующих методов и средств обеспечения надежности и безопасности программных продуктов, в особенности при разработке и обеспечении гарантии качества их наиболее критичных компонентов. В настоящее время осуществляется создание в Республики Беларусь совместно с Организацией европейского сотрудничества по стандартизации в области космической деятельности (ECSS) нормативной базы по установлению единых правил и требований, предъявляемых к гарантии качества ПО наземных сегментов и бортовых космических систем. Она предназначена для оказания методической помощи в выборе и применении методов и средств обеспечения безопасности и надежности ПО. Несмотря на то, что общее описание технологии надежности и безопасности нацелено в основном на разработку космических аппаратов, описываемый подход может быть адаптирован к проектам различной природы, в том числе к КВОИ.

Отказы, вызванные ПО, в значительной степени происходят случайно и могут иногда привести к катастрофическим последствиям, которые мировое сообщество уже неоднократно испытало. К актуальным теоретическим и прикладным вопросам обеспечения безопасности ПО можно отнести: основные угрозы безопасности ПО, методы и средства обеспечения безопасности ПО, безопасность системного ПО, нормативно-правовую базу для применения требований к безопасности ПО.

По данным компании Hewlett Packard можно выделить более 500 классов различных уязвимостей в ПО. Около 95 % всех дефектов программ, относящихся к безопасности, проистекают из 19 типичных ошибок, природа которых вполне понятна. По данным Software Engineering Institute опытный программист пропускает приблизительно один дефект на 100 строк кода. Если в течение жизненного цикла программного обеспечения 99 % этих дефектов будут обнаружены и исправлены, то в пакете программ, состоящем из 1 млн строк исходного кода, останется примерно 1 тыс. дефектов. Например, дистрибутив Red Hat Linux 7.1 состоит приблизительно из 30 млн строк кода, а Microsoft Windows XP содержит около 40 млн строк. Используя упомянутую статистику, число невыявленных дефектов в Red Hat Linux и Windows XP можно оценить соответственно в 30 и 40 тыс.

Чем раньше удастся выявить уязвимость в ПО, тем меньше финансовых средств понадобится для ее устранения.

Стоимость устранения уязвимостей ПО

Этапы разработки ПО	Стоимость устранения уязвимости, долларов США
Разработка технического задания	139
Проектирование	455
Разработка (программирование)	977
Тестирование	7 136
Сопровождение	14 102

Уязвимости кода включают следующие основные классы:

нарушение предположений использования программных функций (переполнение буфера, некорректное применение типов, некорректное разыменование указателей и т. д.);

неправильная работа с системными ресурсами (ошибки работы с динамической памятью, объектами программного взаимодействия и т. д.);

ошибки кодирования, которые могут привести к зацикливанию, потере точности или некорректному результату на выходе программы;

ошибки набора и редактирования текста;

внедрение в программу отладочного кода или кода с недекларированной функциональностью.

Организация «Открытый проект по безопасности Web-приложений» опубликовала «Десять самых критических уязвимостей Web-приложений»: отсутствие проверки входных данных; неправильное управление доступом; неправильная аутентификация; кроссайтовые сценарии; переполнение буфера; внедрение команд; неправильная обработка ошибок; небезопасное хранение; отказ от обслуживания; небезопасное управление конфигурацией.

Подходы к анализу безопасности ПО можно разделить на две основные категории: статический и динамический.

Статический анализ представляет собой анализ исходного кода, производимый без его реального выполнения. С его помощью можно предотвратить ошибки до их внесения в состав основного программного кода и гарантировать, что новый код соответствует стандарту.

Достоинствами статического анализа кода являются отсутствие необходимости в астрономических затратах времени на прогон программ при разных условиях функционирования и возможность добиться большей степени автоматизации проверок на наличие дефектов программ исходя из их конструктивных признаков.

Статический анализ позволяет автоматизировать выявление ограниченного подмножества ошибок (некорректности кодирования, «мертвый код», ошибки портирования), не касаясь вопросов безопасности программных систем.

Динамический анализ предполагает проведение тестирования уже скомпилированного ПО и функционирующего в определенной среде. Динамический анализ позволяет выявлять не только технологические, но и эксплуатационные уязвимости, связанные с неправильной настройкой ПО. Эффективность динамического анализа напрямую зависит от качества и количества входных данных для тестирования. К другим недостаткам динамического анализа следует отнести возможность его применения лишь на поздних этапах разработки, а также необходимость самостоятельно определить фрагмент исходного кода, соответствующий функции или процедуре, во время исполнения которой возникла ошибка. Достоинствами динамического анализа является очень низкий уровень ложных срабатываний, так как об-

наружение ошибки происходит в момент ее возникновения в программе. Кроме того, анализ в рабочей среде позволяет получить наиболее релевантные результаты, учесть особенности среды, влияющие на возможность проведения атаки.

Безопасность используемого системного ПО имеет тесную взаимосвязь с ошибками программирования. Многие простейшие виды ошибок, например переполнение буфера, могут быть предотвращены при использовании типизированных языков вместо традиционных, таких, как C и C++. Языки Java, Scheme и ML являются примерами языков, в которых, по крайней мере, принципиально не может иметь место переполнение буфера.

Следующее поколение языков программирования должно основываться на системах типизации, которые могут выражать и выполнять политики безопасности конкретных приложений. В основу языков системного программирования следующего поколения предлагается положить применение так называемых «утонченных» (refinement) типов данных, т. е. типов, имеющих форму «{x : T | P (x)}», где T – тип, а P (x) – предикат над значениями типа T.

Существующая нормативная, методическая и инструментальная база не позволяет эффективно обеспечивать безопасность ПО. Поэтому потребность в повышении надежности и безопасности ПО привела к разработке в рамках программы «Стандартизация-СГ» СТБ ECSS-Q-HB-80-03A-2014 «Космическая техника. Обеспечение качества продукции. Надежность и безопасность программного обеспечения». Документ представляет собой методические рекомендации по реализации требований к надежности и безопасности ПО, определенные в СТБ ECSS-Q-ST-80C-2014 «Космическая техника. Обеспечение качества продукции. Гарантия качества программного обеспечения».

В стандартах приведена общая программа обеспечения надежности и безопасности ПО, т. е. полный комплекс мероприятий, осуществляемых для обеспечения того, что требования надежности и безопасности, применимые к ПО, определены и выполнены.

К основным методам и средствам обеспечения надежности и безопасности ПО, рассматриваемым в стандарте, можно отнести:

анализ последствий и критичности отказов ПО;

анализ дерева отказов ПО;

анализ отказов ПО, обусловленных общей причиной;

методы и средства разработки, применяемые для оценки надежности и безопасности ПО (например, анализ потоков данных, анализ потоков управления, анализ составления расписаний).

Особое внимание уделяется определению, обоснованию и применению мер по обеспечению надежности и безопасности критического ПО.

Для создания действительно безопасного ПО необходимо сократить на 1–2 порядка число дефектов в спецификациях, ошибок при проектировании и реализации. Разработка ПО должна начинаться с определения наилучших методов проектирования, дополняться хорошо зарекомендовавшими себя техническими подходами и подкрепляться практикой, способствующей успешному завершению процесса создания безопасного ПО, качество которого подтверждается обязательными сертификационными испытаниями.

УДК 330.46

В.М. Шишкин

НЕЛИНЕЙНЫЕ ЭФФЕКТЫ В ОЦЕНКЕ ЗАТРАТ НА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ

Современные объекты реальной, производящей экономики, крупные финансовые структуры, системы государственного, военного управления являются сложными организационно-техническими системами, склонными к нелинейному поведению, возникновение критических состояний в них не должно считаться исключительным явлением. В структурно сложных объектах незначительный локальный сбой, первичный отказ могут сыграть роль малого параметра и привести к непредсказуемому системному, вплоть до катастрофического, эффекту. Такие системы выполняют интегрирующие, инфраструктурные функции в обеспечении основных видов жизнедеятельности людей, объективно становясь критическими в статусном смысле. Но и статусное понимание критичности, что заставляет выделять критически важные объекты, неявным образом свидетельствует о нелинейном характере их поведения, по крайней мере, в восприятии меры риска. Сложные организационно-технические системы должны рассматриваться как нелинейные динамические системы, поведение которых предполагает возможность перехода в критическое состояние в физическом смысле независимо от их назначения.

Определение разумного уровня затрат различных ресурсов на обеспечение безопасности функционирования такого рода систем в условиях присущей им нелинейности, плохой прогнозируемости поведения и неизбежной ограниченности ресурсов является важной нетривиальной и неоднозначной задачей. С одной стороны, неразумны большие затраты при умеренных рисках, а с другой – еще более опрометчивой может быть экономия при их недооценке. Основная сложность при этом состоит в недостаточной определенности идентификации и оценок рисков, возможность которых ограничена знанием (незнанием) и неизбежным субъективизмом экспертов. Кроме того, не всегда оценки стоимостных показателей в номинальном денежном измерении адекватно отражают реальность.

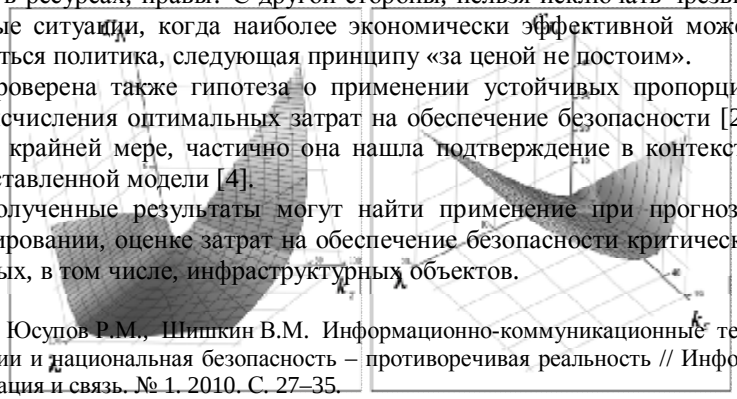
Затраты на обеспечение безопасности можно при желании наращивать почти неограниченно либо, наоборот, недооценить потенциальный ущерб. На вопрос, как определить уровень затрат, оптимизирующий суммарные издержки на защиту и остаточный ущерб как сумму двух разнонаправленных функций, казалось бы давно имеется классический ответ, но практика иногда кардинально ему противоречит, например, в сфере информационной безопасности [1]. К экономике безопасности плохо применимы традиционные подходы, а практика демонстрирует парадоксальное явление одновременного роста как затрат на защиту информационных активов, так и ущерба от нарушений их безопасности.

Характерна в приложении к рассматриваемой ситуации неявно сформулированная антиномия [2]. С одной стороны, утверждается, что «любой аргумент оценки уровня безопасности должен исходить из того, что твердо установлен экономический эквивалент угрозы», далее – «защитные мероприятия … могут быть необходимы и тогда, когда они непосредственно не окупаются экономически». Оба приведенных высказывания, безусловно, справедливы, но как тогда принимать практические решения.

Таким образом, необходим подход, который позволил бы снять формальное противоречие между экономическими ограничениями с одной стороны и требованиями безопасности, развития и т. д. с другой, обеспечив между ними рационально обоснованный компромисс. Он становится возможным, если учесть явно нелинейный характер восприятия меры риска в критических приложениях.

Ранее нами была показана возможность и методика нелинейного преобразования меры риска с использованием функций степенного распределения путем аппроксимации экспоненциального закона распределения, часто используемого в качестве моделей первичных характеристик, связанных со временем [3]. Было признано, что имеются основания считать степенные функции наиболее адекватными как для описания динамических свойств, так и в функциях распределения вероятностей меры риска.

Полученные результаты позволили предложить подход к оценке применения средств защиты информационных активов с нелинейных позиций. Используя представления теории надежности (связав меру рис-



На графике функции C_L видно, что, как ей и положено, она демонстрирует наличие оптимума. Но этот оптимум очень слабо зависит от k_z и, кроме того, располагается в области малых значений k_z, т. е. оптимальность затрат при такой постановке задачи никак не определяется значимостью объекта (так как всюду $(C_L)'_{k_z} > 0$) и существенно ограничивает результативность. Но будет ли разумным такое «опти-

1. Юсупов Р.М., Шишкин В.М. Информационно-коммуникационные технологии и национальная безопасность – противоречивая реальность // Информатизация и связь. № 1. 2010. С. 27–35.

2. Фесечко А.И. Оптимизация защитных мероприятий по безопасности жизнедеятельности людей. Надежность и качество – 2011 : труды Междунар. симп. : в 2 т. / под ред. Н.К. Юркова. Пенза : Изд-во ПГУ, 2011. Т. 2. С. 30–31.

3. Шишкин В.М. Степенное распределение и управление рисками критических систем // Проблемы управления рисками и безопасностью : труды Ин-та системного анализа РАН. 2007. Т. 31. М. : КомКнига, 2007. С. 39–59.

4. Шишкин В.М. Эффективность, оптимальность и устойчивые пропорции затрат на безопасность при нелинейности меры риска // Надежность и качество – 2012 : труды Междунар. симп. : в 2 т. / под ред. Н.К. Юркова. Пенза : Изд-во ПГУ, 2012. Т. 1 . С. 123–127.

РАЗДЕЛ 5

АКТУАЛЬНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ДЕЯТЕЛЬНОСТИ УЧРЕЖДЕНИЙ УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ

УДК 372.862

А.А. Бабкин, С.А. Шлыков

НЕКОТОРЫЕ ВОПРОСЫ И МЕТОДИКИ ПРЕПОДАВАНИЯ КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» ДЛЯ СЛУШАТЕЛЕЙ И КУРСАНТОВ ВЕДОМСТВЕННОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ

Динамичное развитие информационных технологий и глобальной сети Интернет привели к формированию информационной среды, оказывающей влияние на все сферы человеческой деятельности. Без знания и квалифицированного применения современных информационных технологий, стандартов, протоколов и средств защиты информации невозможно достигнуть требуемого уровня информационной безопасности компьютерных систем и сетей.

Наиболее важны требования информационной безопасности для объектов, на которых обрабатывается информация, составляющая государственную тайну. К таким объектам в первую очередь относятся организации и учреждения автоматизированной обработки информации и управления государственного и ведомственного уровня.

В области информационно-коммуникационных технологий для курсантов и слушателей Вологодского института права и экономики ФСИН России ведется преподавание ряда специализированных дисциплин, в том числе и «Информационная безопасность». Обучение использованию методов и средств информационной безопасности является важнейшим направлением подготовки специалистов для уголовно-исполнительной системы по специальности 031001.65 «Правоохранительная деятельность». Для изучения различных аспектов применения информационных технологий и средств информационной безопасности в будущей профессиональной деятельности в стандарте специальности присутствует незначительное количество дисциплин естественнонаучного блока. При этом требования ФГОС ВПО к уровню подготовки выпускника по дисциплине «Информационная безопасность» включают широкий набор умений и навыков специалиста: работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы защиты информации, автоматизированные системы информационной безопасности, соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны, обеспечивать соблюдение режима секретности.

Информационная безопасность относится к находящимся в процессе активного развития предметным областям и включает в себя естественнонаучные, технические и гуманитарные составляющие [1].

Предметная область сформирована в таком ракурсе, что достижение информационной безопасности происходит в процессе постоянной информационной борьбы. Основными объектами информационного воздействия при этом являются информационно-технические системы и средства различного назначения, информативные признаки объектов, защищаемых от противоправных посягательств, а также личность, общество, государство [2, 3]. Следовательно, можно выделить определенные особенности в содержании подготовки специалистов с позиции информационной безопасности. Применительно к естественнонаучным специальностям (направлениям) содержание такой подготовки определяют теоретические основы безопасности информационных систем, специальные разделы математики, криптографическая и программно-аппаратная защита информации. Но для специальности «Правоохранительная деятельность» реализация такого подхода не представляется возможной. Кроме того, необходимо учитывать, что у слушателей и курсантов по специальности «Правоохранительная деятельность», где доминируют гуманитарные дисциплины, часто отсутствует мотивация к изучению дисциплин информационно-технического профиля. Основное внимание мы обращаем на изучение вопросов борьбы с компьютерными преступлениями, их экспертизы и расследования, защиты от информационно-психологического воздействия на человека через технические системы и средства массовой информации, а также организационные, оперативные, правовые и психологические аспекты обеспечения информационной безопасности [2, 3, 4]. Изучение этого курса наиболее актуально с позиций системного подхода. Содержание дисциплины направлено на технологии обеспечения информационной безопасности в открытых системах социальных связей и психологических отношений [3]. Открытые системы динамически взаимодействуют с окружающим миром, стремятся к усложнению структуры и дифференциации.

Приступая к изучению дисциплины «Информационная безопасность», мы определяем основополагающие понятия, характеризующие

следующие свойства информации: реактивность, ресурсность и фоновость, которые открывают новые перспективы в понимании разнообразных явлений, поскольку вся жизнь построена на информационных взаимодействиях [3].

Как уже отмечалось, важность и вместе с тем сложность в изучении представляют технологии инженерно-технической, аппаратно-программной, криптографической защиты информации. Наряду с обеспечением безопасности реактивной информации внимание необходимо уделять защите информационных ресурсов. Уязвимым звеном информационной безопасности остается и сам человек. Так, целью обеспечения безопасности человека является противодействие негативным и деструктивным информационно-психологическим воздействиям, инструментом которых может быть фоновая информация.

Важными объектами изучения дисциплины является информационное и аналитическое обеспечение правоохранительной деятельности. Информационное обеспечение – это единое сформированное пространство ресурсов структурированных данных и сведений, доступных для оперативного использования. Аналитическое обеспечение заключается в получении уже реактивной информации, позволяющей принимать решения и осуществлять действия, нацеленные на конкретный результат по профилактике, предотвращению, пресечению преступной деятельности, раскрытию и расследованию преступлений, охране общественного порядка. Это требует применения методов идентификации, диагностики, прогнозирования с использованием автоматизированных комплексов логико-аналитической обработки и визуализации данных.

Постоянным источником информационных ресурсов и генератором реактивной информации является фоновая информация – массивы сообщений, результаты видеонаблюдений, акустического контроля, мониторинга радиоэфира, телекоммуникаций, средств массовой информации, Интернета. На свойствах фоновой информации строятся стратегические операции и тактические приемы непроцессуального использования оперативно-розыскной информации, информационно-психологических воздействий, информационного противоборства в борьбе с наиболее опасными криминальными явлениями [3].

Информационные технологии открыли для правоохранительной деятельности огромные возможности в моделировании и прогнозировании событий, в отслеживании и контроле ситуаций, в управлении социальными процессами. Но появились и новые угрозы. Совершенствуя только технологии защиты, невозможно обеспечить безопасность ни самой информации, ни ее обладателей, как невозможно победить в войне, рассчитывая только на оборону. Обеспечение информационной

безопасности в деятельности правоохранительных органов должно включать использование как защитных, так и наступательных средств, а также совершенствование инструментов получения информации. Обращая внимание на необходимость комплексного подхода к обеспечению безопасности собственно информации, необходимо выделять технологии защиты реактивной информации, получение которой является целью оперативно-розыскного и следственного процесса и технологии защиты ресурсной информации, накапливаемой на определенных носителях. В комплексе инженерно-технических мер защиты реактивной информации необходимо выделить поиск и нейтрализацию работы действующих каналов утечки информации (оптических, акустических, электрических, электромагнитных), препятствие возможности создания оперативно-технических позиций для скрытого перехвата сигналов, энергетическое сокрытие сигналов, препятствующее их распознанию, регистрации и восстановлению противником. При защите информационных ресурсов наряду с инженерно-техническими мерами, направленными на предотвращение доступа противника к носителям информации и средствам информации, аппаратно-программной и криптографической защитой от злоумышленных разрушений, искажений и хищений информации необходимо обратить внимание на угрозы, связанные с качеством данных.

Касаясь технологий так называемой информационной войны, необходимо представлять, что управление людьми, сообществами, народами все в большей мере осуществляется с помощью целенаправленных информационных воздействий [3].

Технологии обеспечения информационной безопасности в открытых системах социальных связей и психологических отношений становятся инструментом правоохранительной деятельности, построенной на новых организационных принципах. Они включают как защитные, так и наступательные меры информационного противоборства, применение всего комплекса современных средств и методов поиска, обработки, анализа и использования информации в ее реактивных, ресурсных и фоновых проявлениях.

В связи со всем вышесказанным, учитывая многоплановость дисциплины «Информационная безопасность», ее изучение реализуется посредством инновационных подходов и использования передовых образовательных технологий. Примерами могут являться интерактивные технологии обучения, технологии проектного обучения и компьютерные технологии [5].

1. Гафнер В.В. Информационная безопасность : учеб. пособие. Ростов н/Д : Феникс, 2010.

2. Белов Е.Б. Траектории образования в области информационной безопасности // Информ. безопасность. 2007. № 2. С. 32–33.
3. Овчинский А.С. Концепция информационной безопасности правоохранительной сферы в парадигме открытых систем // Информ. технологии, связь и защита информ. МВД России. 2011. С. 50–51.
4. Астахова Л.В. Информационная безопасность: герменевтический подход : монография. М. : РАН, 2010.
5. Казаков В.Г. Новое время – новые технологии профессиональной подготовки // Проф. образование. 2006. № 1. С. 12.

УДК 004.056

С.В. Видов

СОВРЕМЕННЫЕ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В РЕЖИМНЫХ ОБЪЕКТАХ УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ РОССИИ

Обеспечение безопасности в режимных объектах уголовно-исполнительной системы России в первую очередь связано с соблюдением режимных требований в учреждениях, способами противодействия нарушителям режима. Согласно ст. 82 Уголовно-исполнительного кодекса РФ режим в исправительных учреждениях – установленный законом и соответствующими закону нормативными правовыми актами порядок исполнения и отбывания лишения свободы, обеспечивающий охрану и изоляцию осужденных, постоянный надзор за ними, исполнение возложенных на них обязанностей, реализацию их прав и законных интересов, личную безопасность осужденных и персонала, раздельное содержание разных категорий осужденных, различные условия содержания в зависимости от вида исправительного учреждения, назначенного судом, изменение условий отбывания наказания. Режим обеспечивается различными средствами, среди которых информационно-технические средства надзора и контроля играют значительную роль.

Ст. 83 УИК РФ гласит, что администрация исправительных учреждений вправе использовать аудиовизуальные, электронные и иные технические средства надзора и контроля для предупреждения побегов и других преступлений, нарушений установленного порядка отбывания наказания и в целях получения необходимой информации о поведении осужденных. Виды технических средств охраны и надзора и порядок их использования определяются в большей степени приказом Министерства юстиции от 17 июня 2013 г. № 94. Здесь есть определение и детальное описание интегрированной системы безопасности (ИСБ), раскрыты требования к системам, входящим в ее состав, установлен порядок оборудования вновь строящихся и подвергающихся реконструкции объектов УИС. Все эти изменения были внесены в рамках исполнения Концепции развития уголовно-исполнительной системы до 2020 года. Одновременно с этим следует указать, что в полной мере данные правовые нормы почти не применяются, так как учреждений нового типа в России почти нет, что связано с недостаточным финансированием реформ УИС.

Говоря о правовом регулировании вопросов использования современных технических средств и связанных с ними информационных технологий в целях обеспечения безопасности в режимных объектах УИС, нельзя не упомянуть и актуальные проблемы. Первая из них заключается в отсутствии описания компьютерных систем (программной и аппаратной составляющих), входящих в автоматизированные рабочие места специалистов (АРМ), обеспечивающих режим в исправительных учреждениях. Указаны лишь задачи, решаемые при помощи того или иного АРМ, однако информации о минимальных требованиях к техническим средствам, программному обеспечению нет. Это может привести к различным подходам к формированию одних и тех же АРМ в разных учреждениях ФСИН России, что, в конечном счете, приведет к снижению эффективности их использования, разночтениям в оценке важности и необходимости тех или иных программных и технических элементов АРМ. Еще одна проблема заключается в правовом сопровождении новых способов контроля за соблюдением режима, связанных с биометрическими данными человека. Использование средств учета и распознавания биометрических данных определяются нормативными правовыми актами РФ после всесторонней их апробации, исключающей причинение вреда жизни и здоровью осужденных и персоналу. Вместе с тем в федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных» в ст. 11 указано, что обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с уголовно-исполнительным законодательством Российской Федерации, однако в УИК РФ подобной нормы нет. Таким образом, если осужденный не согласится добровольно на обработку и использование своих биометрических данных, сотрудники ИУ не смогут законно использовать современные средства обеспечения режима.

Совершенствование программно-технической стороны средств обеспечения режима в исправительных учреждениях связано в первую

очередь с внедрением биометрических технологий, которые позволяют существенно повысить уровень безопасности в данных ИУ.

Система контроля и управления доступом призвана производить аутентификацию человека, т. е. производить процедуру проверки подлинности. Для этого используется один из трех принципов: «я – то, что я знаю», «я – то, что я имею», «я – то, что я есть». В первом случае речь идет о системе логинов (имен пользователей) и паролей, во втором – о различных контактных и бесконтактных смарт-картах, в третьем – о биометрических параметрах. Система логинов и паролей неудобна по той причине, что здесь велика роль «человеческого фактора». Пользователю необходимо постоянно помнить свои логин и пароль, периодически их менять, постоянно носить с собой мобильный телефон (если пароли одноразовые и приходят при каждой аутентификации в виде СМС) и т. д. Смарт-карты в основном подвергаются критике за то, что их легко можно украсть или использовать без привязки к конкретному человеку.

Самыми надежными и защищенными от подделки считаются на данный момент биометрические системы аутентификации. Они позволяют производить распознавание людей по одной или более физической или поведенческой черте. Наиболее распространенные уникальные физические черты человека, применяемые в СКУД: отпечатки пальцев, форма кисти руки, радужная оболочка глаза, сетчатка глаза, геометрия лица, форма ушной раковины, термограмма лица. Среди поведенческих черт лидирует аутентификация по голосу, реже используется аутентификация по походке, рукописному почерку, скорости и ритму набора текста на клавиатуре. Все перечисленные системы невозможно использовать без современных информационных технологий. Именно они обеспечивают быструю верификацию (сравнение полученных данных с одним шаблоном) или идентификацию (сравнение полученных данных со всеми зарегистрированными шаблонами) человека, хранение и пополнение базы данных шаблонов. Шаблон – это совокупность характеристик, принадлежащих объекту верификации пользователя. Для каждого объекта он различается по способам получения, методам компьютерной обработки и анализа, количеству потребляемых компьютерных ресурсов, необходимых для его хранения и использования. Эффективность, надежность и преимущества у всех вышеперечисленных способов аутентификации различная. Так, верификация по форме кисти руки не выдвигает требований к чистоте и температуре рук, по термограмме лица можно различать даже однояйцевых близнецов, а анализ голоса является одним из самых низкозатратных.

Существуют и минусы – аутентификация по сетчатке глаза невозможна при катаракте, для построения шаблона геометрии лица требуется большое количество характерных элементов, а клавиатурный почерк человека со временем меняется. Некоторые системы верификации применяются в рамках экспериментов в уголовно-исполнительной системе. В исправительных учреждениях ГУФСИН России по Красноярскому краю и УФСИН России по Ивановской области используются системы верификации осужденных по отпечатку пальца для контроля за их передвижениями, в УФСИН России по Омской области используется тот же метод для верификации сотрудников, учета их рабочего времени.

Необходимо также сказать и о возможностях идентификации человека в рамках организации режима в исправительных учреждениях. Использование систем, входящих в состав ИСБ (а это система охранно-тревожной сигнализации, система контроля и управления доступом, система охранного телевидения, система громкоговорящей связи и др.) на данный момент предполагает непосредственное участие оператора в анализе происходящего, особенно в анализе видеоматериала. Возможности идентификации по геометрии лица позволяют автоматизировать поиск конкретного человека в людском потоке, заполнение базы данных о передвижениях сотрудников или осужденных по территории ИУ. Следует заметить, что уровень компьютерного распознавания лиц уже приблизился к человеческому. Недавно компания Facebook поделилась очередным достижением в области развития искусственного интеллекта. Называется оно DeepFace и касается улучшенного алгоритма распознавания лиц. Так, при предъявлении двух разных фотографий одной и той же личности человек распознает сходство в 97,53 % случаев. Алгоритм DeepFace оказался успешен в 97,25 % тестов, причем независимо от различий в характере освещения на снимках и от того, смотрит ли человек на фото в камеру или в сторону. При подобном уровне интеллектуальной идентификации нагрузка на оператора пункта видеоконтроля будет снижена, что позволит проводить более качественный мониторинг действий осужденных.

Таким образом, информационные технологии предлагают широкий спектр программных и технических решений задач адекватного ответа современным угрозам режиму и безопасности в ИУ. Их внедрение и эксплуатация позволит существенно снизить вероятность нарушения режима, улучшить систему противодействия нарушителям, обеспечить должный уровень безопасности как сотрудников ИУ, так и осужденных.

УДК 34.09

А.Г. Голубев, И.В. Попов

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ОСУЖДЕННЫХ ЛИЦ ПРИ РАБОТЕ С ПРОГРАММНО-ТЕХНИЧЕСКИМ КОМПЛЕКСОМ «АКУС»

Согласно закону персональные данные являются конфиденциальными, т. е. не должны распространяться без согласия их субъекта или иного законного основания. Этот принцип применим и к осужденному лицу, отбывающему наказание с изоляцией или без изоляции от общества, поскольку он не лишен прав, а всего лишь ограничен в них.

В то же время одной из основных функций уголовно-исполнительной системы является строгий учет осужденных. Более 10 лет в качестве такой базы данных в УИС Российской Федерации применяется программно-технический комплекс «Автоматизированная картотека учета спецконтингента» (ПТК АКУС).

Проанализируем содержание исследуемого программно-технического комплекса на примере ПТК АКУС УИИ (для уголовно-исполнительных инспекций, исполняющих наказания без лишения свободы). В разделе «Ведение», иконка которого открывает картотеку, в карточке открывается доступ к трем формам: «Регистрация», «Смерть», «Дактокарта». В форме «Регистрация» на одноименной странице особый интерес для обеих сторон процесса исполнения наказания – и для сотрудников, и для осужденных – представляют поля: Адрес, Склонность к наркотикам, Исполнительные листы, Прежние судимости, Учеты. На странице «Анкета» той же формы ценными данными являются: «Гражданство (страна)», «Национальность», «Социальная группа», «Образование», «Профессия», «Семейное положение». На странице «Воинская обязанность»: является ли призывником (до 27 лет), годен ли к военной службе, военкомат по месту жительства, дата призыва, каким военкоматом призывался. На странице «Дополнительно» формы «Регистрация» заполняются поля: личный автотранспорт (модель, госномер); инвалидность, наличие зависимости и др.; имеющиеся заболевания; правительственные награды; другие сведения, в том числе особые приметы. Таким образом, форма «Регистрация» является самой объемной и наиболее содержательной. Она содержит все те сведения, с помощью которых к осужденному можно найти индивидуальный подход.

Две других формы персональной карточки («Смерть» и «Дактокарта») не столь подробны и не имеют такого широкого назначения. По существу, они направлены только на идентификацию лица. Однако если в форме «Смерть» отмечаются только дата установления смерти и

необходимые примечания, то в форме «Дактокарта» описываются весь процесс ее создания и некоторые его технические характеристики.

Остальные разделы ПТК АКУС УИИ – «Запросы», «Макросы», «Быстрые отчеты», «Таблицы», «Буферы», «Справочники», «Статистика», «Константы» – направлены на создание комбинаций упомянутых выше данных об осужденных, а также данных о свойствах и настройке самой информационно-поисковой системы. При создании этих массивов данных речь идет, конечно же, не об одном осужденном, а о группе, выделенной по одному или нескольким признакам, а также об организации работы самого ПТК. Эти данные не должны быть свободно доступны тем лицам, которые в нарушение закона попытались бы ими злоупотребить.

К сожалению, эти попытки нельзя полностью исключить. Очень часто и вне УИС оказывается гораздо выгоднее потратить некоторые усилия и некоторую денежную сумму на приобретение уже существующей технологии, чем гораздо большие усилия и средства на создание новой. Это причина для попытки незаконного доступа к ПТК АКУС лиц из числа сотрудников УИС. Для осужденного с криминальным поведением выигрыш от доступа к данным ПТК АКУС тоже понятен – это возможность уничтожить всю информацию о себе или о других осужденных, так или иначе влияющую на степень тяжести отбывания наказания, или обнародовать технические условия доступа к этой информации в криминальном сообществе.

Последняя цель на первый взгляд представляется нереальной, но ее достижение осужденными вероятно при определенных условиях. Факторами утечки служебной информации в правоохранительных органах уже почти традиционно считаются: стремление сэкономить на средствах, непонимание сути охранных мероприятий, отсутствие прогрессивного опыта организаторской деятельности и опасение обращаться к специалистам за консультацией в случае некомпетентности по каким-либо вопросам, крайняя невнимательность и беспечность, шантаж и запугивание. Таким образом, сведения об осужденных должны быть защищены как от случайного, так и от намеренного незаконного доступа.

В устройстве ПТК АКУС и в организации его использования для этого имеются некоторые средства и приемы. Прежде всего ПТК АКУС устанавливается в локальную сеть исправительного учреждения, не имеющую внешних информационных выходов, в том числе в интернет. Вся информация как текстового, так и графического характера набирается в картотеку вручную из источников, имеющих внутреннее происхождение (в самом учреждении) или полученных в ходе переписки между органами и учреждениями УИС и иными органами власти и управления.

Особо следует отметить градацию доступа к данным ПТК АКУС. Некоторые данные, в первую очередь о свойствах и настройке ПТК, а также данные таблиц и справочников для их изменения, могут быть доступны только администратору. Сотрудники, отвечающие только за ведение учета спецконтингента, заходят в систему под пользовательским паролем. Администратор же, управляющий функционированием комплекса, получает доступ к ПТК не только по особому паролю администратора в самом ПТК АКУС. Он заходит под особым паролем администратора и в операционную оболочку Windows при включении головного компьютера.

В обязанности администратора ПТК входит периодический контроль служебной деятельности сотрудников по заполнению электронных карточек: кто и под каким паролем заходил в информационно-поисковую систему, кто какие карточки (на каких конкретно лиц) заполнял. Учетные записи об этом представлены в символьной форме на языке программирования. В силу этого обязательным требованием к сотруднику на должности администратора ПТК АКУС является наличие знаний, умений и навыков по основам программирования и «материальной части» сервера и локальной компьютерной сети. Соблюдение этого требования, пусть и несколько косвенным образом, также служит условием (если не средством) защиты персональных данных осужденных.

Алгоритм работы с персональными данными в ПТК АКУС закладывается еще в процессе обучения в образовательных организациях высшего образования ФСИН России, начиная с 1-го курса очного обучения. На практических занятиях по ИиИТПД курсанты заполняют электронные карточки осужденных, пользуясь примерами из судебной практики по уголовным делам судов первой инстанции. С правовой точки зрения это особый случай использования открытых персональных данных без разрешения их субъектов, санкционированный законом (ст. 7 ч. 2 закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»). Важной технической особенностью является то, что АИПС «Гарант» или «КонсультантПлюс», откуда и делается выборка, не позволяют прямо копировать сведения из своих документов, предупреждая о соблюдении принципа защиты персональных данных. Поэтому курсантам приходится заполнять карточки путем набора текста либо его поиска в справочнике, встроенном в ПТК АКУС. Вводимые сведения, заканчивающиеся оглашением приговора суда, не имеют прямого отношения к отбыванию наказания, но внесение хотя бы их в электронную карточку формирует умение ее заполнять. После выполнения этой работы всей учебной группой и ее оценки преподавателем учебные карточки удаляются.

Таким образом, конфиденциальность сведений об осужденных обеспечивается комплексом правовых норм, организационных и технических мер, направленных на предотвращение несанкционированного доступа к учетным данным в целях защиты осужденных от злоупотребления его правами и обязанностями со стороны криминального сообщества или отдельных сотрудников. В принципе к учетной деятельности могут привлекаться только сотрудники (в изучаемом нами случае – инспекторы УИИ), допущенные в установленном порядке к работе с документами и материалами конфиденциального характера. Однако большой объем работы одного инспектора с достаточно большим количеством осужденных обусловил обязательность этой компетенции у каждого инспектора УИИ. К ознакомлению и работе со сведениями о содержании картотеки и о ее обслуживании допускается достаточно ограниченный круг лиц, будь они рядовыми операторами или администраторами. Допуск осуществляется с разрешения руководителя органа и только в объеме, касающемся непосредственной деятельности сотрудника.

Установленный режим работ с учетными документами принципиально не ограничивает доступ работающих с ними сотрудников, но препятствует несанкционированному доступу к персональным данным об осужденных лицам, не работающим с ними по своим служебным обязанностям, а также (при условии недопущения указанных выше факторов утечки) самим осужденным. Инспектору, выполняющему функции оператора ПТК АКУС, предоставлено право лишь на внесение и редактирование сведений об осужденном – меньший объем прав по сравнению с администратором, имеющим право менять формы документов и настройки ПТК. При этом вероятность своевременного обнаружения и исправления неточностей в записи учетных данных не снижается. В конечном итоге, с одной стороны, соблюдается конституционный принцип обеспечения права каждого гражданина на неприкосновенность частной жизни, с другой – учитывается особенность соблюдения этого принципа в УИС по отношении к осужденным.

УДК 681.3

И.А. Губин, В.И. Сумин

ВНЕДРЕНИЕ МЕТОДА РАЗГРАНИЧЕНИЯ В ПРОЕКТИРУЕМУЮ СИСТЕМУ ЗАЩИТЫ ИНФОРМАЦИИ УЧРЕЖДЕНИЙ УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ

Особый интерес для лиц, которые стараются осуществить несанкционированное проникновение, вызывают информационные процессы в системах специального назначения, в которых аккумулируется зна-

чительный объем конфиденциальной информации. Одними из таких информационных процессов являются информационные процессы систем специального назначения учреждений уголовно-исполнительной системы (УУИС). Они в системе специального назначения объединяют интегрированный комплекс автоматизированных информационных процессов и структур с единым набором информации в базах данных, правил доступа и протоколирования работы пользователей, протоколов информационного взаимодействия между компонентами системы, а также единым стилем пользовательского интерфейса.

Огромный объем аккумулируемой информации в системах учреждений уголовно-исполнительной системы, как открытой, регистрируемой по официальной линии, так и конфиденциальной, ставит ее в положение наиболее информационно емкой структуры в сфере исполнительной власти. Это делает информационные процессы в системе специального назначения привлекательными для отдельных лиц, группировок, общественно-политических движений и средств массовой информации, которые стремятся использовать служебную информацию для негативных целей.

Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» персональные данные (ПД) определяются как любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПД), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Федеральный закон налагает ответственность за невыполнение требований по защите ПД непосредственно на операторов ПД (сотрудников, осуществляющих обработку ПД, а также определяющих цели и содержание такой обработки), которые при обработке ПД обязаны принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПД, а также от иных неправомерных действий.

Все многообразие угроз безопасности информационной системы (ИС) УУИС можно представить в виде целой связки ключей и отмычек, а систему защиты информации от несанкционированного доступа (СЗИ НСД) – как сейф, в котором содержатся данные. Можно подобрать ключ – получить пароль и доступ к данным. Если умело использовать отмычку, то получится открыть сейф, взломав замок. Новый взгляд на построение лишенной уязвимости ИС предполагает достойную перспективу – обеспечить циркуляцию данных в надежно охра-

няемом месте, спроектированном без наличия уязвимостей, как банковское хранилище.

В данном случае уместно использовать дискреционную модель, которая изначально соответствует структуре и особенностям многих организаций. Но в силу своей гибкости и удобства реализации данная модель доступа содержит уязвимости, которые впоследствии станут угрозами безопасности. Можно использовать модель мандатного разграничения доступа. Данный подход вполне надежен в плане защиты информационных ресурсов, но неэффективен для реализации в силу особенностей информационных процессов.

Недостатки стандартных моделей были устранены путем разработки нового математического аппарата моделирования СЗИ НСД. Разработанная эталонная модель защищенной автоматизированной системы (ЭМЗАС) построена на базе Е-сетей и объединяет достоинства стандартных моделей СЗИ, а следовательно идеально подходит для создания защищенной ИС.

ЭМЗАС представляет идеализированную систему с набором уровней, каждый из которых является промежуточным положением авторизации на пути к данным. Получив доступ, субъект высшего уровня может получить доступ к субъектно-объектному наполнению низшего уровня только в соответствии с предписаниями объекта управления (ОУ). Необходимо все процессы доступа к ресурсам распределить по уровням эталонной модели, в итоге получим защищенную модель ИС УУИС организации с минимальным уровнем уязвимости.

Введем понятие монитора безопасности субъектов (МБС) – элемента, который разрешает порождение субъектов только для фиксированного подмножества пар активизирующих субъектов и порождающих объектов определенного уровня ЭМЗАС.

Рассмотрим 8-й уровень ЭМЗАС («Менеджерский»). Он определяет доступ прикладного компонента сервера ИС, авторизованного некоторым образом, к менеджерам ресурсов данного сервера. Предполагается, что в общем случае информация, располагающаяся на данном сервере, может находиться под управлением различных менеджеров ресурсов, поэтому на данном уровне уместнее всего расположить субъекты полного разграничения данных всего сервера. Субъект менеджера ресурсов «Общие данные» и субъект менеджера ресурсов «Специализированные данные» будут разграничивать информацию на условно допустимую для разглашения (повседневно используемую сотрудниками) и максимально неприемлемую для обнародования (используемые только командирами и руководителями) (табл. 1).

Разграничив данные на 8-м уровне, получили четкое соответствие и на 7-м (информационном) уровне ЭМЗАС. Он определяет доступ менеджера ресурсов сервера АС, авторизованного некоторым образом, к данным, управляемым этим менеджером ресурсов. В результате определенные данные под управлением определенного менеджера ресурсов используются в интересах пользователя, авторизующего доступ (табл. 2). Администратор в любой мой момент времени может заблокировать доступ, сделать резервную копию или перенастроить привилегии к самой важной информации без вмешательства в работу рядовых сотрудников, используя субъект менеджера ресурсов «специализированные данные».

Таблица 2

Информация объекта управления, касающаяся работы монитора безопасности объекта, уровень «Информационный»

Субъекты / Субъекты		Субъект менеджерских ресурсов администрирования ПБД «Филиал»	Управляющий субъект менеджера ресурсов «Объект N»					
			Авторизация Kom	Авторизация amKom	Авторизация SotrBuhg	Авторизация Nach Smeni	Авторизация ZamPoTilu	Авторизация Dezhurniy
Субъекты	Параметры вызова метода	Методы субъектов данного уровня, разрешенные для вызова субъектами вышестоящего уровня с данными						
Субъект менеджера данных администрирования ПБД «Объект N»	Без параметров	Close	–	–	–	–	–	–
	Роли, привилегии ролей	Insert, Delete, Update	–	–	–	–	–	–
Субъект менеджера ресурсов «Специализированные данные»								
Субъект использования данных категории объектов «Объект N»	Без параметров	–	Close	Close	Close	Close	Close	Close
	Отчет «График и распоряжения» Отчет «Рапорты»	–	Select, Delete, Insert, Alter	Select, Delete, Insert, Alter	Select, Insert	Select, Insert	Select	Select
	Отчет «Расчетные операции»							
Субъект использования данных категории объектов «Данные администрирования»	Без параметров	–	Close	Close	–	–	–	–
	Отчет «Журнал записей» Отчет «Ведомость хозяйственной части» Отчет «Данные сотрудников» Отчет «Данные заключенных»	–	Select, Delete, Insert, Alter	Select, Delete, Insert, Alter	–	–	–	–

УДК 343.8

В.Г. Зарубский

ПОВЫШЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УПРАВЛЯЮЩИХ КОМПЬЮТЕРОВ ПЕРСПЕКТИВНЫХ ИНТЕГРИРОВАННЫХ СИСТЕМ ОХРАНЫ НА ОСНОВЕ ЭМУЛЯЦИОННЫХ ПРОЦЕССОВ

В современных условиях успешная деятельность учреждений уголовно-исполнительной системы напрямую связана с эффективным применением инженерно-технических средств охраны. В частности, внедрение интегрированных систем охраны (ИСО), обеспечивающих наглядность отображения сигналов тревоги, позволяет повысить оперативность действий личного состава караулов, снизить риски возникновения чрезвычайных ситуаций на объектах охраны за счет сведения к минимуму человеческого фактора. В связи с этим становится актуальным вопрос выбора ИСО, полностью удовлетворяющих жестким требованиям, определяемым условиями эксплуатации на объектах охраны УИС. В качестве одного из первостепенных требований, предъявляемых к ИСО, необходимо выделить их высокую надежность. Так как интеграция современных ИСО осуществляется на базе управляю-

щего компьютера (УК), то для обеспечения высокой надежности всей системы в целом необходимо обеспечить надежную защиту информации в УК. Данная задача может быть решена путем внедрения в качестве УК структурно устойчивых компьютеров.

Разработка структурно устойчивых УК для ИСО связана с решением ряда частных задач – это разработка модели процесса их адаптации к текущему функциональному состоянию и разработка математической модели процесса функционального диагностирования. Далее рассматривается решения первой из этих частных задач.

Теория структурной устойчивости связана с таким понятием, как функциональная избыточность. Для осознания данного понятия необходимо рассмотреть некоторые термины.

Функцией системы назовем каждый фиксированный в ней алгоритм вычисления некоторого функционального состояния. Множество всех функций системы будем называть функциональной системой (ф-системой).

Функциональную систему будем считать функционально полной (ФП-системой), если для любого вычислимого функционального соответствия существует хотя бы одна вычисляющая его композиция, составленная из элементов этой системы.

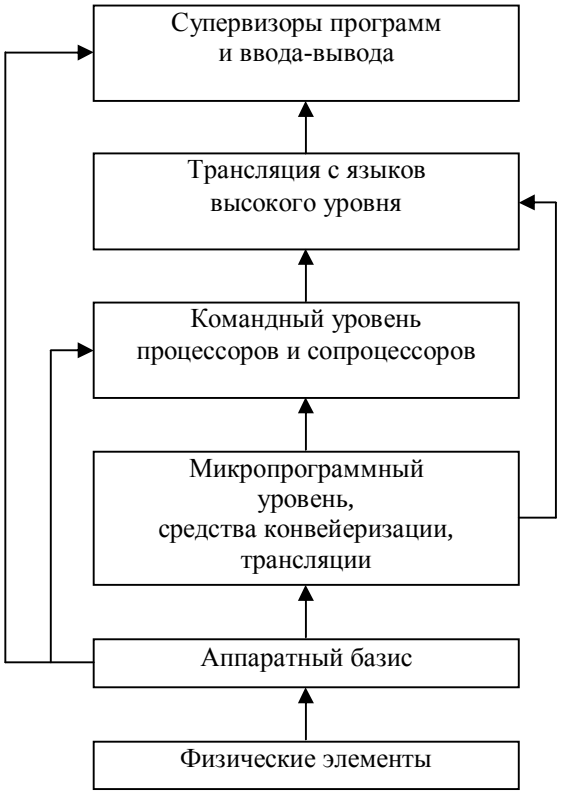
ФП-систему будем считать функционально-избыточной (ФИ-системой), если для любого функционального соответствия из существования вычисляющей его композиции следует существование другой вычисляющей его композиции. И наконец, ФП-система обладает свойством функциональной необходимости и достаточности, если она не содержит строгих недопустимых ФП-подмножеств.

Классификация функциональных систем на формальной основе позволяет ввести строгое определение типов функциональных отказов.

Функциональным отказом (ф-отказом) системы будем называть событие, заключающееся в утрате ею одного или нескольких функциональных элементов.

В связи с тем, что современные компьютеры отличаются существенной сложностью, которая проявляется в их иерархичности (многоуровневости), отказы в таких компьютерах могут проявляться на всех функциональных уровнях архитектуры. Проведенные ранее исследования доказывают существование структурной устойчивости на всех этих уровнях и показывают механизмы ее достижения.

Обобщенная архитектура перспективных УК



Единственным способом поддержания работоспособности УК в условиях стохастически возникающих ф-отказов следует считать восстановление утраченных функций на сохранившемся функциональном базисе, т. е. эмуляцию. Естественно, эмуляционные процессы влияют на характеристики восстанавливаемого УК, а так как исправный УК характеризуется тройкой (θ, T, A), где θ – система команд, T – временные характеристики ее быстродействия, A – множество алгоритмов (программ) специального программного обеспечения, то переводят тройку (θ, T, A) в тройку (q', T', A') по схеме ф-диагностирование – логическое представление УК после проявления отказа в аппаратуре, ф-адаптация – восстановление работоспособного состояния УК, А-адаптация – установление состава алгоритмов, удовлетворяющих требованиям отношения.

(θ, Т, А)→ф-диагностирование→ $\underbrace{ф\_адаптация \rightarrow А\_адаптация}_{Адаптация}$ → (θ′, Т′, А′).

Эмуляционные процессы на любом уровне архитектуры УК тем или иным образом проявляются на базовом командном уровне, в конечном счете характеризующем текущее ф-состояние (состав команд) и ф-состояние после адаптации (быстродействие и остаточная производительность). В связи с этим методику адаптации структурно устойчивых УК к текущему ф-состоянию целесообразно строить по принципу «ядра и оболочки»: в ее основу положить алгоритмы адаптации на командном уровне архитектуры («ядро»), которые по мере необходимости модернизируются под особенности иного функционального уровня, создавая своего рода «оболочку».

Для иллюстрации возможностей данной методики было осуществлено имитационное моделирование с использованием языка Ассемблера вычислительной машины IBM System/370. Данный выбор обусловлен тем, что:

существует достаточно доступное и подробное описание структуры и состава системы команд языка Ассемблера данной вычислительной машины;

несмотря на достаточно «преклонный» возраст данной вычислительной машины, ей установлен стандарт широкой «линейки» вычислительных машин, которые используются и преуспевают по сей день;

имеется возможность проведения экспериментальных исследований на базе имитационной модели DIAMOD, позволяющей получить не только практическое подтверждение работоспособности алгоритмов, реализующих теоретические положения данного исследования, но и временные характеристики данных алгоритмов;

на базе данной вычислительной машины было разработано множество специализированных компьютеров, которые нашли применение в различных отраслях (в том числе и ракетно-космической технике).

Система команд язык Ассемблера IBM System/370 насчитывает 54 команды, однако для упрощения примера будем использовать ограниченную систему команд. Для иллюстрации возможности ограниченная система команд содержит 13 команд, выбранных с учетом обеспечения ими эмуляционных процессов.

Результаты, полученные в процессе имитационного моделирования, приведены в таблице. Они показали эффективность предложенной методики и позволили оценить временные затраты на процессы адаптации различных команд.

Временные затраты на алгоритмы адаптации различных команд

Команда	З	ЗР	НР	ПУР	ВР	СЛР	ЗП	ПУ	ЗГ	КР	ДЗР	ЗДР	ЗПГ
Штатное время выполнения команды, мкс	1	1	1	3	1	1	3	3	3	1	1	3	3
Время выполнения процессов адаптации команды, мкс	–	–	80	6	16	30	126	14	44	22	38	28	44

Данные приведенные в таблице наглядно демонстрируют значительное превышение временных затрат на выполнение адаптационных процессов неработоспособных команд. Необходимо отметить и тот факт, что для УК ИСО такая характеристика, как быстродействие является не самой актуальной и незначительно влияющей на эффективность работы ИСО в целом. Однако решение данной проблемы возможно путем разработки оптимального алгоритма адаптации, чему и предполагается посвятить дальнейшие исследования в данном направлении.

УДК 681.3

А.С. Кравченко, А.А. Загуменнов, А.А. Мытницкий

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В УЧРЕЖДЕНИЯХ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ИСПОЛНЕНИЯ НАКАЗАНИЙ РОССИИ

Проблемы защиты информации в автоматизированных системах (АС) не теряют своей актуальности вот уже почти 40 лет. Это объясняется тем, что накапливаемая, хранимая и обрабатываемая в АС информация является достаточно уязвимой как с точки зрения опасности ее искажения или уничтожения, так и с точки зрения несанкционированного доступа к ней лиц, не имеющих на это полномочий.

Развитие методов защиты информации в АС от нарушения ее физической и логической целостности, а также от несанкционированного доступа происходило параллельно с развитием самих электронных средств обработки данных. Формировались основные подходы к раз-

работке методов, способов защиты данных и программ, которые в настоящее время предполагают использование специально создаваемых аппаратных и программных средств. Однако это не исключает возможности коренного изменения в будущем самого подхода к разработке новых и значительно защищенных информационных технологий, попытки создания которых подготавливаются бурным процессом информатизации общества.

С развитием инновационных технологий не в малой степени вопросы информационной безопасности и защиты от несанкционированного доступа беспокоят и силовые ведомства. В связи с концепцией развития УИС до 2020 г. в системе осуществляется переход к новым технологиям. Одним из решений проблемы безопасности баз данных является применение различных систем защиты информации (СЗИ) от несанкционированного доступа (НСД).

В ходе изучения имеющих в России предложений по организации системы информационной безопасности наиболее перспективным является внедрение и использование СЗИ от несанкционированного доступа Dallas Lock с применением электронных USB-ключей и смарт-карт eToken.

Dallas Lock – сертифицированная система защиты информации от несанкционированного доступа. Использование средств защиты информации от НСД Dallas Lock в проектах по защите информации ограниченного доступа позволяет привести автоматизированные системы в соответствие требованиям законов РФ, стандартов и руководящих документов. Основные из них: федеральный закон № 98-ФЗ «О коммерческой тайне»; федеральный закон № 5485-1 «О государственной тайне»; приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»; приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»; руководящий документ Гостехкомиссии РФ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»; Доктрина информационной безопасности РФ.

Система предназначена для защиты компьютера, подключенного к локальной вычислительной сети, от несанкционированного доступа с возможностью подключения аппаратных идентификаторов. Система защиты информации Dallas Lock может быть установлена на компьютеры, работающие под управлением следующих операционных систем (ОС): Windows XP (Service Pack не ниже 3), Windows Server 2003

(SP не ниже 2), Windows Vista (SP не ниже 2), Windows Server 2008 (SP не ниже 2), Windows 7 и Windows 8. Dallas Lock поддерживает 32 и 64-битные версии ОС.

СЗИ от несанкционированного доступа «Dallas Lock» обеспечивает: защиту информации от несанкционированного доступа на ПЭВМ в ЛВС через локальный, сетевой и терминальный входы; разграничение полномочий пользователей (локальных, сетевых, доменных, терминальных) по доступу к файловой системе и другим ресурсам компьютера.

Основные возможности системы защиты информации от несанкционированного доступа Dallas Lock: запрет загрузки компьютера посторонними лицам; двухфакторная авторизация по паролю и аппаратным идентификаторам (USB eToken, смарт-карты eToken, Rutoken, Touch Memory); разграничение прав пользователей на доступ к локальным и сетевым ресурсам; контроль работы пользователей со сменными накопителями; мандатный и дискреционный принципы разграничения прав; организация замкнутой программной среды; аудит действий пользователей; контроль целостности ресурсов компьютера; очистка остаточной информации; возможность автоматической печати штампов (меток конфиденциальности) на всех распечатываемых документах; защита содержимого дисков путем прозрачного преобразования; удаленное администрирование; выделенный центр управления, работа в составе домена безопасности; возможность установки на портативные компьютеры; отсутствие обязательной аппаратной части; работа на сервере терминального доступа; удобные интерфейс, установка и настройка.

Dallas Lock в отличие от большинства аналогичных средств защиты от несанкционированного доступа может поставляться как в программном варианте комплектации, так и с опциональным дополнением аппаратных средств защиты, что значительно повышает их эксплуатационные характеристики, снимая вопросы совместимости с аппаратными платформами используемых средств вычислительной техники. Кроме того, предусмотрена возможность подключения различных видов считывателей и идентификаторов (TouchMemory, eToken, Rutoken) через com- и USB-порты.

Электронные USB-ключи и смарт-карты eToken – компактные устройства, предназначенные для обеспечения информационной безопасности. Устройства eToken содержат процессор и модули памяти, функционируют под управлением своей операционной системы, выполняют необходимые прикладные программы и хранят информацию.

Ключи eToken базируются на высокозащищенной платформе, разработанной для производства смарт-карт – области, в которой традиционно предъявляют повышенные требования к информационной безопасности. Поэтому USB-ключи и смарт-карты eToken фактически являются миниатюрным компьютером, обеспечивающим безопасное

хранение персональных данных и надежно защищенным от несанкционированного вмешательства.

Применение eToken способствует решению следующих задач: усовершенствованию процесса аутентификации на локальном компьютере и в сети, а также защищенный доступ к базам данным и приложениям; шифрованию данных на серверах, ноутбуках и рабочих станциях; обеспечению защиту персональных данных; безопасности финансовых операции; внедрению электронной цифровой подписи и защите документации в системах сдачи электронной отчетности.

Преимущество ключей eToken заключается в возможности их становления основой инфраструктуры информационной безопасности в учреждениях УИС. Электронные ключи поддерживаются всеми ведущими производителями информационных систем, соответствуют требованиям российских регулирующих органов. Внедрение USB-ключей или смарт-карт eToken позволит не только решить нынешние актуальные задачи, но и сохранить инвестиции в последующих проектах обеспечения информационной безопасности.

Система защиты информации от несанкционированного доступа Dallas Lock полностью соответствует заявленным характеристикам, а также требованиям законодательства и руководящих документов в области защиты информации, что подтверждено сертификатом ФСТЭК РФ. Для ФСИН России критически важным является возможность управления рядом основных параметров системы информационной безопасности, а именно установление контроля за работой с отчуждаемыми носителями информации, жесткими дисками и за действиями пользователей в системе, загрузкой операционной системы.

СЗИ Dallas Lock не предъявляет каких-либо специальных требований к системе: достаточно, чтобы на защищаемом компьютере была установлена ОС из ряда поддерживаемых. Такая способность снижает затраты на ввод в эксплуатацию, последующее использование и обновление приложений.

УДК 004.056

А.Ю. Кирьянов, Р.В. Безносюк

ПРОБЛЕМНЫЕ ВОПРОСЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЕ НА ПРИМЕРЕ АКАДЕМИИ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ИСПОЛНЕНИЯ НАКАЗАНИЙ РОССИИ И ПУТИ ИХ РЕШЕНИЯ

Современный этап развития в информатизации государственных органов связан с широким использованием информационных технологий в процессе подготовки и реализации управленческих решений органами государственной власти. Поэтому защита персональных данных занимает особое место в уголовно-исполнительной системе.

Согласно российскому законодательству персональными данными является любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе его фамилия, имя, отчество и другая информация. Рассмотрим действующую правовую базу защиты персональных данных. Во-первых, это Конституция РФ, в которой признается само право на неприкосновенность личной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, ч. 1 ст. 24 запрещает сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. Персональные данные отнесены к категории конфиденциальной информации указом Президента РФ от 6 марта 1997 г. № 188.

Федеральным законом РФ от 27 июля 2006 г. № 152-ФЗ установлены условия обработки персональных данных. Ст. 6 установлено, что обработка персональных данных может осуществляться оператором с согласия субъектов персональных данных, за исключением случаев обработки персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности (ч. 7).

Постановлением правительства РФ от 1 ноября 2012 г. № 1119 установлено, что система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

Постановлением правительства РФ от 21 марта 2012 г. № 211 утвержден перечень необходимых мероприятий для обеспечения безопасности при работе с персональными данными.

Документом, регламентирующим защиту персональных данных, являются приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК) от 18 февраля 2013 г. № 21, а также приказ ФСТЭК от 11 февраля 2013 г. № 17 регламентирующий определение классов защищенности информации и соответствующие им методы защиты.

Кроме того, существуют нормативно-правовые акты, регламентирующие обработку персональных данных в уголовно-исполнительной системе. К ним относятся приказ ФСИН от 7 декабря 2009 г. № 478, который обязывает представлять сведения о доходах, а также регламентирует порядок размещения кадровыми подразделениями учрежде-

ний и органов ФСИН указанных сведений на официальных сайтах ФСИН России.

Приказом Минюста РФ от 21 марта 2013 г. № 36 утверждена прилагаемая типовая форма согласия на обработку персональных данных работников Министерства юстиции.

В целом под защитой персональных данных понимается комплекс мероприятий, позволяющий выполнить требования законодательства РФ, касающиеся обработки, хранения и передачи персональных данных.

Разберем на примере Академии ФСИН России необходимые действия при планировании обеспечения безопасности информационной системы персональных данных сотрудников, содержащей информацию согласно анкете, формируемой отделом кадров. Для этого необходимо ответить на ряд вопросов:

1. Определить цель обработки персональных данных. Это – сбор сведений о работниках с целью обеспечения соблюдения законодательства Российской Федерации в сфере отношений, связанных с поступлением на государственную службу и ее прохождением.

2. Определить ответственных должностных лиц за организацию обработки персональных данных. В соответствии с постановлением правительства РФ от 21 марта 2012 г. № 211 назначаются ответственные должностные лица с закреплением их обязанностей в должностной инструкции.

3. Определить необходимость предоставления согласия субъекта на обработку его персональных данных. Данное согласие необходимо в соответствии с требованиями приказа Минюста РФ от 21 марта 2013 г. № 36, которым утверждена типовая форма согласия субъекта на обработку персональных данных.

4. Определить состав обрабатываемых данных. Перечень персональных данных, обрабатываемых в Министерстве юстиции Российской Федерации в связи с реализацией трудовых отношений, утвержден приказом Минюста РФ от 21 марта 2013 г. № 36.

5. Определить категорию обрабатываемых данных. Данные, содержащиеся в анкете, относятся к информационным системам, обрабатывающим общедоступные персональные данные.

6. Определить тип существующих угроз безопасности персональных данных в соответствии с постановлением правительства РФ от 1 ноября 2012 г. № 1119. В данном случае актуальны угрозы 3-го типа, т. е. не связанные с наличием недокументированных возможностей в системном и прикладном программном обеспечении.

7. Определить необходимый уровень защищенности персональных данных с 1-го по 4-й уровень. В соответствии с постановлением правительства РФ от 1 ноября 2012 г. № 1119 в данном случае актуален 4-й уровень защищенности (самый низкий).

8. Определить необходимый класс защищенности персональных данных. В соответствии с приказом ФСТЭК от 11 февраля 2013 г. № 17 для персональной информации это 4-й уровень и класс защищенности информационной системы – К4.

9. Рассмотреть необходимость получения лицензии на проведение работ по защите персональных данных в соответствии с постановлением правительства РФ от 3 февраля 2012 г. № 79 либо возложить эти функции на специализированную организацию, имеющую такую лицензию.

10. Рассмотреть необходимость декларирования соответствия свойств и характеристик информационных систем персональных данных предъявляемым к ней требованиям, которые установлены законодательством РФ о персональных данных, а также нормативными и методическими документами Роскомнадзора, ФСТЭК и ФСБ России. Декларирование является одной из форм подтверждения соответствия наряду с аттестацией информационных систем персональных данных и осуществляется собственными силами либо с привлечением сторонних организаций или специалистов. В данном случае будет целесообразным выполнить декларирование соответствия.

Таким образом, мы рассмотрели простейший из примеров информационной системы обрабатывающей персональные данные, из которого видно, с каким количеством нормативных документов приходится иметь дело при организации обеспечения безопасности персональных данных в информационных системах. Необходимо отметить, что данная работа наряду с требованиями к знанию нормативной базы требует также знания технических и технологических процессов защиты информационных систем.

Мы считаем, что одним из путей решения проблемы защиты персональных данных будет упорядочивание законодательной базы в этой сфере. Например, издание ведомственного нормативного акта, такого, как «Концепция информационной безопасности при работе с информационными системами, содержащими персональные данные в ФСИН России», на основании которой будут разрабатываться локальные приказы и распоряжения, в подведомственных учреждениях ФСИН России. Предполагается, что данная концепция не будет базироваться на использовании отсылочных норм на законодательство Российской Федерации и будет регламентировать:

1. Ведение перечня информационных систем персональных данных, используемых в УФСИН России.

2. Порядок представления в Роскомнадзор сведений об операторе.

3. Разработку инструкций, определяющих порядок выполнения мероприятий по защите персональных данных, содержащихся в информационных системах УФСИН России.

4. Определение должностных обязанностей лиц, ответственных за организацию обработки персональных данных (разработка типовых должностных инструкций).

5. Порядок проведения аттестаций (декларирования соответствия) информационных систем, содержащих персональные данные.

Наличие подобного ведомственного правового акта позволит обеспечить единообразный подход к обработке и защите информации, используемой в органах ФСИН России, тем самым будут устранены имеющиеся недостатки при работе с персональными данными в подведомственных организациях УФСИН России. Осознавая необходимость исполнения подразделениями ФСИН России действующего законодательства в области защиты персональных данных, предполагаем, что рассматриваемая тема в настоящее время особенно актуальна и требует своего решения.

УДК 004.056

А.С. Кравченко, А.Г. Фадеев

КРИПТОЗАЩИТА ВЕДОМСТВЕННОЙ ИНФОРМАЦИИ В УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЕ НА ПРИМЕРЕ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Реализация угроз возможна практически на всех уровнях информационной структуры: физическом, сетевом, уровне сетевых приложений

и сервисов, операционных систем, систем управления базами данных, технологических процессов и приложений.

Оценка опасности в уголовно-исполнительной системе производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения: низкая опасность – реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных; средняя опасность – реализация угрозы может привести к негативным последствиям для субъектов персональных данных; высокая опасность – реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Рассмотрим нарушителей безопасности информационных систем в УИС России. По признаку принадлежности к информационной системе передачи данных все нарушители делятся на две группы: внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны; внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны.

Наибольшую опасность представляют собой внешние нарушители. Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию только во время ее передачи по каналам связи. Следовательно, каналы передачи данных будут являться самыми уязвимыми местами в области защиты информации в УИС.

В соответствии с приведенными выше исследованиями угроз безопасности и примерной модели нарушителя можно составить модель реализации угроз безопасности в УИС (рис. 1).

Рис. 1. Модель реализации угроз информационной безопасности уголовно-исполнительной системы.

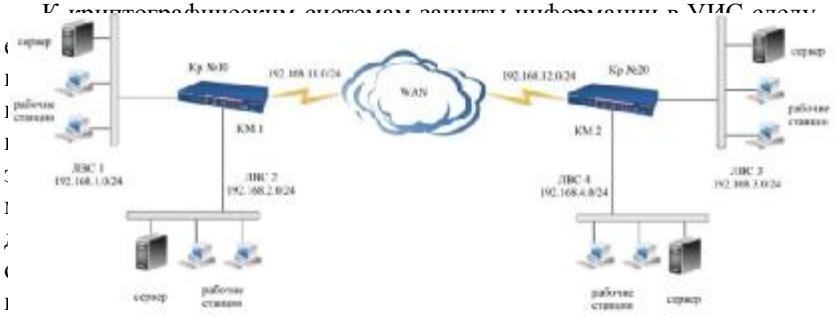
Единственным надежным способом защиты конфиденциальной информации при передаче по каналам связи большой протяженности будет являться ее криптографическое закрытие.

Под криптографической защитой информации понимается такое преобразование исходной информации, в результате которого она становится недоступной для ознакомления и использования лицами, не имеющими на это полномочий.

Основное достоинство криптографического метода в том, что он обеспечивает гарантированную высокую стойкость защиты передаваемой по каналу информации, которую можно рассчитать и выразить в числовой форме (временем, необходимым для раскрытия зашифрованной информации или вычисления ключей, средним числом операций).

Криптографическая защита данных может осуществляться как программно, так и аппаратно. Предпочтительнее использовать аппаратную реализацию, так как ей присущи следующие преимущества: простота, защищенность и высокая производительность.

К криптографическим системам защиты информации в УИС отлу-



но используемыми в процессе шифрования, не должно быть простых и легко устанавливаемых зависимостей; надежная защита информации должна обеспечиваться любым ключом из множества возможных; надежность защиты не должна зависеть от знания алгоритма шифрования; при незначительном изменении ключа должно происходить существенное изменение вида зашифрованного сообщения, даже при использовании одного и того же ключа; структурные элементы алгоритма шифрования должны быть неизменными; дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть надежно скрыты в шифрованном тексте.

Наиболее эффективным средством защиты, в данном случае выполняющим все вышеперечисленные требования, будет являться криптомаршрутизатор КМ-07.

Он сочетает в себе функции следующих устройств:

1. Многофункциональный IP-маршрутизатор (Ethernet, синхронные и асинхронные последовательные интерфейсы).

2. Терминальныйсервер, обеспечивающий доступ множества абонентов телефонной сети общего пользования к ресурсам TCP/IP сети.

3. Межсетевой экран длязащиты IP-сетей от несанкционированного доступа, попыток взлома и нарушения работоспособности.

4. Шифратор IP-потоков, позволяющий организовывать защищенное взаимодействие распределенных сегментов ведомственных сетей.

5. Сервер прикладных протоколов Internet, необходимых для обеспечения работы внутренних сегментов корпоративных сетей (DNS, DHCP, SNTP).

Совмещение функций межсетевого экрана и элементов криптографической защиты позволяет защитить ведомственную информацию как при ее передаче, так и непосредственно в ведомственной сети.

Приведем схему построения ведомственной локальной сети, в которую включен криптомаршрутизатор (КМ) (рис. 2).

Рис. 2. Схема ведомственной локальной сети
с включением нескольких ЛВС в один криптомаршрутизатор

Обмен данными через внешнюю сеть осуществляется с использованием КМ, причем две ЛВС подключены к одному КМ.

Для данной схемы предполагается наличие одного или нескольких серверов, находящихся внутри защищаемых ЛВС и имеющих статический IP-адрес.

Требования по разграничению взаимодействия между отдельными компонентами ЛВС следующие: две ЛВС, находящиеся под защитой одного КМ, не должны взаимодействовать друг с другом; ЛВС взаимодействуют через открытую сеть только с одной из других защищаемых ЛВС.

Настройки КМ в данном случае соответствуют следующим критериям: данные, передаваемые между КМ зашифрованы; блокируется обмен между ЛВС и внешней сетью.

Для рассматриваемого примера настройка каждого КМ предполагает настройку трех сетевых интерфейсов, два из которых должны быть подключены к защищаемым ЛВС, третий – к внешней (открытой) сети. При настройке интерфейсов выполняются следующие условия: для каждого интерфейса, подключенного к защищаемой ЛВС, выбран статический IP-адрес из диапазона, используемого в защищаемой ЛВС, к которой подключен интерфейс; интерфейсы постоянно активны при работе КМ (режим активизации интерфейса «статический»); интерфейс, подключенный к внешней (открытой) сети, обрабатывает только туннелированные датаграммы.

Результаты данного анализа эффективности решений по защите информации алгоритмами криптографической защиты при передаче ее по каналам связи УИС России позволяют разработать системные проектные решения по обеспечению комплексной защиты данных информационных систем ФСИН России в соответствии с требованиями законодательства Российской Федерации.

УДК 681.3

С.Е. Крупенко, В.И. Новосельцев, Д.Е. Скоробогатова

ОЦЕНКА КАЧЕСТВА ПРОЕКТНЫХ РЕШЕНИЙ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ СОЗДАНИИ БАЗ ЗНАНИЙ

Количественные критерии. В общем случае основной целью функционирования баз знаний (БЗ) является удовлетворение потребностей пользователей в обеспечении надежного и своевременного представления полной и достоверной информации. При этом безопасность информации является одним из необходимых условий достижения требуемого качества функционирования БЗ. Она определяется состоянием защищенности БЗ от различных угроз и в итоге способностью БЗ обеспечить конкретному пользователю доступность, целостность и конфиденциальность требуемой информации. Формируемые требования к качеству функционирования БЗ должны быть направлены на достижение цели ее применения при ограничениях на допустимые затраты и достигаемый уровень безопасности информации. При этом должно учитываться, что системные требования к качеству функционирования БЗ и обеспечению ее информационной безопасности являются взаимосвязанными.

В техническом задании на разработку БЗ и в постановках функциональных задач должны быть установлены системные требования к качеству процессов представления запрашиваемой (выдаваемой принудительно) выходной информации и выполнения задаваемых критичных технологических операций. Рекомендуется использовать следующие типовые формулировки:

«средняя наработка на отказ или сбой программно-технического средства объекта $T_{нар.}$ должна быть не менее $T_{нар.\ зад.}$ – задают для всех программно-технических средств и системы в целом;

среднее время восстановления объекта после отказа или сбоя $T_{вос.}$ должно быть не более $T_{вос.\ зад.}$ – задают для всех программно-технических средств и системы в целом;

коэффициент готовности объекта $K_г$ должен быть не менее $K_{г\ зад.}$ – задают для всех программно-технических средств и системы в целом».

Системные требования к достоверности информации и способам ее обеспечения образуют совокупность требований к актуальности, безошибочности и корректности обработки информации. При этом должны быть реализованы алгоритмы обеспечения истинности изначальных исходных данных, формирующих входную информацию БЗ. Рекомендуется использовать следующие типовые формулировки требований:

«алгоритм сбора и обновления информации должна обеспечивать актуальность информации, используемой пользователем. При этом вероятность $P_{акт.}$ сохранения актуальности конкретного типа информации на момент ее использования в определенный период функционирования должна быть не ниже $P_{акт.\ зад.}$;

качество прикладного программного обеспечения и квалификация его пользователей должны обеспечивать возможность получения корректных результатов обработки, при этом вероятность $P_{корр.}$ после получения корректных результатов обработки информации объемом V единиц за заданное время $T_{зад.}$ должна быть не ниже $P_{корр.\ зад.}$», при этом $T_{зад.}$ характеризуется временем, превышение которого может привести к ухудшению задаваемого уровня целостности системы.

При задании требований сохранения конфиденциальности информации в БЗ целесообразно использовать следующую типовую формулировку: «вероятность $P_{конф.}$ сохранения конфиденциальности конкретного типа информации в течение периода ее объективной конфиденциальности Тконф должна быть не ниже $P_{конф.\ зад.}$», при этом $T_{конф.}$, характеризуется средним временем, в течение которого нарушение конфиденциальности данного типа информации может привести к недопустимому ущербу в процессе функционирования системы.

Для задания требований по защищенности БЗ от опасных программно-технических воздействий целесообразно использовать следующую типовую формулировку: «вероятность отсутствия опасного воздействия $P_{возд.}$ в течение заданного периода функционирования БЗ $T_{зад.}$ должна быть не ниже $P_{возд.\ зад.}$», при этом длительность периода

$T_{зад.}$ выбирают исходя из того, что за это время должны быть решены конкретные задачи без какого-либо опасного программно-технического воздействия.

Качественные критерии. Для этой группы критериев характерно то, что они не выражаются числом в его метрическом понимании, а задаются либо в форме словесных формулировок, либо фиксируются на лингвистических шкалах, либо выражаются сравнительными категориями. К их числу относятся прагматические, технические, эксплуатационные, технологические и эргономические критерии.

Прагматические критерии характеризуют так называемую действенность БЗ, т. е. степень удовлетворения своего предназначения, и выражаются, например, такими сравнительными категориями, как полное, частичное, условное.

Технические критерии характеризуют уровень технического совершенства БЗ и ее компонентов (подсистем, узлов, блоков) и оцениваются с помощью лингвистических шкал типа высокий-низкий или таких категорий, как мировой уровень, отечественный уровень.

Эксплуатационные критерии характеризуют БЗ и ее компоненты с точки зрения удобства проведения различных организационно-технических мероприятий (настроек, профилактик, регламентных работ и т. п.). Их оценка основывается на качественных шкалах типа: удобно-неудобно, доступно-недоступно и других подобного характера.

Технологические критерии характеризуют уровень алгоритмов, использованных при проектировании БЗ и ее компонентов, а также уровень технологичности разработки спроектированной БЗ. Они (как и технические) оцениваются с помощью лингвистических шкал типа высокий-низкий или таких категорий, как мировой уровень, отечественный уровень.

Эргономические критерии характеризуют степень удобства общения пользователей с техническими и программными средствами БЗ, необходимый уровень обученности обслуживающего персонала и уровень специальной подготовки конечных пользователей и операторов данной БЗ.

Социальные критерии характеризуют социальные последствия использования БЗ в составе ИКС. Для оценки таких последствий пока не найдено универсальных шкал и методов их измерения (даже понятийных), поэтому для каждого класса БЗ используются свои специфические социальные критерии, отражающие особенности и характерные черты проблемной области и окружающей среды данного проекта.

УДК 002:004.056

С.В. Озёрский, Н.Б. Сенаторова

ПРОБЛЕМА МИНИМИЗАЦИИ ВЛИЯНИЯ ЧЕЛОВЕЧЕСКОГО ФАКТОРА НА БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В ОРГАНАХ И УЧРЕЖДЕНИЯХ УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ

Современный уровень информационных технологий достиг небывалых высот, однако и он не может обеспечить полную информационную безопасность учреждений Федеральной службы исполнения наказаний России, поскольку одним из неотъемлемых компонентов данной системы является человек.

Несомненно, что число угроз информационной безопасности в учреждениях и органах ФСИН стремительно растет во многом из-за появления все новых средств коммуникации и передачи информации (смартфоны, коммуникаторы и т. д.), но подавляющее число утечек происходит из-за присутствия в системе человека, который образует неискоренимый, по мнению многих экспертов, человеческий фактор. Роль человеческого фактора определяется, по мнению психологов, высокой степенью психологической неопределенности совершения преступления во времени и различной обстановке, когда желанию сотрудника разгласить конфиденциальную информацию в корыстных целях не могут помешать даже самые дорогостоящие средства и методы защиты.

Концепция развития уголовно-исполнительной системы Российской Федерации до 2020 года в качестве приоритетов указывает: на совершенствование мер предупреждения и пресечения возможных неслужебных связей личного состава уголовно-исполнительной системы с осужденными, преступных связей осужденных между собой и осужденных с лицами, находящимися за пределами исправительных учреждений.

Также в рассматриваемом документе указывается на важность введения мониторинга за поведением осужденных с помощью технологий электронного контроля (видеонаблюдение, электронные браслеты, беспроводные технологии и др.), но ничего не сказано о возможности повышения безопасности информации посредством технологий электронного контроля за сотрудниками, хотя представители экспертного сообщества на основе ряда исследований пришли к выводу, что системные сбои и человеческий фактор стали причиной $^{2}/_{3}$ всех утечек информации. К наиболее существенным составляющим причин вышеупомянутых утечек информации относятся: отсутствие у сотрудников

четкого представления о конфиденциальности информации и необходимости ее сохранения, недостаточность системного контроля (средств управления системой), а также несоблюдение государственных и отраслевых нормативов.

Информационная безопасность в учреждениях и органах ФСИН касается конфиденциальности, целостности и доступности данных независимо от формы их представления: электронных, печатных, вербальных или любых других.

Важно понимать, что информационная безопасность – это не продукт, а непрерывный, требующий постоянного контроля и корректив процесс. Отметим также, что информационная безопасность в уголовно-исполнительной системе в большей степени проблема людей и управления, нежели технологическая проблема.

В то время как разработчики средств информационной безопасности в УИС совершенствуются в создании эффективных и малозатратных технологий защиты, затрудняющих возможность использования технических уязвимостей, атакующие все чаще используют человеческий фактор. К основным причинам, способствующим ошибочным действиям сотрудника ФСИН в вопросах информационной безопасности, относятся: недостатки информационного обеспечения или их отсутствие (наглядные материалы и инструкции); ошибки, вызванные воздействием внешних факторов (отвлечение внимания от возникшей проблемы); ошибки, вызванные физическим и психологическим состоянием и свойствами человека (внезапный стресс при общей монотонной работе, эмоциональная напряженность, импульсивность или наоборот, подавление реакции на проблему); ограниченность ресурсов поддержки и исполнения принятого решения; отсутствие человеческого фактора в списке возможных причин инцидента.

Одним из надежных способов повышения информационной безопасности является видеонаблюдение за сотрудниками ФСИН. Видеонаблюдение – это неотъемлемая часть почти любой современной системы безопасности. Главная функция систем охранного телевидения (СОТ) – это оценка ситуации на контролируемой территории. Чтобы оператор СОТ мог оперативно и адекватно оценивать ситуацию, подсистема должна быть эффективно спроектирована и установлена в полном соответствии с проектом. Не должно быть «слепых», неконтролируемых зон или вследствие объективных причин количество и размеры таких зон должны быть минимальными. В СОТ не должно быть слишком много камер. Излишнее дублирование сцен, отражаемых видеокамерами, может ввести оператора СОТ в заблуждение или увеличить время принятия решения. Кроме того, чем больше камер у

оператора, тем сложнее ему с ними управляться, тем мощнее требуется оборудование для обработки видеопотоков и больше места для хранения архивных видеозаписей.

Методика минимизации влияния человеческого фактора на эффективность политики безопасности изучена на опыте видеонаблюдения в лекционных залах и специализированных учебных аудиториях в Самарском юридическом институте ФСИН России. Можно сделать однозначный вывод о повышении дисциплины как со стороны курсантов и слушателей, так и со стороны преподавательского состава.

Интересен положительный опыт зарубежных коллег. В польской тюрьме (одной из самых современных в мире), расположенной в городе Петркув-Трибунальский, видеонаблюдение установлено в каждом служебном помещении, кроме туалетов. Видеосигнал подается на пульт дежурного сотрудника и дублируется в кабинете начальника тюрьмы, что исключает сговор между сотрудниками тюрьмы. Таким образом, мы наблюдаем многоуровневую систему контроля, которая обеспечивает минимизацию человеческого фактора.

Еще одним важным направлением в минимизации человеческого фактора является внедрение систем конфиденциального электронного делопроизводства. Концепция развития УИС до 2020 года предусматривает внедрение электронного делопроизводства, включая оснащение всех учреждений и органов уголовно-исполнительной системы автоматизированными рабочими местами, формирование и ведение регистра унифицированной системы электронных документов, перевод в цифровой формат 100 % документов информационных фондов и архивов учреждений и органов уголовно-исполнительной системы к 2020 г., дальнейшее развитие сети специальной связи в целях обеспечения информационной безопасности уголовно-исполнительной системы, участие в создании и развитии межведомственных сетей передачи шифрованной информации органов государственной власти, организация на их основе межведомственного электронного документооборота, комплексов информационного взаимодействия.

После проведенного анализа для минимизации влияния человеческого фактора на утечку информации можно рекомендовать следующие мероприятия: использование «Полиграфа» (детектора лжи) при приеме сотрудников, назначаемых на должности, связанные с обработкой информации ограниченного доступа; многоуровневый контроль за сотрудниками с помощью видеонаблюдения; внезапные проверки, провокационные ситуации (для выявления ненадежных сотрудников); использование систем электронного документооборота с разграничением прав доступа; сужение круга сотрудников, имеющих доступ к

информации, не подлежащей разглашению (в том числе посредством внедрения систем электронного документооборота).

Так как работа в учреждениях системы ФСИН является стрессовой для сотрудников, вероятность совершения ошибки значительно превышает средний уровень. Соответственно, минимизация влияния человеческого фактора, является первоочередной задачей для повышения информационной безопасности в данной сфере. Наиболее эффективное средство для достижения этой цели – создание высокотехнологической современной системы защиты информации, включающее в себя следующие компоненты: нормативно-правовой, организационный, технический, технологический.

При создании системы тотального видеоконтроля в учреждениях ФСИН необходимо при помощи современных средств имитационного моделирования и привлечения высококвалифицированных экспертов избегать возможных «белых пятен» в эффективности работы рассматриваемых систем.

Таким образом, политика в области управления личным составом является узловым компонентом системы информационной безопасности ФСИН для минимизации влияния человеческого фактора, являющегося основной угрозой безопасности информации.

УДК 343.851.3

А.М. Рудаков

РЕАЛИЗАЦИЯ ОСУЖДЕННЫМИ СВОБОДЫ СОВЕСТИ КАК ОДНА ИЗ ФОРМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В УЧРЕЖДЕНИЯХ УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ: ИНФОРМАЦИОННЫЙ АСПЕКТ

Безопасность (в соответствии с прежним законом Российской Федерации от 5 марта 1992 г. № 2446-ФЗ «О безопасности») – это состояние защищенности жизненно важных интересов, личности, общества и государства от внутренних и внешних угроз. Новый федеральный закон Российской Федерации от 28 декабря 2010 г. № 390-ФЗ «О безопасности» не содержит определения понятия «безопасность», тем не менее в содержание деятельности по обеспечению безопасности входит выявление, анализ и оценка угроз безопасности, их предупреждение и устранение, локализация и нейтрализация последствий их проявления, организация научной деятельности в области обеспечения безопасности. Под угрозой безопасности закон понимает совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

В частности, угроза безопасности может исходить от специфического мышления и соответствующего поведения как отдельного осужденного, так и группы осужденных. Само слово «поведение» состоит из двух частей: «по» и «ведение». Слово «ведение», «ведать», по В.И. Далю, – знать, иметь сведения о чем-то, т. е. осужденный действует так, как знает, какой информацией обладает. Поведение – рефлексия на полученную и воспринятую информацию. Согласно ст. 28 Конституции РФ человек действует в соответствии со своими убеждениями, реализуя, таким образом, свободу совести.

Наше понимание свободы совести в рассматриваемом аспекте исходит из понятия совести как свободы выбора ориентира для самоопределения субъекта правоиспользования и его способности нести ответственность за сделанный выбор, в том числе при принятии им решения на основе собственных убеждений. Иными словами, осужденный является субъектом – получателем информации, использующим ее для формирования собственных убеждений, принятия на их основе решений.

Необходимо сказать, что жизнедеятельность любого человека – это непрерывная цепочка принятия деловых и личных решений, их реализация. Поскольку часто решения людьми принимаются в состоянии разной степени неопределенности, задача норм права – максимально снизить уровень неопределенности посредством гарантий со стороны государства (ст. 28 Конституции РФ, ст. 3 и 4 федерального закона «О свободе совести и религиозных организациях» и п. 1 ст. 14 УИК РФ), предоставить субъекту полную и объективную информацию для ее использования в принятии решения.

По нашему мнению, под гарантиями реализации осужденными права на свободу совести должно пониматься следующее: во-первых, обеспечение открытости информации. Она должна быть представлена в очевидной форме при помощи разъяснений и ссылок на соответствующие нормативные источники, научные исследования, в случае отсутствия таких доказательств потребитель информации – субъект, принимающий решения, должен быть осведомлен об этом до принятия им решения.

Во-вторых, защита субъекта правоиспользования от нарушений свободы совести. Нарушениями свободы совести являются любое сознательное введение в заблуждение (обман), укрывательство или иное искажение информации (как правило, с целью спровоцировать требуемое поведение от субъекта – получателя информации) или сознательное ее замалчивание (если только оно не вызвано интересами государственной безопасности или сохранением тайны личной жизни третьих лиц), так как перечисленные действия препятствует свободному при-

нятию субъектом решения или напрямую способствуют принятию субъектом ошибочного решения.

В настоящее время мы постоянно сталкиваемся с беспринципным искажением информации, ее укрывательством, сознательным замалчиванием или напрямую с введением в заблуждение. Субъектами, искажающими информацию, часто являются средства массовой информации: телевизионные программы, интернет, радиопередачи, журналы, книги, компьютерные программы и т. д., а также деструктивные организации, иные организации, спекулирующие на неосведомленности граждан в тонкостях правовых, экономических, психологических (духовных) и иных социальных вопросов. Иногда субъектами, искажающими информацию, становятся как раз те организации, которые непосредственно должны быть гарантами ее истинности. Что касается вопросов внутренней безопасности учреждения, то субъектами, искажающими информацию, могут быть группы осужденных отрицательной направленности, которые, искажая информацию, побуждают других осужденных к пропаганде криминальных ценностей, нарушениям установленного порядка отбывания наказания.

Опасность искажения информации состоит в следующем: сформированные на основе искаженной информации убеждения могут способствовать принятию неверных решений. Иначе говоря, в конкретной ситуации субъект полагает, что действует правильно, так как, принимая решение, он исходит из тех убеждений, которые считает верными, правильными, соответствующими той информации, которая ранее была преподнесена ему как правильная. Но ввиду того что ранее эта преподнесенная информация была в значительной степени искажена, принятое решение стало неверным, ошибочным, к тому же оно может привести и к негативным последствиям, например нарушению прав других людей, преступлению.

При этом субъект принятия решения – осужденный, не воспринимает свои действия как ошибочные, как нарушение норм общества, поскольку он считает, что действовал в соответствии со своими убеждениями, которые, в свою очередь, были сформированы из полученной из того же общества информации. И если такая информация им все же получена и при этом никаким образом не была ограничена государством (например, выражено предупреждение, предоставлено разъяснение о возможных вредных последствиях, о значении результата воздействия этой информации для заинтересованных лиц), или иным образом не раскрыто ее истинное содержание и значение, субъект, принимающий такую информацию, определяет ее как верную, правильную, поскольку позиция современной системы права гласит: разрешено все, что не запрещено законом.

Именно раскрытие истинного содержания и значения той информации, которая сформировала искаженные убеждения лиц, преступивших закон, является одной из основных задач профилактической работы с осужденными. Главенствующую роль в работе по организации реализации осужденными свободы совести призван сыграть метод разъяснения.

Таким образом, убеждение как элемент свободы совести – это готовый алгоритм поведения, основанный на устойчивых знаниях, сформированных в сознании из полученной информации. Поэтому для того чтобы скорректировать убеждения правонарушителя, необходимо предоставить ему полные и достоверные сведения, раскрывающие истинное содержание и значение той информации, на которой строятся его (осужденного) убеждения. Но, раскрыв прежнюю искаженную информацию, необходимо предоставить альтернативную, правильную, разобранную до очевидности, при необходимости научно обоснованную. Для этого ее необходимо иметь и в последующем помочь адаптировать социально полезную, правовую информацию непосредственно конкретным осужденным для себя при поддержке сотрудников с учетом психологических и физиологических особенностей, помочь выработать на ее основе новые убеждения. Именно это должно стать одной из основных задач индивидуального подхода в работе с осужденными, учитываться при реализации направлений воспитательной работы с осужденными: нравственном, правовом, трудовом, физическом, этическом, половом и т. д.

Используя полученную информацию и методологию из изложенных ресурсов, необходимо раскрыть природу и историю идеологий потребления, «культурного пития», культа секса и насилия, наркотизации, идеологии преступного сообщества, таких идеологических направлений, как «эмо», «готы», «чайлдфри», «цветные» революции, национализма и иных идеологических направлений, имеющих скрытые деструктивные цели, а также сущность и цели деятельности организаций, позиционирующих себя как научные, одновременно с этим имеющие скрытые намерения (например, МУДО Центр медико-психологической и социальной помощи населению «Холис»).

Таким образом, обеспечив реализацию осужденными свободы совести – свободы выбирать и иметь свои убеждения, системы ценностей, обучив осужденных навыкам критического мышления, администрация тем самым способствует повышению уровня доверия к сотрудникам со стороны осужденных, повышению степени контроля за оперативной обстановкой в учреждении и качества управления коллективом осужденных, препятствуя слепому следованию осужденных за преступными и деструктивными авторитетами с целью дестабилизации обстановки в учреждении, реализации иных угроз безопасности.

УДК 651.23

В.Н. Ручкин, Г.В. Ручкин, В.В. Фомин

ИНТЕЛЛЕКТУАЛЬНЫЕ ВОЗМОЖНОСТИ БЕЗОПАСНОСТИ УЧРЕЖДЕНИЙ УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ

Интернет – чудо информационно-коммуникационных технологий XX в. представляет идеальное пространство для реализации компьютерных или кибернетических преступлений. Число сообщений о проникновении в корпоративные сети и атаках на web-серверы постоянно возрастает, прогнозируется тенденция дальнейшего роста. Причем интернет-атаки на различные компьютерные системы прокатываются как цунами, не зная ни государственных границ, ни расовых или социальных различий. Злоумышленники прячутся под логинами авторизованных пользователей, используют промежуточные узлы для сокрытия своего истинного адреса и осуществляют атаки, распределенные по времени в течение нескольких часов и в пространстве одновременно с нескольких узлов. Процесс обнаружения таких атак является неоднозначным и нет стопроцентной гарантии осуществления атаки или с той же вероятностью обеспечения безопасности системы. Существующие современные системы обнаружения далеки от совершенства и часто не замечают настоящую атаку и генерируют большое число ложных тревог. В некоторых случаях большинство краж данных происходят не благодаря хитроумным способам, а из-за небрежности и невнимательности самих пользователей. Поэтому актуальной проблемой обеспечения безопасности любой организации, включая и Федеральную службу исполнения наказаний России, является создание интеллектуальных систем информационной безопасности (ИСИБ) с учетом постоянно возрастающего объема различных атак.

Компонентами концептуальной модели информационной безопасности являются: объекты угроз; угрозы; источники угроз; цели угроз со стороны злоумышленников; методы защиты; средства защиты. Они и составляют базу знаний в виде различных моделей: продукционная, семантические сети, фрэймы, нейронные сети. Они определяют управление доступом и включают следующие функции защиты:

идентификация пользователей, ресурсов и персонала системы информационной безопасности сети;

опознание и установление подлинности пользователя по вводимым данным;

допуск к определенным условиям работы согласно регламенту, предписанному каждому отдельному пользователю;

протоколирование обращений пользователей к ресурсам, информационная безопасность которых защищает ресурсы от несанкционированного доступа и отслеживает некорректное поведение пользователей системы;

информационная безопасность банков и экономическая информационная безопасность.

Исходя из этого, рассматривают и меры защиты информации от неправомерных действий, приводящих к нанесению ущерба. Предлагается использование большого числа способов защиты информации в виде многоуровневой организации, внедрения аппаратной защиты информации, повышения качества программной защиты информации, развития комплексной аппаратно-программной защиты ИСИБ.

В процессе защиты информации различают: атаку – это любое действие нарушителя, которое приводит к реализации угрозы путем использования уязвимостей вычислительной системы; обнаружение атак – это процесс идентификации и реагирования на подозрительную деятельность, направленную на вычислительные или сетевые ресурсы и система обнаружения атак (Intrusion Detection Systems, IDS). Последнее представляет собой широкую область, охватывающую многие аспекты, начиная с датчиков движения и систем видеонаблюдения и заканчивая системами обнаружения мошенничества в реальном времени.

В настоящее время комплексные технологии используют совокупность методов обнаружения атак: анализ журналов регистрации (log, audit, trail); анализ «на лету» заключается в мониторинге сетевого трафика в реальном или близком к реальному времени; использование профилей «нормального» поведения для наблюдения за пользователями, системной деятельностью или сетевым трафиком; использование сигнатур атак заключается в описании атаки в виде сигнатуры (signature) и поиска данной сигнатуры в контролируемом пространстве (сетевом трафике, журнале регистрации и т. д.); анализ и корреляция данных на основе статистического метода, использования экспертных систем и нейронных сетей.

Для реализации интеллектуальных IDS используют экспертные системы, которые представляют наиболее распространенную форму подходов к обнаружению атак на основе правил, записанных в виде последовательности действий или сигнатуры базирующихся на знаниях эксперта. Основным достоинством такого подхода является практически полное отсутствие ложных тревог. Однако игнорирование обновлений или обновление вручную администратором как минимум приведет к снижению защищенности. Кроме того, любое разделение атаки либо во времени, либо среди нескольких злоумышленников является трудным для обнаружения при помощи экспертных

систем. Более того, сетевые атаки постоянно изменяются, поскольку хакеры используют индивидуальные подходы. Перечисленные недостатки усиливаются вследствие регулярности изменения программного обеспечения (ПО) и аппаратных средств. Поэтому одним из перспективных путей устранения названных проблем является использование нейронных сетей.

Нейросеть проводит анализ информации и предоставляет возможность оценить согласование данных с характеристиками, которые она обучена распознавать. Первоначально нейросеть обучается путем правильной идентификации предварительно выбранных примеров предметной области. Реакция нейросети анализируется и система настраивается с целью достижения удовлетворительных результатов. С течением времени по мере накопления данных нейросеть набирается опыта, обучается и переходит в режим автоматического слежения, обнаружения и предотвращения несанкционированного доступа.

Искусственная нейросеть (Artificial Neural Network) состоит из набора элементарных взаимосвязанных между собой элементов-нейронов и трансформирует набор входных данных во множество желаемых выходных сигналов. При этом результат преобразования определяется характеристиками самих элементов и весовыми коэффициентами, соответствующими взаимосвязи между ними. Широкое применение они нашли в системах распознавания образов, обработки сигналов, предсказания и диагностики, в робототехнических и бортовых системах, криптографии и других сферах народного хозяйства. Поэтому применение нейронных сетей в интеллектуальных системах ФСИН оправданно тем, что отсутствует алгоритм или неизвестны принципы решения задач, но накоплено достаточное число примеров; проблема характеризуется большими объемами входной информации; данные неполны или избыточны, изменены, частично противоречивы. Все эти признаки в той или иной степени характерны для хакерских атак.

Наиболее важное преимущество нейросетей при обнаружении злоупотреблений заключается в их способности изучать характеристики умышленных атак и идентифицировать элементы, которые не похожи на наблюдаемые в сети прежде. Кроме того, нейросети поддерживаются аппаратными средствами на базе отечественных нейропроцессоров NM 640X и процессоров ELBRUS. Более того, нейропроцессоры NM 640X объединяются в мощные мультинейропроцессорные системы, а ELBRUS представляет собой многоядерный процессор. В результате появляется возможность создавать интеллектуальные системы с достаточным быстродействием для противодействия хакерским атакам в реальном времени.

В ходе разработки, внедрения, эксплуатации государственных ИС субъектам правоотношений может быть причинен: материальный ущерб от разглашения защищаемой информации; материальный, моральный ущерб от неправомерных действий с объектами защиты; материальный, физический и моральный ущерб личности от разглашения персональных данных.

При этом причиненный ущерб может квалифицироваться как состав преступления, предусмотренный уголовным правом или сопоставляться с рисками утраты, предусмотренными гражданским, административным или арбитражным правом.

Потеря конфиденциальной информации как главного ресурса приносит материальный, физический и моральный ущерб организации, государству, ФСИН России и человеку, что квалифицируется как состав преступления, предусмотренный уголовным правом.

Неограниченное разнообразие атак и хакеров в условиях регулярности изменения ПО и аппаратных средствах требует применения аппаратных средств на базе отечественных нейропроцессоров NM 640X и процессоров ELBRUS для создания интеллектуальных нейросетевых систем обнаружения атак, регистрации нестандартных, распределенных во времени и пространстве с нескольких узлов атаки, снижение затрат на обслуживание за счет самообучающихся алгоритмов обеспечения заданной информационной безопасности.

УДК 004

М.Е. Рычаго

НЕКОТОРЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ НА ОБЪЕКТАХ УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ

Конец прошлого и начало нынешнего тысячелетия ознаменовались для человечества резким увеличением чрезвычайных ситуаций (ЧС) техногенного, природного и социального происхождения. Масштабы последствий в таких случаях трудно переоценить. Практически все модели и системы принятия решения в условиях чрезвычайных ситуаций ЧС, связанные с техногенными катастрофами или природными явлениями, дают возможность разработать ряд сценариев и выбрать из них оптимальный, так как события более или менее растянуты во времени. В условиях же ЧС социального характера, когда информация

быстро меняется и подчас противоречивая, времени на исследование вариантов решений практически нет.

Прежде всего, отметим, что любая ЧС характеризуется рядом количественных и качественных показателей, которые имеют различную степень информативности для лица, принимающего решение (далее – ЛПР). Чтобы обеспечить объективную оценку ситуации, необходимо выделить наиболее информативные показатели, которые уменьшают энтропию системы.

Очень часто в условиях ЧС при анализе интересующей нас структуры число элементов и их взаимосвязей столь велико, что превышает способность ЛПР воспринимать информацию в полном объеме. В таких случаях система делится на подсистемы. Элементы в каждой группе (называемой уровнем или кластером) независимы. В сложной ЧС нельзя надеяться на то, что проблемы могут быть разрешены интуитивным, а не четко сформулированным пониманием важнейших факторов. Если ЛПР сталкивается с некоторым количеством действий, среди которых нужно сделать выбор, необходимо попарно сравнить критерии и построить матрицу попарных сравнений относительно их эффективности.

Рассмотрим следующий важный пример, разработанный группой ученых под руководством профессора Национального университета внутренних дел Украины Н.М. Зацеркляного, предложившего математическую модель иерархического типа, позволяющую определить приоритеты в сложных условиях ЧС социального характера. В частности, была предложена следующая модель массовых беспорядков (МБ), содержащая в себе 3-уровневую иерархическую структуру. Первый уровень характеризует причины возникновения МБ: сепаратизм, политические, религиозные, социально-экономические, хулиганские действия. Второй уровень отражает состав участников по полу и возрасту: мужчины до 30 лет, мужчины от 30 до 50 лет, мужчины старше 50 и аналогично для женщин. Третий уровень характеризует состояние участников: вооруженный нетрезвый, вооруженный трезвый, невооруженный нетрезвый, невооруженный трезвый.

Построение иерархий, т. е. специального типа упорядоченных множеств, может служить мощным инструментом исследования большого числа элементов, группируемых в кластеры в соответствии с их относительной значимостью. В результате вся сложная и многообразная система факторов, влияющих на ЧС, представляется в виде нескольких кластеров (уровней): самые важные элементы, умеренно важные и т. п. Так, в указанном выше примере количественные характеристики второго и третьего уровней оказывают значительное влияние на элементы первого уровня.

С точки зрения известного ученого и специалиста в области исследования мировых террористических угроз В.С. Овчинского, на сегодняшний день приходится констатировать существенное изменение самого характера протекания современных явлений, связанных с массовыми беспорядками, в том числе и в местах лишения свободы. Истинной целью зачинщиков массовых беспорядков могут стать сегодня не столько заявляемые ими традиционные претензии к администрации учреждений, сколько желание вызвать реакцию средств массовой информации, общественный резонанс и т. п. Специфика сегодняшнего времени такова, что доля информации, получаемая отдельными людьми из информационных источников (телевидение, радио, газеты, журналы, книги, интернет и др.), становится значительно больше доли информации, получаемой ими из непосредственного личного общения. В результате возникает возможность информационно-психологического воздействия как на отдельного человека, так и на общественное мнение в целом, что хорошо прослеживается в продолжающейся «информационной войне», развернувшейся в мировых средствах массовой информации вокруг острых общественных событий, вызванных украинским кризисом.

Сам факт информационного воздействия не вызывает тревоги при условии, если он осуществляется по цивилизованным правилам. Но есть множество причин неадекватно отражать окружающий мир и вводить людей в заблуждение. В этом случае возникает феномен манипулирования информацией, информационно-психологической агрессии по отношению к отдельному человеку, когда против воли и желания модифицируют его мировоззрение и поведение.

Поскольку главным источником информационного влияния на человека являются средства массовой информации, их реакция и общественный отклик очень важны для зачинщиков массовых беспорядков и являются иногда их основными целями. Причем достижение этих особых и завуалированных целей может иметь определяющее значение для участников массового протеста по сравнению, например, с требованием о смене руководства того или иного исправительного учреждения. Важно отметить, что реализация таких скрытых намерений осужденных часто диктуется и режиссируется из-за пределов мест лишения свободы, в том числе из-за рубежа. В связи с этим встает необходимость качественного изменения работы оперативных подразделений, учитывая информационные процессы, протекающие в обществе, позволяя устанавливать связи между негативными проявлениями массового характера в конкретном учреждении исполнения наказаний с определенными событиями в стране и мире. Такое новое качество современного оперативного подразделения названо В.С. Овчинским «дея-

тельностью в информационном пространстве», призванной наряду с традиционными мероприятиями повысить эффективность принятия решений при борьбе с фактами МБ.

В данной работе предлагается по-новому взглянуть и несколько дополнить рассмотренную выше математическую модель МБ новым уровнем, отражающим возможную реакцию средств массовой информации и (или) правозащитных организаций. Этот уровень, как и все другие, может состоять из большого числа элементов, но для простоты изложения мы ограничимся здесь тремя элементами, условно обозначающими реакции региональных (Р), федеральных (Ф) или международных (М) СМИ.

Математическая техника, применяемая для анализа иерархических моделей указанного типа, основана на отыскании собственного вектора так называемой матрицы попарных сравнений, построенной по исходным данным, получаемым, возможно, оперативным путем. Пусть, например сразу же после возникновения МБ в определенном учреждении ФСИН России были зафиксированы 14 сообщений об этих событиях в различных средствах массовой информации или со стороны правозащитных организаций, причем 2 из них были зафиксированы на местном уровне, 5 – на федеральном и 7 – на международном. Тогда матрица попарных сравнений может быть составлена путем вычисления соотношений вида: Ф : Р = 5 : 2, Р : Ф = 2 : 5, М : Р = 7 : 2, Р : М = 2 : 7, М : Ф = 7 : 5, Ф : М = 5 : 7.

Поскольку эта матрица обратно симметрическая (ее элементы, симметричные относительно главной диагонали, взаимно обратны), то стандартная задача линейной алгебры на собственные значения существенно упрощается и может быть сведена к простой процедуре последовательного пересчета исходной матрицы, предложенной украинскими авторами. В любом случае математическая техника легко автоматизируется, в том числе средствами широко известных электронных таблиц. Нормированный собственный вектор рассмотренной матрицы попарных сравнений примет вид (0,14; 0,36; 0,5) и показывает условные баллы элементов данного уровня, свидетельствующие о приоритете международных откликов на ЧС со стороны СМИ и международных правозащитных организаций. Дальнейшее следование вычислительному алгоритму позволяет выделить доминирующие показатели на других уровнях иерархической структуры МБ (причины, состав и состояние участников) и получить комплексную оценку ЧС в целом. Такая комплексная оценка должна, безусловно, помочь ЛПР при выработке наиболее эффективного управленческого решения.

Данная модель и связанная с ней техника расчета позволяют получить именно комплексную оценку всех параметров, которая становится

все менее очевидной при большом числе исследуемых элементов. Так, достаточно увеличить число компонент последнего уровня, учитывая, к примеру, реакцию СМИ и правозащитников отдельно (или разделить дополнительно электронные и печатные СМИ), как выводы потеряют свою очевидность.

В заключении отметим, что рассмотренная иерархическая модель, включающая в себя кластер информационной безопасности, в течении ряда лет подробно изучалась на кафедре специальной техники и информационных технологий Владимирского юридического института ФСИН России. Весь вычислительный аппарат, применяющийся в данной модели, автоматизирован с помощью программных средств и внедрен в образовательный процесс. Видится перспективным, как с теоретической, так и с практической точки зрения, проведение апробации и проверки эффективности данной модели на фактическом статистическом материале, отражающем факты МБ, имевшие место на объектах УИС.

УДК 004.056.5

П.А. Сидельников, С.Л. Сахаров

ОРГАНИЗАЦИЯ МОНИТОРИНГА ПРОГРАММНОЙ И АППАРАТНОЙ КОНФИГУРАЦИЙ ЛОКАЛЬНОЙ СЕТИ УЧРЕЖДЕНИЯ

Сети на основе сервера стали промышленным стандартом, и их использование в уголовно-исполнительной системе необходимо учитывать при разработке и планировании мероприятий, реализующих политику информационной безопасности каждого учреждения. На основе политики безопасности устанавливаются необходимые средства и процедуры безопасности, а также определяются роли и ответственность сотрудников организации.

Политика безопасности учреждения должна устанавливать, как обрабатывать информацию, кто и как может получить к ней доступ. Работа по созданию системы безопасности должны выполняться постепенно и последовательно. Структура и состав политики безопасности зависит от объема и назначения обрабатываемой информации и обеспечивается набором специализированных политик и процедур.

К специализированным политикам (затрагивающим значительное число пользователей) относятся: политика допустимого использования (норм безопасного использования компьютерного оборудования и сервисов); политика защиты информации; политика защиты паролей и др.

К специализированным политикам (связанным с конкретными техническими областями) относятся: политика конфигурации межсетевых экранов; политика безопасности виртуальных защищенных сетей VPN; политика по оборудованию беспроводной сети и др.

Конкретный тип и количество политик зависят от результатов анализа условий обработки информации и оценки рисков в учреждении.

На долю пользователей и обслуживающего персонала приходится более половины всех случаев нарушения правил обеспечения безопасности информации. Как преднамеренные, так и непреднамеренные угрозы связаны главным образом со сбоями и отказами технических и программных средств. Реализация угроз приводит, как правило, к нарушению достоверности, сохранности и конфиденциальности информации. Причиной возникновения угроз являются несанкционированные действия пользователя: установка непроверенных или нелицензионных программ (в том числе и автоматическая установка со съемных носителей), установка несовместимых аппаратных устройств и т. д.

Опыт работы системных администраторов различных учреждений и организаций позволяет сделать вывод, что рядовой пользователь либо игнорирует меры безопасности, либо неохотно и не в полной мере придерживается установленных правил.

Процедуры безопасности являются необходимым и важным дополнением к политикам безопасности. Политики безопасности только описывают, что должно быть защищено и каковы основные правила защиты. Процедуры безопасности определяют, как защитить ресурсы и каковы механизмы исполнения политики. По существу, процедуры безопасности представляют собой пошаговые инструкции для выполнения оперативных задач. Часто процедура является тем инструментом, с помощью которого политика преобразуется в реальное действие. Например, политика паролей формулирует правила конструирования паролей, правила о том, как защитить пароль и как часто его заменять.

Многие процедуры, связанные с безопасностью, должны быть стандартными средствами в любом подразделении. В качестве примеров можно указать процедуры для резервного копирования и внесистемного хранения защищенных копий, а также процедуры для вывода пользователя из активного состояния и (или) архивирования логина и пароля пользователя, применяемые сразу, как только данный пользователь увольняется из организации.

Практически невозможно указать отклики на все события нарушений безопасности, но нужно стремиться охватить основные типы нарушений, которые могут произойти, поэтому необходимо определять: обязанности должностных лиц; тип защищаемой информации; мероприятия, проводимые при выявлении нарушений; мероприятия по профилактике типовых нарушений.

Учитывая специфику информации учреждений уголовно-исполнительной системы, среди процедур обеспечения информационной безопасности в обязательном порядке должны присутствовать меры по контролю целостности и работоспособности программного и аппаратного обеспечения рабочих станций пользователей.

Контроль и управление аппаратной и программной конфигурацией обычно определяется на уровне учреждения и его подразделений с учетом специфики их работы. Эта мероприятия должны определять процесс документирования и запроса изменений конфигурации на всех уровнях принятия решений. Должностное лицо, исполняющее обязанности системного администратора, должно быть наделено правами рассматривать все запросы на изменения конфигурации и принимать необходимые решения о распределении полномочий и документировании изменений.

Процесс управления конфигурацией важен, так как документирует сделанные изменения и обеспечивает возможность аудита; документирует возможный простой системы; дает способ координировать изменения так, чтобы одно изменение не помешало другому.

Для успешного администрирования сети полезно иметь представление об используемых в ней компонентах и возможностях современного программного обеспечения инвентаризации локальной компьютерной сети организации.

Зарекомендовавшая себя программа «10-Страйк: Инвентаризация Компьютеров» для инвентаризации компьютеров в локальных сетях позволяет администраторам сетей создать и вести базу данных компьютеров, комплектующих, программ и лицензий. Имеется возможность по сети просматривать и отслеживать конфигурации удаленных компьютеров, вести учет аппаратного и программного обеспечения на них.

Собрав информацию в инвентарную базу данных, администратор сможет узнать типы установленных процессоров, количество оперативной памяти, типы и объемы жестких дисков, получить информацию о разделах дисков, CD/DVD-приводах, использующихся USB-накопителях, видеокартах, принтерах, установленной операционной системе, приложениях и используемых серийных номерах, ярлыках в автозагрузке, вести учет практически всего использующегося аппаратного и программного обеспечения компьютеров сети, подготавливать и печа-

тать любые отчеты. В новых версиях поддерживается опрос компьютеров с Linux и устройств на Android.

PKCC Inspector предназначен для автоматизации контроля конфигураций, текущих настроек и объектов файловой системы сетевого оборудования, хранение версий конфигураций. Возможности этого программного средства позволяют осуществлять: контроль неизменности настроек сетевых устройств; проверку контроля целостности по расписанию или по требованию; автоматическое взаимодействие с сетевыми устройствами; восстановление файлов на локальных дисках сетевых устройств; автоматическое выполнение заданных команд как реакции на нарушения; просмотр и сравнение версий файлов и выводов команд; ведение журнала выполненных операций.

Разработчиками получен сертификат ФСТЭК России № 2362 от 7 июня 2011 г., согласно которому PKCC Inspector является программным средством контроля защищенности информации, не содержащий сведения, составляющие государственную тайну.

Spiceworks Desktop является бесплатной программой инвентаризации оборудования, программного обеспечения и других доступных ресурсов, которая обнаруживает все присутствующие в сети Windows, Mac и Linux-системы, серверы, маршрутизаторы, принтеры и другие устройства, собирает информацию об установленном программном обеспечении и проверяет отсутствие противоречий с действующими лицензионными соглашениями.

Как правило, в готовых программных решениях редко присутствует весь функционал, необходимый сетевому администратору. Основными задачи сводятся следующему перечню: мониторинг сети, мониторинг аппаратной конфигурации рабочих станций, мониторинг и изменения (загрузка и обновление) программного обеспечения, создание отчетов, создание схем расположения техники. Для администратора, имеющего четкое представление о стоящих перед ним задачах (определяемых политикой информационной безопасности) возможен вариант не комплексного решения, а набора программ, выполняющих одну или несколько из перечисленных функций. Такие предложения размещены на многочисленных сайтах в сети Интернет (например: http://www.securitylab.ru/software/1308/, http://popprograms.com/uchet-kompiuterov/). Однако следует учитывать, что некоторые из предлагаемых решений могут быть нестабильны в работе и требуют предварительной проверки и наладки на резервном сервере.

УДК 681.3

Е.Ю. Смаков, В.И. Новосельцев

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ СИНТАКСИЧЕСКОГО АНАЛИЗА ТЕКСТОВ ПРИ СОЗДАНИИ ИНТЕЛЛЕКТУАЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

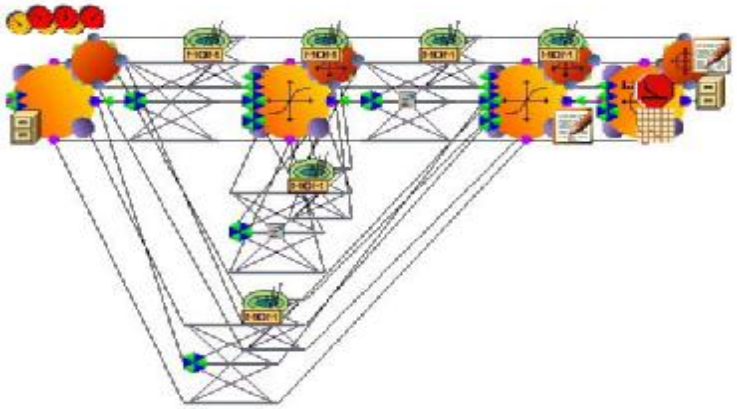
В наши дни задачи автоматизированного анализа текстов являются весьма актуальными в связи с широким обменом текстовой информации, в частности, через интернет и мобильные каналы связи. Одной из таких задач является разработка обезличивателя судебных решений, способного удалять персональные данные из юридических документов такого рода, чья необходимость решения обусловлена выходом закона от 22 декабря 2008 г. № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации». Ее развитие может иметь применение не только для анализа судебных текстов, но и в перспективе для последующей обработки разнотипных текстов на естественном языке.

Задачи обработки текста на естественном языке. В рамках автоматизированной обработки естественного языка можно выделить определенное подмножество этих задач: определение частей речи (морфологический разбор), распознавание поименованных сущностей, определение членов предложения, семантический анализ.

Как демонстрирует литература, на основе нейронных сетей возможно выработать унифицированный подход к решению указанных выше задач. На начальном этапе нужно выбрать модельную задачу, которая позволяла бы отработать этот подход, выбрать топологию сети и методику ее обучения. В качестве такой задачи был выбран синтаксический разбор предложений ввиду двух обстоятельств. С одной стороны, в литературе и интернет-источниках можно найти примеры синтаксических разборов, необходимых для обучения и настройки сети. С другой стороны, сама задача представляет определенную ценность, поскольку до сих пор не удается получить удачную программу этого типа для практических нужд.

Использование нейронных сетей для обработки текстов. В данной работе рассматривается методика построения парсера или разборщика текстов, основанная на сочетании сетей Simple Recurrent Network (SRN) и Recurrent Network Auto-Associative Memory (RAAM). Сеть RAAM (рис. 1) является автоассоциативной сетью с обратным распространением ошибок. Во входном и выходном слоях RAAM элементы организованы в поля, где каждое поле содержит одинаковое число

элементов. Число полей определяется валентностью кодируемых и декодируемых деревьев, а число элементов в скрытом слое соответствует числу элементов одного слоя.



ю
с об и-
ем в
скр ь-
екти ь-
ную и затем считается ошибка cost = (decoded-input).

Простая рекуррентная сеть имеет обратные связи у скрытых элементов, направленные обратно во входной слой.

Скрытые элементы составляют внутренне редуцированное представление данных, предшествующих текущему вводу. Это редуцированное представление образует контекст, оказывающийся для определенных задач существенным.

В данной модели сеть SRN (рис. 1) обучает сопоставлению входных слов, поочередно подающихся на вход, сжатому представлению синтаксического разбора, зашифрованного при помощи сети RAAM. Таким образом, после подачи всего рассматриваемого предложения веса сети SRN подстраиваются выдаче соответствующего сжатого представления синтаксического разбора.

Среда формирования нейросетей NeuroSolution. Для реализации данной программы использовался пакет Neurosolution. Универсальный нейропакет NeuroSolutions фирмы NeuroDimension, Inc. предназначен для моделирования широкого круга искусственных нейронных сетей. Основное достоинство описываемого нейропакета состоит в его гибкости: помимо традиционно используемых нейросетевых парадигм нейропакет позволяет создавать практически любые собственные нейронные структуры и алгоритмы их обучения. Функция активации нейрона может быть выбрана из пяти стандартных функций, а также задана в произвольном виде пользователем. Нейропакет поддерживает все известные типы связей: прямые, перекрестные и обратные.

Создание нейросетевой модели. Сеть SRN создавалась при помощи встроенного настройщика (wizard) среды NeuroSolution (рис. 1, 2).

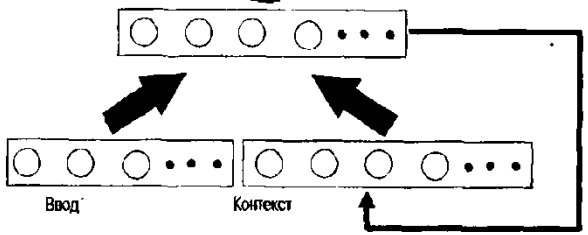


Рис. 2. Топология сети SRN, построенная с помощью NeuroSolution

Однако функционала данного настройщика не хватило для формирования сети RAAM в виду сложности ее структуры, поэтому потребовалось модифицировать исходный код проекта, адаптировав стандартизированные объекты среды под необходимую структуру RAAM.

Слова в предложении необходимо подавать по парам только лишь во время первого прохода, затем необходимо подать следующее слово, а его парой станет закодированная структура из скрытого слоя (рис. 3).

Рис. 3. Последовательная обработка слов сетью RAAM
в разработанной модели

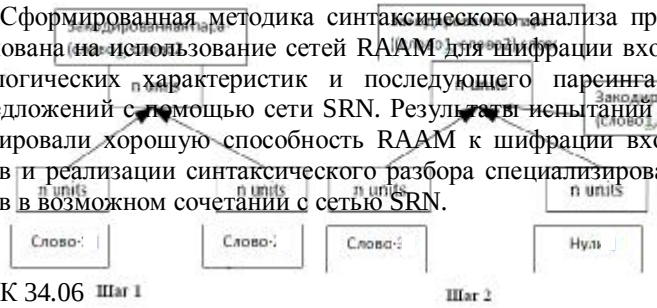
При этом выходным (desired) файлом является такой же файл, как и входной (input) с одной лишь разницей: в нем введено фиктивные *n* столбцов, в которых на первом шаге стоят зарезервированные числа, а затем подаются свернутые значения для определения ошибки.

В результате работы данной модели (рис. 4) для каждого предложения переменной длины ставится в соответствие числовое представление размерности 10. Сохранив настроившиеся в результате обучения веса, в дальнейшем можно будет расшифровывать полученные значения работы нейронной сети.

*Рис. 4.*Топология сети RAAM, реализованная средствами NeuroSolution

В данной модели для сети RAAM могут применяться разные функции активации. Выбор подходящей функции позволяет оптимизировать длительность обучения сети шифрации входных фраз. Испытания продемонстрировали, что линейная функция является предпочтительной в условиях данной задачи.

Сформированная методика синтаксинеского анализа предложений основана на использование сетей RAAM для шифрации входных морфологических характеристик и последующего парсинга (разбора) предложений с помощью сети SRN. Результаты испытаний продемонстрировали хорошую способность RAAM к шифрации входных текстов и реализации синтаксического разбора специализированных текстов в возможном сочетании с сетью SRN.



УДК 34.06

В.В. Сурин

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНОВ УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ

Федеральная служба исполнения наказаний является федеральным органом исполнительной власти, осуществляющим правоприменительные функции, функции по контролю и надзору в сфере исполнения уголовных наказаний в отношении осужденных, функции по содержанию лиц, подозреваемых либо обвиняемых в совершении преступлений, и подсудимых, находящихся под стражей, их охране и конвоированию, а также функции по контролю за поведением условно осужденных и осужденных, которым судом предоставлена отсрочка отбывания наказания.

В соответствии с указом Президента РФ от 13 октября 2004 г. № 1314 ФСИН России обеспечивает: правопорядок и законность в учреждениях, исполняющих наказания; безопасность объектов уголовно-исполнительной системы; защиту сведений, составляющих государственную и иную охраняемую законом тайну, в уголовно-исполнительной системе.

В месте с этим, как показывает статистика последних лет, с одной стороны, остается непростой криминогенная обстановка внутри исправительных учреждений, в том числе фиксируются попытки незаконного доступа к служебным сведениям. С другой стороны, широкое распространение современных информационных технологий создает благоприятную обстановку для незаконного ознакомления со сведениями конфиденциального характера, отражающими работу учреждений уголовно-исполнительной системы.

В сложившихся условиях особую актуальность имеет деятельность, направленная на обеспечение информационной безопасности органов уголовно-исполнительной системы.

Обозначенная деятельность достаточно давно реализуется на практике, ей уделяется внимание в современных нормативных актах, прежде всего управленческого характера, однако в настоящее время остро ощу-

щается дефицит ее научного осмысления. Это проявляется в бессистемном использовании обсуждаемого термина в текстах документов и противоречивости выделяемого в нем содержания, что, в свою очередь, не способствует единообразному принципу применения закона.

В содержании понятия «информационная безопасность органов уголовно-исполнительной системы» можно выделить три составных элемента: во-первых, это собственно понятие «безопасность», во-вторых, это информационная составляющая безопасности, в-третьих, это интерпретация вышеуказанных двух элементов относительно процесса исполнения наказаний. В подобных случаях, как правило, изначально следует определиться со смысловым содержанием составных частей, а затем сформулировать значение специального термина. Это достаточно распространенный подход, он часто используется на практике.

Безусловно, ключевым элементом исследуемого понятия является термин «безопасность». Существует немало исследований его содержания, при этом анализ проводится с правовой, социологической, нравственной и других позиций. В соответствии с существующей традицией остановимся прежде всего на философско-этическом подходе. В этом случае интересным является мнение С.К. Рощина. Он рассматривал безопасность как состояние общественного сознания, при котором общество в целом и каждая отдельная личность воспринимают существующее качество жизни как адекватное и надежное, поскольку оно создает реальные возможности для удовлетворения естественных и социальных потребностей граждан в настоящем и дает им основания для уверенности в будущем.

Правовая позиция во многом восприняла данный подход. Однако акцент сместился из личной сферы в общественную, и это понятно, учитывая, что право выражает, прежде всего, интересы общества в целом. Учитывая многогранность самого понятия «безопасность» и сфер его применения, в документах можно найти множество вариантов определения рассматриваемого термина. Несмотря на многообразие мнений, большинство из них все же используют подход, предложенный законодателем в ранее действовавшем федеральном законе «О безопасности». Согласно обозначенной позиции «безопасность» – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Многие исследователи также берут за основу это определение, например С.В. Степашин, который определяет безопасность как защищенность качественного состояния общественных отношений, обеспечивающих прогрессивное развитие человека и общества в конкретных исторических и природных условиях, от опасностей, источником возникновения которых являются внутренние и внешние противоречия.

Гораздо больший разброс во мнениях мы находим при исследовании более узкого понятия «информационная безопасность». Обратимся, прежде всего, к содержанию международных документов. Например, Концепция информационной безопасности государств – участников Содружества Независимых Государств определяет данный термин как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Несколько схожее определение мы можем встретить в решении Совета глав государств СНГ «О Концепции сотрудничества государств – участников Содружества Независимых Государств в сфере обеспечения информационной безопасности…», принятое в Бишкеке 10 октября 2008 г. Оно определяет информационную безопасность как состояние защищенности от внешних и внутренних угроз информационной сферы, формируемой, развиваемой и используемой с учетом жизненно важных интересов личности, общества и государства.

Одним из ключевых национальных правовых актов, создающим основы обеспечения безопасности в информационной сфере, является Доктрина информационной безопасности Российской Федерации. Этот документ определяет информационную безопасность Российской Федерации как состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Т.А. Полякова рассматривает информационную безопасность как состояние защищенности национальных интересов РФ в информационной сфере, состоящих из совокупности сбалансированных интересов личности, общества и государства, от внутренних и внешних угроз. В.Д. Курушин, В.А. Минаев под информационной безопасностью понимают состояние защищенности информационной среды общества, обеспечивающее ее формирование и развитие в интересах граждан, организаций и государства.

В результате анализа вышеприведенных определений понятия «информационная безопасность» мы должны сделать вывод, что, как правило, его основой служит определение самого понятия «безопасность», а далее конкретизируется сфера его применения, в нашем случае – информационная. Используя этот подход, попытаемся сформулировать определение еще более узкого понятия «информационная безопасность уголовно-исполнительной системы».

Хотя данный вопрос является достаточно специфическим, тем не менее уже существуют исследования в этой сфере. Например, А.И. Одинцов считает, что под информационной безопасностью во ФСИН России следует понимать состояние защищенности информационной сферы уголовно-исполнительной системы, достигаемое в результате прогнозирования,

выявления и нейтрализации факторов, создающих опасность реализации функции информационного обеспечения управления во ФСИН России. Это определение, использующее вышеупомянутый методологический подход, безусловно, является достаточно корректным. Вместе с тем, с нашей точки зрения, автор не совсем обоснованно сузил содержание понятия, ограничив его лишь обеспечением стабильности функционирования информационного обеспечения управления во ФСИН России. Ведь деятельность УИС не сводится лишь только к управленческой, она гораздо более обширна и разнообразна. Следовательно, содержание термина «информационная безопасность уголовно-исполнительной системы» должно обязательно учитывать этот факт. Таким образом, предложенное определение, на наш взгляд, должно быть расширено.

Для выполнения поставленной задачи предлагаем прежде всего определиться с правовым пространством, в котором нам предстоит действовать. УИС существует для исполнения уголовных наказаний. Согласно содержанию ч. 2 ст. 43 УК РФ и ч. 1 ст. 1 УИК РФ целью применения наказаний, а соответственно и существования пенитенциарной системы является восстановление социальной справедливости, а также исправление осужденных и предупреждение совершения новых преступлений. Определяемое понятие должно, безусловно, принимать во внимание указанное обстоятельство, именно цель исполнения наказаний должна определять особенности информационной безопасности УИС.

Учитывая все вышеизложенное, постараемся сформулировать свою интерпретацию обсуждаемого термина: «Информационная безопасность органов уголовно-исполнительной системы – состояние защищенности уголовно-исполнительной системы в информационной сфере, состоящей из совокупности сбалансированных интересов органов УИС, ее сотрудников, осужденных и иных лиц от внутренних и внешних угроз, обеспечивающее восстановление социальной справедливости, а также исправление осужденных и предупреждение совершения новых преступлений».

УДК 343.8:004

А.В. Хорошева

ПРОБЛЕМЫ ЗАЩИЩЕННОСТИ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В ОРГАНАХ И УЧРЕЖДЕНИЯХ УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ

Управление информационными ресурсами имеет для деятельности структурных подразделений ФСИН России, учреждений, непосредственно подчиненных ФСИН России, территориальных органов и образовательных учреждений особое значение. На протяжении ряда лет достаточно четко прослеживается тенденция увеличения объемов информационных потоков, проходящих через учреждения и органы УИС. Характерно, что происходит рост не только документооборота на традиционных носителях, но и информации, проходящей по электронным каналам, а также документов, связанных с функционированием компьютерных систем. Поэтому остро ощущается необходимость организации эффективного управления документооборотом, информационными ресурсами с использованием компьютерных технологий.

Концепцией развития уголовно-исполнительной системы Российской Федерации до 2020 г. определены следующие приоритетные направления: внедрение электронного делопроизводства, формирование и ведение регистра унифицированной системы электронных документов, перевод в цифровой формат 100 % документов информационных фондов и архивов учреждений и органов УИС к 2020 г. Важнейшим шагом, позволяющим ФСИН России перейти на безбумажный документооборот, является внедрение системы электронного документооборота.

Система электронного документооборота (СЭД) – это система автоматизации работы с документами на протяжении всего их жизненного цикла (создание, изменение, хранение, поиск, классификация и пр.), а также процессов взаимодействия между сотрудниками. При этом под документами в первую очередь подразумеваются неструктурированные документы (файлы Word, Excel и пр.). Как правило, СЭД включает в себя электронный архив документов и систему автоматизации деловых процессов.

Внедрение системы электронного документооборота позволяет оптимизировать управленческую деятельность, сократив время на пересылку, рассмотрение документов и обеспечив прозрачность их согласования. С развитием системы межведомственного электронного документооборота появляется возможность осуществлять отправку документов в электронном виде с использованием электронной подписи из ФСИН России в федеральные органы исполнительной власти и принимать от них аналогичную информацию. СЭД существенно повышает эффективность работы с документацией, а также позволяет оптимизировать и ускорять процессы ее обработки и хранения. В то же время внедрение таких систем способствует образованию дополнительных угроз информационной безопасности, пренебрежение которыми может привести к компрометации конфиденциальных данных, хранящихся в СЭД.

В настоящее время в учреждениях и органах УИС уже используется несколько различных СЭД. Они обрабатывают информацию, содер-

жащую сведения, составляющие государственную тайну, поэтому актуальным является вопрос обеспечения информационной безопасности в таких системах.

Принято разделять требования к защищенным СЭД на две группы:

обеспечение юридической значимости электронного документа;

обеспечение защиты электронного документа от стандартных угроз.

Для того чтобы электронные документы имели юридическую силу, требуется сохранение их аутентичности и целостности. Аутентичность электронного документа может быть доказана путем применения к нему электронной подписи. Надежность современных криптографических систем защиты (в том числе электронной подписи) достаточна и превосходит надежность экспертных оценок аутентичности (почерка или печати).

В основе обеспечения безопасности информации лежит обеспечение целостности, конфиденциальности и доступности информации, а набор угроз для СЭД является стандартным, как и для любой другой защищенной информационной системы:

угроза целостности – это повреждение, уничтожение или искажение информации, которое может быть как ненамеренное, в случае ошибок и сбоев, так и злоумышленное;

угроза конфиденциальности – это любое нарушение конфиденциальности, в том числе кража, перехват информации, изменение маршрутов следования;

угроза работоспособности системы – это угроза, приводящая к нарушению или прекращению работы системы, включая умышленные атаки, ошибки пользователей, а также сбои в оборудовании и программном обеспечении;

угроза доступности – это угроза, нарушающая возможность за приемлемое время получить требуемую информацию пользователями, имеющими к ней право доступа.

Защиту именно от этих угроз в той или иной мере должна реализовывать любая система электронного документооборота.

При построении защищенной СЭД необходимо учитывать ряд факторов, связанных со спецификой функционирования информационных систем в УИС:

территориальная разобщенность информационных ресурсов и самих участников информационного взаимодействия;

обработка информации различных уровней конфиденциальности, в том числе относящейся к государственной тайне;

разнородность информационных ресурсов;

необходимость в гарантированном доведении и обработке информации при ненадежных каналах связи;

необходимость обеспечения гарантированной автономной работы отдельных узлов системы;

необходимость в постоянном мониторинге функционирования системы;

постоянное масштабирование системы и т. д.

В настоящее время существуют механизмы, позволяющие строить информационные системы (в том числе СЭД), учитывая все эти факторы в комплексе.

Традиционный подход в решении проблемы обработки информации, различной по уровню конфиденциальности, сводится к созданию нескольких контуров обработки информации, каждый из которых обрабатывает только информацию конкретного грифа секретности.

Одним из перспективных подходов в решении проблемы обработки информации, различной по уровню конфиденциальности, является следующий: информация различных грифов секретности должна обрабатываться в едином защищенном контуре с использованием в качестве основы технологии промежуточного программного обеспечения (ППО). Оно является интерфейсным слоем между прикладными программами и операционной системой и призвано решать проблемы взаимодействия между распределенными прикладными и системными программными компонентами. За счет применения данной технологии как платформы для построения защищенной СЭД обеспечивается связь субъектов и прикладных процессов, гарантированное доведение информации участникам информационного обмена, возможно использование внутриплатформенных средств хранения информации.

ППО со встроенными средствами обеспечения защиты информации имеет множество преимуществ перед другими вариантами решения вышеописанных задач обеспечения безопасности информации, так как в рамках единого защищенного информационного пространства распределенной гетерогенной информационной системы может использоваться единая политика безопасности.

Кроме того, информационная система (в частности, СЭД), обрабатывающая сведения, составляющие государственную тайну, должна иметь сертификат соответствия определенному классу защищенности по требованиям соответствующего руководящего документа ФСТЭК РФ, при этом все средства защиты информации, используемые в данной системе, также должны быть сертифицированы. Решения, построенные на базе технологии промежуточного программного обеспечения, позволяют объединить набор средств вычислительной техники в единую среду за-

щиты информации, что исключит необходимость осуществлять сертификацию всех средств защиты информации в отдельности.

Технология электронной подписи должна быть реализована на основе средств криптографической защиты, интегрируемых в среду ППО, или механизмами, реализованными непосредственно в среде ППО.

Таким образом, все вышеперечисленные факторы, влияющие на построение защищенной СЭД, будут учтены на уровне ППО. В настоящее время существует возможность построения безопасной полнофункциональной СЭД, соответствующей современным требованиям информационной безопасности, на основе технологии промежуточного программного обеспечения за счет создания единого безопасного информационного пространства в рамках информационной инфраструктуры организации. Построение такой СЭД будет способствовать дальнейшему развитию электронного документооборота в органах и учреждениях УИС.

УДК 681.3

В.В. Цветков, А.В. Душкин

СТРУКТУРИРОВАНИЕ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ БЕЗОПАСНОСТИ

Использование систем поддержки принятия решения (СППР) при разработке современных систем охраны и защиты информации, применяемых на объектах ФСИН России, предполагает создание рационально организованных банков данных для хранения информации о вариантах развития ситуаций Ω и их характеристиках. Известно, что любое представление данных в памяти ЭВМ должно включать в себя данные, а также явно и неявно задаваемые взаимосвязи между ними, которые определяют структурирование данных. Такие структуры могут представлять собой упорядоченные классы альтернатив, сгруппированные по определенным признакам. Каждый из классов наделяется определенным приоритетом обращения к нему и включает в себя наборы несравнимых и эквивалентных по принятому критерию вариантов.

Для эффективного использования информационных массивов они должны быть организованы так, чтобы их структурирование отвечало целям, для которых они создавались. Такие информационные массивы должны характеризоваться следующими соотношениями скоростей изменения массивов исходных данных для решения задачи выбора либо требованиями технического задания:

$$|\Omega_t \setminus \Omega| / |\Omega| << /(C_{Дt} \setminus C_Д)| / |C_Д|, \quad (1)$$

$$|C_{kt} \setminus C_k| / |C_k| << /(C_{Дt} \setminus C_Д)| / |C_Д|), \quad (2)$$

где Ω – множество возможных альтернатив (МВА) Ω в другой, новый момент времени *t;*

$C_{Дt}$ – требования по допустимости в момент времени *t;*

C_{kt} – критериальные требования в момент времени *t.*

Вышеприведенные свойства дают основания для однократного (при создании СППР) структурирования Ω в соответствии с возможными постановками задач многокритериального выбора для любых требований по допустимости.

Рассматриваемый подход основан на наделении исходного множества альтернатив (ИМА) структурой, связанной с его функциональным назначением и отражающей устойчивые критериальные требования, присущие ИМА Ω. Принятые цели определяют задаваемый вид структурирования.

Паретовское расслоение МВА Ω. Послойное представление частично упорядоченного множества в виде последовательно задаваемых π_{sp}-слоев означает, что процедура выбора на структурированном множестве должна начинаться сразу с потенциально эффективных концевых решений посредством проверки допустимости альтернатив по $C_Д$. Если допустимых вариантов в $\Omega_{\pi 1}$-решениях нет, то выбор проводится на следующем слое $\Omega_{\pi 2}$ частично упорядоченного множества Ω, если их нет и там, то переходят к 3-му слою и т. д.

Таким образом, все ИМА Ω априорно разбивается на линейно упорядоченные $\Omega_{\pi s}$-слои, которые представляют собой настроенную на целевые устремления ЛПР, эффективную структуру представления данных для решения задач многокритериального выбора.

Таким образом, если в СППР на основании свойств (1) и (2) альтернативы структурируются в соответствии с паретовскими расслоениями, это означает, что решение задачи выбора можно свести к проверке ограничений на допустимость концевых (π-оптимальных) альтернатив, т. е. на первом шаге осуществляется поиск допустимых вариантов по $C_Д$ в $\Omega_{\pi 1}$-слое, если $\Omega_{p1} = \varnothing$, то переходят ко 2-му $\Omega_{\pi 2}$ -слою и т. д.

Слейтеровское структурирование альтернатив. Послойное представление частично упорядоченного множества в виде последовательно задаваемых S_p-слоев означает, что процедура выбора на s-структурированном множестве должна начинаться так же, как и в случае π-структурирования, сразу с потенциально эффективных (оптимальных по S-критерию) концевых решений посредством проверки допустимости альтернатив по $C_Д$. Если допустимых вариантов в Ω_{s1}-решениях нет, то выбор проводится на следующем Ω_{s2} слое *s*-упорядоченного множества МВА Ω если их нет и там, то переходят к 3-му слою и т. д.

Таким образом, все исходное множество альтернатив Ω априорно разбивается на линейно упорядоченные Ω_{sp}-слои, которые представляют структуру представления данных для решения задач в соответствии с S-критерием.

Линейные порядки классов альтернатив при априорном структурировании по Слейтеру (а) и Парето (б) представлены на рисунке.

Выбор типа структурирования (по Слейтеру или Парето) предполагает проведение предварительного анализа устойчивости решений.

В случае существенно неустойчивых решений целесообразно проводить S-структурирование, приводящее к меньшему числу слоев, но позволяющему не отбросить возможные оптимальные решения при более глубоком анализе.

Если же оценка устойчивости критериальной постановки дает положительные результаты, целесообразно провести более жесткое паретовское структурирование, так как оно позволяет сократить число проверок на допустимость и процедура выбора оптимальных вариантов займет меньше времени.

Априорное критериальное структурирование альтернатив для решения задачи выбора при условиях (1) и (2) принципиально возможно и для метрических критериев.

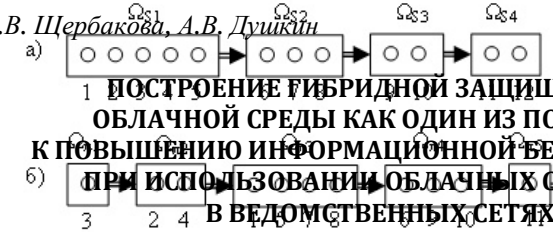
Анализ приведенных способов априорного структурирования альтернатив в соответствии с π- и S-расслоениями позволяет сделать вывод о целесообразности таких настроек структур в СППР только для случаев относительно жесткой привязки показателей качества к выбираемым объектам. Если же динамика смены показателей на МВА Ω от одной задачи к другой имеет высокую вероятность, то и структурирование альтернатив должно быть адаптировано к новой системе показателей. Такое переструктурирование МВА Ω от принятой устойчивой критериальной постановки имеет смысл только в том случае, если его трудоемкость существенно ниже, чем собственно процедура выбора из априори неструктурированного множества.

Вышесказанные принципы структурирования можно использовать в информационных системах поддержки принятия решения при проектировании комплексных систем безопасности объектов ФСИН России

для оптимального выбора и размещения периметровых датчиков обнаружения, видеокамер охранного видеонаблюдения, средств защиты информации и иных компонентов систем охраны.

УДК 681.3

Ю.В. Щербакова, А.В. Душкин



ПОСТРОЕНИЕ ГИБРИДНОЙ ЗАЩИЩЕННОЙ ОБЛАЧНОЙ СРЕДЫ КАК ОДИН ИЗ ПОДХОДОВ К ПОВЫШЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ СЕРВИСОВ В ВЕДОМСТВЕННЫХ СЕТЯХ

Вопрос защиты информации в федеральных службах и ведомствах Российской Федерации необходимо рассматривать в контексте развития современных ИТ-технологий, которые позволяют, с одной стороны, сократить издержки и использовать современные подходы к организации ИТ-инфраструктуры, с другой, вносят новые задачи по обеспечению конфиденциальности, доступности и модификации обрабатываемых данных. В связи с этим подход к построению ИТ-инфраструктуры на основе облачных вычислений с целью повышения уровня безопасности является актуальной задачей, требующей применения стоимостных методик расчета в совокупности с методами оценки риска нарушения информационной безопасности (ИБ).

Федеральные ведомства и службы, которые традиционно считаются одними из самых требовательных заказчиков, при выборе и внедрении новых технологий прежде всего обращают внимание на степень проработанности аспектов информационной безопасности.

Несмотря на высокую динамику распространения и использования технологии облачных вычислений в различных средах деятельности, ряд вопросов в области ИБ остается открытым, что подтверждает необходимость исследования и разработки методики построения гибридной защищенной облачной среды (ГЗОС), позволяющей использовать преимущества облачной среды с возможностью обработки критически важных данных в пределах демилитаризованной зоны, роль которой может выполнять частная облачная среда (ЧОС).

Существует точка зрения, что технология облачных вычислений является эволюционным этапом развития ИТ-индустрии, постепенно сменяющим традиционные модели построения ИТ-инфраструктуры. Основным сдерживающим фактором повсеместного распространения облачных сервисов является опасение потерять контроль над критически важными данными.

При построении облачной ИТ-инфраструктуры в первую очередь необходимо учитывать главный фактор риска, который заключается в потере контроля со стороны управлений уголовно-исполнительной системы над обрабатываемыми данными.

Если федеральные ведомства и службы решаются на использование облачных сервисов, то единственным приемлемым вариантом является построение частного облака для своей территориальной организационной структуры.

К стимулирующим факторам использования облачных сервисов относятся:

1) сокращение издержек на поддержку инфраструктуры;

2) повышение гибкости инфраструктуры;

3) перераспределение людских и финансовых ресурсов.

Как видно, использование облака может предоставить организации большой набор преимуществ, но изменения всегда сопровождаются новыми и часто неожиданными рисками в области информационной безопасности. Самой серьезной проблемой является невозможность со стороны клиента определить, где располагаются его данные. Риск потерять контроль заставляет организации искать альтернативные варианты использования публичных облачных сервисов с предоставлением возможности управления данными в рамках своей инфраструктуры его качеством. Это позволяет клиенту самостоятельно проводить техническое обслуживание, планировать необходимые исправления, включать дополнительные механизмы защиты данных.

Применение ГЗОС востребовано при решении нижеперечисленных практических задач:

1. ГЗОС в качестве партнера. При этом критически важные приложения и данные обрабатываются в частной облачной среде, а остальные располагаются в более доступной облачной среде.

2. ГЗОС в качестве полигона, когда речь идет о необходимости использования временного рабочего пространства.

3. ГЗОС в качестве дополнительной емкости, когда ОС используется при возникновении внезапных пиковых нагрузок.

Таким образом, гибридное облако – это сочетание компонентов ЧОС и одной облачной инфраструктуры общедоступного пользования, которая обеспечивает прозрачный доступ к ЧОС и может динамически масштабироваться для управления неравномерной нагрузкой. Особо отметим, что при такой организации происходит усиление внутреннего контроля над критически важными приложениями (процессами), которые организация не хочет выводить за пределы демилитаризованной зоны, но в то же время остается возможность при необходимости использовать ключевые преимущества облачных вычислений.

Политика ИБ при использовании ГЗОС должна включать в себя решение нижеперечисленных ключевых задач:

1. Определение ролей доступа к информационным активам организации.

Установление контроля над запросами, которые оперируют с данными, построение маршрутов распределения обработки данных для выбора наиболее оптимального варианта развертывания облачной среды.

2. Описание контролируемых показателей для принятия решений.

Организация должна провести анализ и оценку производительности критически важных служебных приложений, сформировать показатели эффективности использования дополнительных мощностей, определить исключения и ограничения при выделении ресурсов в ОС.

3. Соглашения об уровне обслуживания.

Ключевым этапом является необходимость установления уровней надежности как для приложений, так и для всей облачной инфраструктуры, ряд договоренностей с провайдером.

4. Гарантированное качество обслуживания.

Определение критериев качества предоставляемых услуг, конечно, должно регулироваться лучшими практиками и рекомендациями со стороны ведущих институтов в области стандартизации.

Таким образом, для эффективного управления гибридным облаком необходимо создать всеобъемлющую инфраструктуру в соответствии с выработанной в учреждении на начальных этапах концепцией.

При практической реализации ГЗОС необходимо принять во внимание следующие задачи:

1) адаптация функциональных возможностей локальных приложений для использования в облачной среде, определение способа развертывания данных;

2) настройка механизма аутентификации пользователей и авторизация рабочих процессов;

3) проработка механизма передачи данных из ОС в ЧОС;

4) настройка логики и маршрутизации потоков данных;

5) проведение синхронизации данных;

6) поддержка требуемого уровня масштабируемости, производительности и доступности с возможностью выделения дополнительных экземпляров облачных компонентов приложения с целью выполнения различной нагрузки и обеспечения защиты от кратковременных проблем с сетью.

Как показало исследование, гибридный тип развертывания облачной среды является одним из наиболее экономичных и эффективных подходов для достижения организацией целей минимизации издержек на ИТ-инфраструктуру с возможностью самостоятельного управления обработкой критически важных данных.

РАЗДЕЛ 6

ПОДГОТОВКА СПЕЦИАЛИСТОВ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 378.14

А.С. Баранова

ФОРМИРОВАНИЕ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

В информационном обществе в условиях отсутствия идеальной информационной среды важно обучить личность адекватному восприятию и оценке информации, ее критическому осмыслению на основе нравственных и культурных ценностей. Важно также обучать средствам защиты личной информации и прививать навыки обращения с информацией в рамках закона. На современном этапе развития общества актуально формирование культуры информационной безопасности личности.

Формирование культуры информационной безопасности личности предполагает осмысление понятий «информационная безопасность», «информационная преступность», «компьютерная преступность», «киберпреступность», «преступность в сфере массовых коммуникаций», выбор наиболее полных определений из имеющихся. В процессе формирования культуры информационной безопасности можно предложить назвать виды преступлений, способы наказаний и привести конкретные примеры. Важна также проработка Уголовного кодекса, поиск и осмысление статей, касающихся ответственности за информационную, компьютерную преступность.

В современной научной литературе определена сущность понятия «культура информационной безопасности», что означает такой способ организации и развития жизнедеятельности, при котором гражданин знает и способен реализовать свои конституционные права и свободы в информационной сфере (владеет технологиями доступа к государственным информационным ресурсам, может сохранить свою личную тайну, интеллектуальную собственность), умеет распознать негативные информационные воздействия, угрожающие его здоровью, и владеет технологиями защиты от них. Культура информационной безопасности – процесс освоения знаний, умений и навыков в области информационной безопасности и процесс их применения с целью достижения более высокого уровня информационной безопасности. Сущность понятия «культура информационной безопасности» можно схематично изобразить в виде пирамиды, в основании которой находится информационная культура и как и надстройка к ней культура информационно-психологической безопасности личности, технологическая культура информационной безопасности и правовая культура.

Формирование культуры информационной безопасности личности является актуальным и востребованным в информационном обществе и правовом государстве. Значимость данного направления для формирования информационно-правовой компетентности и культуры отражается целым рядом важнейших характеристик: дает возможность получить необходимые знания и умения критически относиться к информации с позиции правовых предписаний и запретов; ориентировать на формирование правовых знаний; способствует воспитанию активных и ответственных граждан своей страны; предупреждает преступность в информационной сфере. В процессе изучения аспектов правовой культуры происходит привитие культуры использования легального информационного продукта, формируется критическое отношение к незаконному обороту контрафактной продукции в реальной и виртуальной средах (например, в информационно-телекоммуникационной сети Интернет). Одним из основных средств реализации данного направления являются социальные проекты, осуществляемые педагогами, обладающими информационно-техническими, правовыми и педагогическими знаниями. Такие проекты предполагают консолидацию усилий администраций образовательных учреждений, структур дополнительного образования, социальных институтов (например, центров бесплатного доступа к правовой информации, некоммерческих организаций, занимающихся правовыми проблемами), международных организаций и других заинтересованных субъектов. Значительную роль в развитии информационно-правовой культуры сегодня играет программа ЮНЕСКО «Информация для всех», в частности ее Российский комитет, постоянно оказывающий содействие как в распространении социально значимой информации, так и в проведении различных мероприятий по обеспечению открытости к общедоступной информации, открытии центров правовой помощи.

До недавнего времени уголовное законодательство большинства стран призвано было обеспечить защиту законных прав и интересов личности, общества и государства в материальном мире. В ходе поступательного развития информационных технологий и средств телекоммуникации они стали незаменимой составляющей жизни человека, деятельности общества и механизмов государства. Это поставило на повестку дня во всех странах мира необходимость нормативно-правовой

поддержки новых отношений, возникающих при использовании информационных и телекоммуникационных технологий, формирование правовой среды с четко очерченным кругом категорий и понятий – важнейших элементов эффективного развития новых явлений.

Формированию культуры информационной безопасности личности способствуют правовые знания, информационно-правовые умения, навыки и компетенции, а также правовое сознание и культура.

В настоящее время необходима борьба с информационной преступностью. Культура информационной безопасности предполагает овладение термином «информационная преступность», умение различать ее виды, знание уголовного законодательства об ответственности за компьютерные преступления.

Информационная преступность – противоправные действия в информационной сфере, нарушающие установленные законом права личности, организации или государства и наносящие им моральный вред или материальный ущерб. К информационной преступности относят компьютерную преступность, или киберпреступность, преступность в сфере массовых (печатных, электронных, иных) коммуникаций, массовой информации. В странах, где компьютеризация общественной жизни находится на высоком уровне, существует самостоятельный вид преступлений, обобщенно называемый компьютерными или высокотехнологичными преступлениями («computer crimes» или «high-tech crimes»). Сфера компьютерной информации, будучи составной частью информационной сферы, является многоуровневой и в самом общем виде включает отношения, возникающие по поводу производства, сбора, обработки, накопления, хранения, поиска, передачи, распространения и потребления компьютерной информации, создания и использования информационных компьютерных технологий и средств их обеспечения, защиты компьютерной информации и прав субъектов, участвующих в информационных процессах и информатизации с использованием компьютеров, их систем и сетей. Ее фундаментом является совокупность информационных ресурсов в виде компьютерной информации, компьютерных технологий и оборудования, а также связанной с ними компьютерной инфраструктуры, включая сети электросвязи.

С учетом этого выделяют виды преступлений, совершаемых с применением компьютерных технологий и использованием компьютерной информации:

преступления в сфере компьютерной информации, посягающие на информационные компьютерные отношения, т. е. отношения, возникающие по поводу осуществления информационных процессов производства, сбора, обработки, накопления, хранения, поиска, передачи, распространения и потребления компьютерной информации, создания

и использования компьютерных технологий и средств их обеспечения, а также защиты компьютерной информации, прав субъектов, участвующих в информационных процессах и информатизации;

преступления в информационном компьютерном пространстве, посягающие на отношения, возникающие по поводу реализации прав на информационные ресурсы (собственности и т. д.), информационную инфраструктуру и составляющие ее части (ЭВМ, системы и сети ЭВМ, программы для ЭВМ и т. д.);

иные преступления, для которых характерно использование компьютерной информации или составляющих ее элементов информационного пространства при совершении деяний, посягающих на иные охраняемые уголовным законом правоотношения (собственности, общественной безопасности и т. д.).

В Уголовном кодексе Республики Беларусь имеется семь статей, устанавливающих ответственность: за несанкционированный доступ к компьютерной информации (ст. 349), модификацию компьютерной информации (ст. 350), компьютерный саботаж (ст. 351), неправомерное завладение компьютерной информацией (ст. 352), изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети (ст. 353), разработку, использование либо распространение вредоносных программ (ст. 354), нарушение правил эксплуатации компьютерной системы или сети (ст. 355).

Отдельные статьи предусматривают максимальный срок наказания до двух лет лишения свободы, другие – до семи лет. Так, за несанкционированный доступ к компьютерной информации либо самовольное пользование электронной вычислительной техникой, средствами связи компьютеризованной системы, компьютерной сети, повлекшие по неосторожности крушение, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия, наказывается лишением свободы на срок до семи лет. В двух случаях предусмотрено наказание в виде лишения свободы на срок до 10 лет – за компьютерный саботаж, сопряженный с несанкционированным доступом к компьютерной системе или сети или повлекший тяжкие последствия, а также за разработку, использование либо распространение вредоносных программ, если это повлекло тяжкие последствия.

Развитие культуры информационной безопасности личности будет способствовать формированию правого государства и гражданского общества, содействовать всестороннему развитию личности.

УДК 004.056.55

Е.В. Белюженко, В.А. Липницкий

ОСОБЕННОСТИ ПРЕПОДАВАНИЯ КУРСА «ПРИКЛАДНАЯ МАТЕМАТИКА» В ВОЕННОЙ АКАДЕМИИ РЕСПУБЛИКИ БЕЛАРУСЬ

Давно известен афоризм: «Техника – овеществленная математика». Его лишь усилил XXI в.: «Новая техника требует новой математики, а серьезная новая техника требует серьезной новой математики».

С последней четверти XX в. наша цивилизация постепенно переходит в информационную эпоху, когда точная и достоверная информация в конкретный момент времени может оказать решающее влияние на судьбы людей и целых стран (диспетчерские службы в аэропортах, современные войны). Информационную эпоху характеризуют экспоненциально растущие объемы потоков передаваемой и хранящейся информации, которая требует своей защиты.

Защита информации включает в себя два аспекта: защита от разного рода помех и шумов и защита от несанкционированного доступа. Оба эти аспекта взаимодополняемые и взаимопересекающиеся. Защита информации от помех решается средствами помехоустойчивого кодирования. Сегодняшние методы криптографической защиты информации, как и помехоустойчивое кодирование, насыщены методами современной математики в сочетании с компьютерными средствами.

Кроме того, средства обработки цифровой информации, применяемые сегодня в системах локации, навигации, организации трафика, а также в системах защиты информации, требуют современного математического аппарата.

В целях удовлетворения потребностей курсов инфокоммуникационной обработки, хранения, передачи и защиты информации в Военной академии Республики Беларусь, как и в других учреждениях высшего образования Республики Беларусь, организован курс «Прикладная математика». Он состоит из следующих разделов: «Элементы теории чисел», «Основы теории групп», «Классическая криптография», «Элементы современной криптографии», «Кольца и идеалы», «Свойства полей и полей Галуа», «Теория конечных полей для помехоустойчивого кодирования и криптографии».

Выпускники факультета связи и автоматизированных систем управления Военной академии Республики Беларусь должны быть профессионально подготовлены в области основных исторических, теоретических и методологических положений передачи, хранения и защиты информации как от помех, так и от несанкционированного

доступа. Также курсантам необходимо обладать практическими навыками использования современных алгоритмов криптографической защиты информации. В связи с этим изучение дисциплины «Прикладная математика» и факультативного курса «Защита информации» представляется необходимым, полезным и актуальным.

Знание математических основ защиты информации от помех и несанкционированного доступа необходимо для действенного усвоения алгоритмов и сути современных криптосистем, с которыми, возможно, придется столкнуться в своей деятельности будущим специалистам-инженерам.

Изучение таких разделов алгебры, как «Теория чисел», «Теория групп» приводит к понимаю курсантами основ криптографии, принципов построения различных алгоритмов.

Как показывает практика, вычисления различных величин малых порядков не вызывают особых затруднений, но работа с числами длиной 10 и более знаков вынуждает курсантов разрабатывать алгоритмы, используя ранее изученные языки программирования, такие как, например, C++ и C#. Программа курса построена так, что написав простой алгоритм для решения простой задачи, курсант совершенствует, усложняет его, а затем применяет для успешного решения задачи более высокого уровня сложности.

Необходимо отметить, что разработка алгоритмов на различных языках программирования не входит в программу дисциплины, но такой подход значительно сокращает время решения поставленной задачи. К тому же реализованный однажды алгоритм можно использовать многократно.

Важным аспектом такого подхода является то, что для реализации конкретной задачи при помощи программирования курсанту необходимо мыслить в нескольких плоскостях: как реализовать алгоритм математически и как сделать его понятным для машины, чтобы избежать критических ситуаций. Если при изучении дисциплины «Основы алгоритмизации и программирования» был важен результат, то сейчас курсанту важно дальнейшее использование результата.

Например, внешне элементарный алгоритм разложения целых чисел на простые множители уже вызывает трудности для программирования. В результате написания программы можно вывести результат на экран и на этом практическое применение такого алгоритма заканчивается. А можно результат записать в виде одномерного массива и в дальнейшем использовать его для вычисления, скажем, значений функции Эйлера.

Скорость нахождения решения поставленной задачи стимулирует курсантов на использование ранее изученных языков программирования.

На данном этапе мы не ставим цель написать эффективный алгоритм. Наша задача – сформировать у курсантов стремление мыслить широко, актуализировать ранее полученные знания и применить их на практике.

Что касается оказания помощи преподавателем в обсуждении и написании алгоритма на языке программирования, то такая помощь оказывается со стороны профессорско-преподавательского состава кафедры высшей математики и физики, так как многие преподаватели знакомы в разной степени с такими языками программирования, как Pascal, C, C++ и C#.

УДК 343.985.7:343.542.1

П.Л. Боровик

КУРС ПОВЫШЕНИЯ КВАЛИФИКАЦИИ СОТРУДНИКОВ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ БЕЛАРУСИ И СТРАН СНГ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ДЕТСКОЙ ПОРНОГРАФИИ В СЕТИ ИНТЕРНЕТ: ПРЕДПОСЫЛКИ, СОДЕРЖАНИЕ И ПЕРСПЕКТИВЫ

Динамика преступности, связанной с оборотом детской порнографии, позволяет утверждать, что в Республике Беларусь, как и во всем мире, по-прежнему продолжается период ее роста. Если с 2006 г. по 2009 г. среднегодовой темп прироста выявленных в Беларуси преступлений данного вида составлял 26 %, то с 2010 г. по 2013 г. этот показатель увеличился на 9 %. При этом наибольшую опасность представляют порнографические материалы с изображением несовершеннолетних, распространяемые в сети Интернет. С учетом широкого распространения компьютерной техники, цифровых фото- и видеозаписывающих устройств и иных информационно-коммуникационных технологий изготовление и сбыт детской порнографии приобрели угрожающие масштабы и, как правило, являются преступными деяниями международного характера. Так, по некоторым оценкам, с 1996 г. количество детской порнографии в сети Интернет возросло на 2000 %, а общее число веб-сайтов, предлагающих подобную продукцию, превышает 100 тыс.

В нашей стране оперативно-следственная практика располагает многочисленными примерами успешного выявления и расследования преступлений в сфере оборота детской порнографии. Вместе с тем анализ эмпирической базы по избранной теме позволил не только обобщить положительный практический опыт производства по материалам и делам данного вида, но и выявить некоторые типичные ошибки. Результаты проведенного исследования (нами изучено 45 архивных уголовных дел об обороте детской порнографии, расследованных по ст. 173, ч. 2 ст. 343 УК Республики Беларусь (в редакции закона Республики Беларусь от 4 мая 2005 г. № 15-З) и ст. 343^1 УК (в редакции закона Республики Беларусь от 10 ноября 2008 г. № 451-З) на территории республики за период с 2005 г. по 2012 г., что составило 95,74 % от общего количества завершенных дел рассматриваемой категории за указанный период; 128 архивных уголовных дел об обороте общего вида порнографии, необходимость анализа которых вызвана сходством субъекта и предмета преступления, а также способов совершения общественно опасного деяния), анкетирование 152 следователей и оперативных работников, специализирующихся на выявлении и расследовании рассматриваемых деяний в Республике Беларусь) позволили обнаружить ряд существенных проблем, возникающих на практике.

Так, одной из них является отсутствие единообразного подхода к пониманию сущности детской порнографии, что в ряде случаев ведет к игнорированию отдельных признаков этого социально опасного явления при проведении проверочных, следственных и иных процессуальных действий, а также при принятии решения о возбуждении уголовного дела. Это обусловлено прежде всего тем, что в литературе, посвященной данной проблематике, а также в соответствующих нормативных правовых актах содержатся определения детской порнографии, не позволяющие полно и отчетливо уяснить ее сущность. Отсутствие научно обоснованных критериев определения предмета преступного посягательства по уголовным делам обозначенного вида констатируют 81,58 % опрошенных нами следователей и оперативных работников.

Рассматривая результаты изучения оперативно-следственной и судебной практики о преступлениях, предусмотренных ст. 343^1 УК, нельзя оставлять вне сферы внимания и проблему неоднозначной квалификации таких видов преступного деяния, как распространение, рекламирование и публичная демонстрация порнографической продукции применительно к сетям электросвязи общего пользования, включая сеть Интернет. Данное положение дел, изначально детерминированное действующей редакцией указанной уголовно-правовой нормы, иногда приводит к неверной юридической оценке деяния и, как следствие, необоснованному судебному решению. Это обусловлено еще и тем, что в литературе, посвященной этой проблеме, имеются спорные толкования указанных деяний и отсутствуют четкие научно обоснованные рекомендации по их разграничению.

Анализ практики расследования преступлений об обороте детской порнографии показывает, что не всегда в полном объеме исследуется и

предмет доказывания. Ненадлежащее определение органом уголовного преследования круга обстоятельств, подлежащих установлению при расследовании рассматриваемых преступлений, ведет к ненадлежащему планированию, тактическим просчетам, а в итоге снижает эффективность всего расследования. Отчасти это объясняется неразработанностью научно обоснованной системы обстоятельств, подлежащих доказыванию при расследовании рассматриваемых преступлений, что подтверждают преобладающее большинство опрошенных нами респондентов из числа следователей.

Изучение уголовных дел свидетельствует также о часто встречающихся недочетах прежде всего тактического и методического характера, связанных с установлением оснований к возбуждению уголовных дел и проведением соответствующих следственных и иных процессуальных действий. Недостаточное качество доследственных проверок по указанным категориям дел обусловлено и отсутствием надлежащих криминалистических рекомендаций по рассматриваемому вопросу. Настоятельную потребность практики в наличии таких рекомендаций подтвердили 94,09 % опрошенных нами респондентов из числа следователей и оперативных работников.

Наибольшую сложность по делам данной категории вызывают вопросы назначения и проведения судебной экспертизы по данной категории дел. Так, например, на сегодняшний день для установления признаков детской порнографии практика идет по пути назначения искусствоведческих экспертиз. Однако искусствоведческая экспертиза имеет свои специфические цели (анализ и оценка художественных произведений с целью их атрибуции, определения историко-культурной, материальной и иной ценности) и не может решать задачи отнесения предметов и материалов к категории детской порнографии. Все это приводит к тому, что выводы экспертов являются не результатом применения специальных познаний, как того требует закон, а результатом субъективной оценки, основанной на личных взглядах и вкусах на уровне бытовых представлений и воспитания. Необходимые в этих случаях специалисты, как правило, не привлекаются. Кроме того, головным экспертным учреждением в настоящее время является Республиканская экспертная комиссия при Министерстве культуры Республики Беларусь, в составе которой нет ни одного судебного эксперта. Сама комиссия существует на правах общественного объединения. Говорить о соблюдении норм уголовно-процессуального законодательства и рекомендаций криминалистики в этом случае можно лишь условно.

Под углом зрения обозначенных проблем одной из задач для Академии МВД Республики Беларусь в 2011 г. стал вопрос организации международного курса повышения квалификации сотрудников право-

охранительных органов Беларуси и стран СНГ (Россия, Украина, Молдова и др.) по противодействию детской порнографии в сети Интернет. Его основу должны были составить не столько теоретические положения профильных юридических дисциплин, сколько научно обоснованные практические рекомендации, направленные на совершенствование деятельности органов уголовного преследования в рассматриваемой сфере. Следует отметить, что до указанного времени в системе подготовки сотрудников правоохранительных органов должного внимания вопросам их переподготовки и повышения квалификации в рамках обозначенной тематики не уделялось.

Указанные обстоятельства обусловили актуальность, теоретическую и практическую значимость проведения комплексной научно-исследовательской работы, посвященной рассматриваемой проблематике и являющейся составной частью научных изысканий, осуществляемых в соответствии с п. 11 Плана распределения полномочий по реализации Государственной программы противодействия торговле людьми, нелегальной миграции и связанным с ними противоправным деяниям на 2011–2013 годы.

В результате проведенного научного исследования (Боровик П.Л., Федоров Г.В. Детская порнография: выявление и возбуждение уголовных дел / под ред. В.П. Шиенка. М. : Юрлитинформ, 2013. 248 с.), основной целью которого являлась разработка комплекса научно обоснованных криминалистических рекомендаций, направленных на совершенствование деятельности органов уголовного преследования по выявлению преступлений и возбуждению уголовных дел об обороте порнографии с изображением несовершеннолетнего, проведению отдельных следственных и иных процессуальных действий, а также соответствующих предложений по изменению и дополнению отдельных норм некоторых правовых актов Республики Беларусь, нами были разработаны: научно обоснованные критерии определения детской порнографии; выявлены криминалистически значимые особенности личности преступника по делам об обороте детской порнографии, а также потерпевшего от смежных и сопутствующих деяний; исследованы сущность и содержание способов оборота порнографической продукции с изображением несовершеннолетнего; конкретизированы и детализированы обстоятельства, подлежащие установлению при расследовании уголовных дел рассматриваемого вида; разработан комплекс криминалистических рекомендаций, направленных на совершенствование деятельности органов уголовного преследования по возбуждению уголовных дел; разработаны предложения по созданию организационных основ экспертизы продукции, имеющей признаки порнографии с изображением несовершеннолетнего; предложен комплекс практических ре-

комендаций криминалистического характера по назначению и производству судебной экспертизы указанной продукции и ее оценке.

В 2011 г. автором был подготовлен учебно-тематический план международного курса повышения квалификации «Противодействие детской порнографии в интернете» (см. таблицу), предназначенного для сотрудников правоохранительных органов, разработаны лекции и иные материалы (методические рекомендации для проведения семинарских и практических занятий, раздаточный материал и пр.), в которых нашли свое отражение результаты проведенного исследования. В сентябре этого же года данный курс успешно апробирован в Международном учебном центре подготовки, повышения квалификации, переподготовки кадров в сфере миграции и противодействия торговле людьми на базе Академии МВД Беларуси, где и проводится в настоящее время.

№ п/п	Тематика	Итого	Количество учебных часов				
			Распределение по видам занятий				
			Лекции	Практические занятия	Семинарские занятия	Круглые столы, тематические дискуссии	Деловые игры
1	**Международное и национальное законодательство в сфере противодействия детской порнографии**	2	2	–	–	–	–
1.1.	Международное и национальное законодательство в сфере противодействия детской порнографии	2	2	–	–	–	–
2	**Уголовно-правовая, криминологическая и криминалистическая характеристика преступлений, связанных с детской порнографией**	8	6	–	–	2	–
2.1	Уголовно-правовая и криминологическая характеристика преступлений, связанных с детской порнографией	2	2	–	–	–	–
2.2	Криминалистическая структура личности преступника, совершающего деяния, связанные с детской порнографией	2	2	–	–	–	–

2.3	Характеристика способов и следов совершения преступлений, связанных с детской порнографией	4	2	–	–	2	–
3	**Деятельность по выявлению и расследованию преступлений, связанных с детской порнографией**	24	10	2	2	2	8
3.1	Особенности возбуждения уголовных дел о преступлениях, связанных с детской порнографией	4	2	–	–	–	2
3.2	Предмет доказывания и типичные следственные ситуации по делам о преступлениях, связанных с детской порнографией	4	2	–	–	–	2
3.3	Взаимодействие следователя с оперативными подразделениями, занимающимися выявлением преступлений, связанных с детской порнографией	4	2	–	–	–	2
3.4	Тактика проведения отдельных следственных действий по делам о преступлениях, связанных с детской порнографией (осмотр, выемка, допрос и др.)	6	2	–	2	–	2
3.5	Использование специальных знаний при расследовании преступлений, связанных с детской порнографией	6	2	2	–	2	–
4	**Международное сотрудничество в сфере противодействия детской порнографии**	4	4	–	–	–	–
4.1	Порядок и особенности взаимодействия с правоохранительными органами иностранных государств в сфере противодействия детской порнографии	4	4	–	–	–	–
	Всего:	38	22	2	2	4	8

Целью предложенного нами курса является повышение квалификации сотрудников правоохранительных органов в сфере выявления и расследования преступлений, связанных с оборотом порнографической продукции с изображением несовершеннолетних.

Достижение указанной цели обеспечивается посредством решения ряда следующих задач: анализ международного и национального законодательства в сфере противодействия детской порнографии; изучение уголовно-правовой, криминологической и криминалистической характеристики преступлений, связанных с детской порнографией; приобретение необходимых знаний и формирование практических навыков организации деятельности по выявлению, раскрытию и расследованию преступлений рассматриваемого вида; изучение практики международного сотрудничества в сфере противодействия порнографии с участием несовершеннолетнего.

Предполагается, что в результате освоения данного курса повышения квалификации слушатели должны знать: международные и национальные правовые акты в сфере противодействия обороту детской порнографии; уголовно-правовую, криминологическую и криминалистическую характеристики преступлений данного вида, а также меры по их профилактике; характеристику способов совершения деяний по делам данной категории; особенности возбуждения уголовных дел, предмет доказывания и типичные следственные ситуации по делам о преступлениях, связанных с оборотом детской порнографии; порядок взаимодействия следователя с оперативными подразделениями, занимающимися выявлением преступлений обозначенного вида; уметь: проводить отдельные следственные действия по делам о преступлениях, связанных с детской порнографией (осмотр, выемка, допрос и др.); иметь навыки: использования специальных знаний при расследовании преступлений об обороте порнографии с участием несовершеннолетнего; организации взаимодействия с правоохранительными органами иностранных государств в сфере противодействия уголовно наказуемым деяниям рассматриваемого вида.

Материал курса изучается на лекциях, семинарских занятиях, семинарах по обмену опытом; умения и навыки отрабатываются в ходе проведения практических занятий, в процессе решения ситуационных задач, проведения занятий типа «Круглый стол», а также в процессе самостоятельной работы обучающихся путем последовательного усвоения материала от простого к сложному. Общее количество часов в соответствии с учебным планом распределяется по видам занятий следующим образом: 22 – лекции, 2 – семинары по обмену опытом, 4 – занятия типа «Круглый стол», 8 – решение ситуационных задач, 2 – практические занятия. Итоговой формой контроля является собеседование (экзамен).

В качестве экспертов, участвующих в проведении учебных занятий по данному направлению, приглашаются опытные практические работники из правоохранительных органов, Следственного комитета, прокуратуры, суда, а также экспертных подразделений. Кроме того, в

рамках данного курса учебный процесс обеспечен специалистами из Великобритании – экспертами Колледжа по переподготовке полицейских кадров Соединенного королевства Великобритании и Северной Ирландии, обладающими многолетним опытом работы в специализированных подразделения Скотланд-Ярда по борьбе с торговлей людьми и детской порнографией.

Обобщив опыт организации и проведения в 2011–2014 гг. учебных занятий в рамках обозначенной тематики, можно с уверенностью констатировать, что разработанный нами курс повышения квалификации занимает центральное место в системе подготовки специалистов, специализирующихся по противодействию распространению детской порнографии в сети Интернет, что обусловлено потребностями правоохранительной практики. Учебный курс позволяет сотрудникам правоохранительных органов не только повысить свою квалификацию в сфере противодействия обороту порнографической продукции с изображением несовершеннолетних в сети Интернет, но и обменяться опытом, наладить тесное взаимодействие науки и практики. В целях определения качественного уровня организации обучения в рамках представленного курса повышения квалификации проводится анкетирование слушателей, которые традиционно дают высокую оценку проведенному тренингу и методическому обеспечению занятий.

Говоря о дальнейшем развитии этого учебного курса, следует обратить внимание на необходимость проработки вопроса о повышении квалификации в рамках обозначенной тематики представителей судов и прокуратуры. Это связано прежде всего с тем, что противодействие детской порнографии – деятельность комплексная, направленная, с одной стороны, на выявление и расследование преступлений рассматриваемого вида, а с другой – на полное изобличение лиц, виновных в их совершении, и вынесение справедливого приговора в суде. Поэтому эффективность данной деятельности обусловлена не только квалификацией оперативного работника или следователя, но и уровнем подготовки прокурора и судьи, их осведомленностью о способах и механизмах совершения рассматриваемых уголовно наказуемых деяний.

Таким образом, в условиях роста преступности, связанной с оборотом детской порнографии в сети Интернет, особую актуальность приобретает проблема качественного повышения квалификации специалистов, способных надлежащим образом реагировать на современные угрозы общественной и индивидуальной нравственности. Работа профессорско-преподавательского состава, участвующего в подготовке специалистов в этом направлении, должна основываться на изучении научной литературы, освещающей проблемные вопросы в данной сфере, глубоком анализе существующей практики противодействия пре-

ступлениям рассматриваемой категории, а также обобщении, использовании и передаче положительного опыта этой практической деятельности. При определении объема знаний, умений и навыков в рамках исследуемой проблематики следует исходить прежде всего из потребностей правоприменительной практики, наиболее часто встречающихся трудностей и ошибок, которые ее сопровождают. Указанные обстоятельства предопределили необходимость проведения комплексного научного исследования проблемных аспектов противодействия детской порнографии, результаты которого нашли свое отражение в содержании и методике проводимого с 2011 г. по настоящее время в Академии МВД Республики Беларусь курса повышения квалификации сотрудников правоохранительных органов Беларуси и стран СНГ «Противодействие детской порнографии в интернете».

УДК 349:37.035.41

Е.В. Булгакова

НЕОБХОДИМОСТЬ РАЗРАБОТКИ И ВНЕДРЕНИЯ В УЧЕБНЫЙ ПРОЦЕСС ПРОФЕССИОНАЛЬНЫХ КОМПЬЮТЕРНЫХ ИГР, СПОСОБСТВУЮЩИХ ФОРМИРОВАНИЮ КОМПЕТЕНЦИЙ ЮРИСТА В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационные технологии прочно вошли в профессиональную деятельность юриста. Угрозы информационной безопасности, связанные с информатизацией юридической деятельности, переходом к системе электронного правосудия, носят глобальный характер, и главная уязвимость, как мы полагаем, заключается в пробелах формирования компетенций юриста в сфере информационной безопасности. Сложившаяся ситуация приводит к утечке конфиденциальной информации по различным каналам, искажению, уничтожению информации и др.

Уклон в обеспечении информационной безопасности делается на защиту автоматизированных информационных систем, которые используют юристы в своей профессиональной деятельности, а вот меры по обеспечению личной информационной безопасности (как субъектов правоприменительной деятельности), в том числе и как пользователей этих систем, запоздали и являются недостаточными.

В этой связи полагаем, что подготовке и переподготовке юристов в вопросах обеспечения информационной безопасности не уделяется должного внимания, что негативно влияет на процесс обеспечения информационной безопасности юридической деятельности. Знания, умения и навыки в сфере информационных технологий и обеспечения информационной безопасности значительно отстали относительно стремительного развития и внедрения информационных технологий в деятельность юриста.

Учитывая сложившуюся на практике ситуацию с обеспечением информационной безопасности юристов, автор статьи обращается к необходимости формирования компетенций юриста в сфере информационной безопасности с применением инновационных методов обучения. В России на сегодняшний день подготовку юристов в сфере информационного права и правового регулирования информационной безопасности осуществляют несколько образовательных организаций высшего образования и ведущие позиции занимает Российская правовая академия Министерства юстиции Российской Федерации. Профессиональная подготовка юристов (бакалавров, специалистов, магистров) по правовому обеспечению информатизации и информационной безопасности осуществляется кафедрой информационного права, информатики и математики Российской правовой академии Министерства юстиции Российской Федерации, уделяя особое внимание разработке современных методик преподавания. В программу подготовки юристов входят такие дисциплины, как «Информационное право», «Информационные технологии в юридической деятельности», «Правовая информатика», «Правовое обеспечение информационной безопасности» и др. С электронными учебными методическими комплексами (ЭУМК) можно ознакомиться на сайте РПА Минюста России (http://www.rpa-mu.ru), портале «Юстиция» (http://www.pravoinfo.su).

Примером современных образовательных методик, используемых в учебном процессе преподавателями кафедры информационного права, информатики и математики РПА Минюста России по подготовке юристов, может служить компьютерная игра по формированию компетенций, связанных с информационной безопасностью юриста. Компьютерная игра была разработана кандидатом юридических наук, доцентом кафедры информационного права, информатики и математики Е.В. Булгаковой и преподавателем кафедры информационной безопасности Волгоградского государственного университета Н.А. Корневым. Целью создания игры и ее использования в учебном процессе является непосредственная отработка навыков и умений на основе полученных теоретических знаний применения методов и средств защиты по противодействию угрозам информационной безопасности юриста.

Игра по количеству игроков относится к многопользовательским онлайновым играм, к жанру пошаговой локальной стратегии. Согласно теории игр была разработана игровая матрица, в которой строками являются стратегии атаки, а столбцами стратегии защиты. На пересечении столбца и строки стоит коэффициент успешности выбранного средства защиты: если он близок к единице, то вероятность успешной атаки минимальна, соответственно, если близок к нулю, то вероятность успешной атаки высока. В учебном процессе используется игра со смешенной стратегией, так как при игре в чистых стратегиях будет все время один исход. В данной игре как злоумышленник, так и защитник наделены организационно-правовыми, техническими, программными средствами защиты (рис. 1).

Фигуры и ее вид	Защитник	Злоумышленник
Общий вид сервера		
Общее вид фигур (противник не видит средства фигуры)		
Вид со стороны игрока (или противника в случае раскрытия фигуры)		
Организационно-правовые		
Технические		
Программные		
Вид со стороны игрока, если их средство стало известно противнику		
Организационно-правовые		
Технические		
Программные		

Рис.1. Изображение средств атаки и защиты

Исходя из вышесказанного, можно сформулировать следующие правила игры:

1. Организационно-правовые средства + Технические средства = Организационно-правовые средства.
2. Технические средства + Программные средства = Технические средства.
3. Программные средства + Организационно-правовые средства = Программные средства.

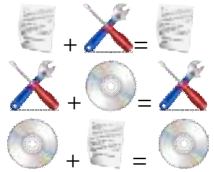
Исходя из классической теории игр, можно представить игру в матричном виде (табл. 1).

Таблица 1

Матрица игры

	Организационно-правовые	Программные	Технические
Организационно-правовые	0	-1	1
Программные	1	0	-1
Технические	-1	1	0

Визуально правила можно представить следующим образом:



Игровое поле состоит из таблицы размером 6 × 7, для начального заполнения игроку выделятся две нижние строчки.

Игрок может выбрать место расположения сервера в этих строках, после чего автоматически сгенерируются средства атаки (защиты), если игрока не устраивает расположение средств атаки (защиты), он может повторять их заполнение, пока не добьется оптимального расположения (рис. 2).

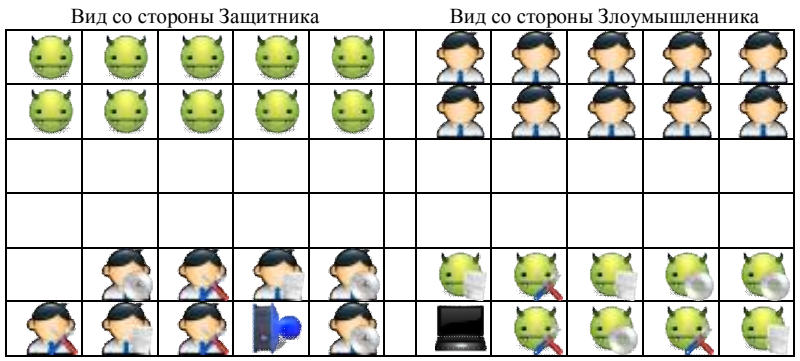


Рис. 2. Вид игрового поля

После того как соперники расположили свои фигуры, одному из них предоставляться право хода, ходы осуществляться по очереди (табл. 2).

Таблица 2

Список возможных ходов и средств

Средства	Ход вперед	Ход назад	Ход влево	Ход вправо
Организационно-правовые (СИ)	1	1	1	1
Технические	1	1	1	1
Технические	1	1	1	1
Сервер (ноутбук)	0	0	0	0

Выбор игрока, который сделает первый ход, определяется псевдослучайным способом, на основе пары генераторов псевдослучайных чисел. В данном случае первый ход сделал злоумышленник (рис. 3). Ходы симметрично отображаются относительно доски.

Далее предоставляется право хода защитнику (рис. 4), а злоумышленник будет ожидать выбора защитника.

После ответного хода нарушителя возникает острый момент и кто-то должен первым атаковать, исходя из правил: Организационно-правовые средства + Технические средства = Организационно-правовые средства. В данном случае (рис. 5) атака злоумышленника или оборона будет успешной для него, но не один из игроков не знает наверняка какое средство у противника до удара.

Рис. 3. Ход злоумышленника

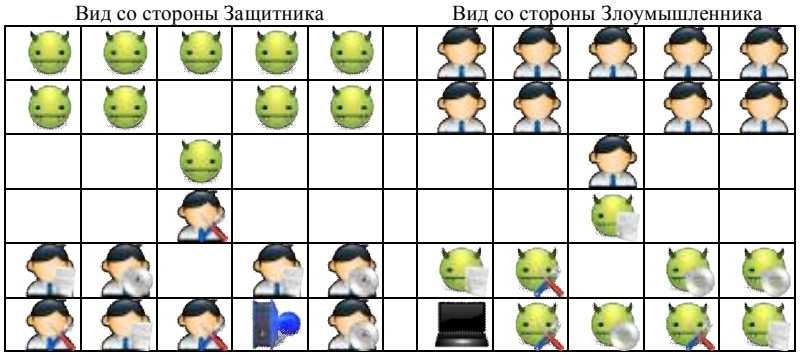


Рис. 4. Ход защитника

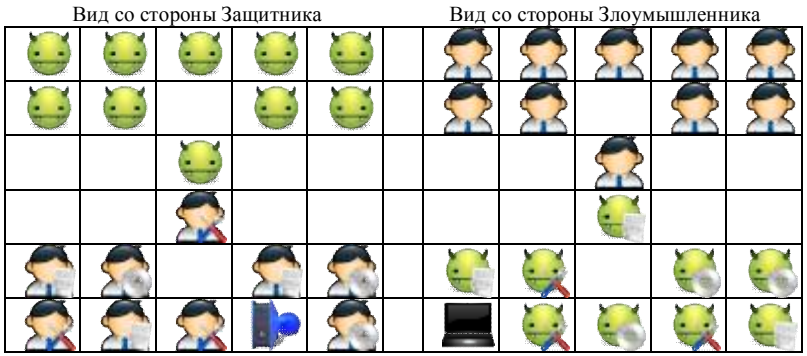


Рис. 5. Удар злоумышленника

При этом не имеет значения, кто нанесет удар первым, так как исход игры зависит от средств противника.

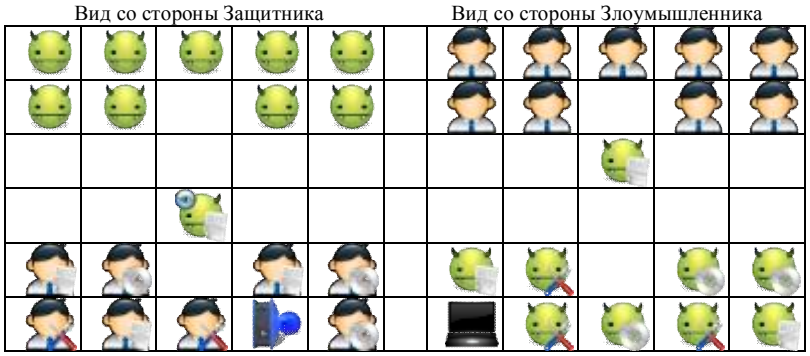


Рис. 6. Вид после удара

После удара противнику раскрывается фигура оппонента, и он знает, каким средством противостоять (рис. 6).

Игра будет продолжаться, пока один из игроков не найдет место расположения компьютера другого.

Полагаем, что использование профессиональных компьютерных игр в учебном процессе позволит повысить компетентность юриста в сфере обеспечения информационной безопасности.

Таким образом, юристу, живущему и работающему в информационном обществе, приходится задумываться о вопросах информационной безопасности не только в рамках своих профессиональных обязанностей, но и помнить о соблюдении данных мер в информационном пространстве в целом. Профессиональные риски в данной сфере увеличиваются ввиду появления качественно новых видов угроз информационной безопасности и пренебрежения мерами по обеспечению информационной безопасности, из-за недостатка знаний, умений и навыков по защите информации, противодействию угрозам информационной безопасности, уязвимости профессиональных автоматизированных систем могут привести к негативным последствиям. Следовательно, одним из компонентов компетентности современного юриста являются знания, умения и навыки безопасного применения информационных технологий, соблюдение мер по защите информации, требований правовых актов в области защиты государственной тайны и информационной безопасности, обеспечения режима секретности. Юристам необходимо понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе. Динамичность процесса развития информационных технологий, применяемых в деятельности юриста, сопряженные с этим новые угрозы информационной безопасности определяют специфику подготовки юристов, ее уровень напрямую зависит от применения в учебном процессе современных образовательных методик.

УДК 65.01

О.Н. Ежова, О.Р. Шебец

ПОДГОТОВКА СОТРУДНИКОВ УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ К ВНЕДРЕНИЮ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ И ТЕХНИЧЕСКИХ СРЕДСТВ В ПРАКТИКУ ИСПОЛНЕНИЯ НАКАЗАНИЙ КАК ОСНОВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Одной из задач, стоящих перед Федеральной службой исполнения наказаний России, в соответствии с Концепцией развития уголовно-

исполнительной системы Российской Федерации до 2020 года является повышение эффективности управления уголовно-исполнительной системой, использование инновационных разработок и научного потенциала.

Начиная с 2010 г., была проделана большая работа, направленная на внедрение в деятельность УИС современных информационных технологий. Можно отметить наиболее значимые достижения в этой области:

в соответствии с Ведомственной целевой программой «Внедрение современных информационно-коммуникационных технологий в деятельность Федеральной службы исполнения наказаний на 2011–2013 годы» создана ресурсная основа для формирования единого 3-уровневого информационного пространства ФСИН России и осуществление единой технической политики в сфере информационного и телекоммуникационного обеспечения деятельности УИС;

создана автоматизированная система делопроизводства УИС (все учреждения и органы УИС оснащены автоматизированными рабочими местами);

в УИС функционируют свыше 60 цифровых канала передачи данных из территориальных органов в подразделения;

все территориальные органы ФСИН России и учреждения, непосредственно подчиненные ей, имеют электронную почту;

начиная с 2010 г., в деятельность УИС внедрен программный комплекс автоматизированного картотечного учета спецконтингента (ПК АКУС), который используется во всех исправительных колониях и колониях-поселениях, следственных изоляторах, в уголовно исполнительных инспекциях;

создана информационная система кадрового учета УИС, автоматизированы процессы бухгалтерского учета и бюджетной отчетности;

проведена аттестация объектов информатизации подразделений собственной безопасности ФСИН России;

автоматизирована информационная система обработки подразделениями УИС статистической отчетности, сформирована центральная база данных статистической отчетности; в территориальных органах созданы собственные локальные вычислительные сети;

начиная с 2010 г., уголовно-исполнительными инспекциями используются электронные средства надзора и контроля, совокупность которых составляет систему электронного мониторинга подконтрольных лиц ФСИН России (СЭМПЛ) для обеспечения дистанционного надзора за осужденными к ограничению свободы и за лицами, в отношении которых избрана мера пресечения в виде домашнего ареста.

В рамках внедрения в деятельность ФСИН России инновационных технологий в соответствии с распоряжением ФСИН России от 4 февра-

ля 2010 г. № 20-р «Об организации обмена документами по каналам электронной почты» с 10 февраля 2010 г. осуществляется обмен документами, не требующими заверения гербовой печатью, в виде сообщений электронной почты с использованием аппаратно-программного комплекса REX-400 между ФСИН России, учреждениями, непосредственно подчиненными ФСИН России, территориальными органами и образовательными учреждениями.

В настоящее время информационный ресурс УИС составляет свыше 250 форм отчетных документов.

ПТК (ПК) АКУС позволяет решать задачи по обеспечению текущей деятельности учреждений УИС в сфере документооборота, вести накопление и обработку данных об абонентах, быстро получать необходимую информацию, обобщенные данные, статистические сводки, справки, решает задачи по обеспечению и координации деятельности служб учреждений в сфере документооборота. Все пользователи ПТК АКУС в пределах учреждения работают с единой базой данных.

На сегодняшний день СЭМПЛ функционирует во всех территориальных органах ФСИН России. Наказание в виде ограничения свободы введено в 2010 г., а возложение на УИИ контроля за нахождением подозреваемых или обвиняемых в месте исполнения меры пресечения в виде домашнего ареста – с 2012 г.

Как показала практика, применение оборудования СЭМПЛ позволяет сотрудникам УИИ более эффективно осуществлять надзор за соблюдением ограничений подконтрольными лицами, выявлять латентные преступления, установление которых без применения электронного мониторинга было бы затруднено, и незамедлительно применять меры взыскания к нарушителям.

Под информационной безопасностью в УИС следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.

При построении системы управления информационной безопасностью в УИС возникает целый ряд вопросов, относящихся к администрированию механизмов безопасности, непосредственно не относящихся к безопасности программных средств и данных. На первый план выходит человек со своими потребностями в доступе к полноценной информации и его защита от ее негативного воздействия. Эффективное управление сферой информационной безопасности не только ограждает от информационных угроз сотрудников УИС комплексом специальных средств, но и закладывает фундамент информационно-безопасного взаимодействия в социальной среде.

В этой связи следует рассматривать следующие виды защиты.

Правовая защита. Правовая защита информации как ресурса определяется межгосударственными договорами, конвенциями, декларациями и реализуется патентами, авторским правом и лицензиями на их защиту. В случае сотрудника УИС – это еще и нормативно-правовые акты, регламентирующие действия сотрудника при работе с информационными ресурсами с учетом всех возможных ситуаций, в том числе и ситуаций поломки оборудования, отключения света и т. д.

Организационная защита – это регламентация деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.

Электронные документы должны храниться на электронных носителях, которые обеспечили бы их сохранность, однако и у электронных носителей есть определенный срок годности, поэтому возникает проблема сохранности информации. В УИИ и СИЗО, где особенно большой объем информации, сотрудники не всегда обновляют резервные копии, что может привести к утере информации. В связи с этим сотрудники вынуждены дублировать информацию и на бумажных носителей, что значительно увеличивает трудоемкость.

Информационно-психологическая защита. Использование информационных технологий, с одной стороны, существенно сокращает время на подготовку справок, отчетов и списков, улучшает контроль за сроками пребывания, исключает возможность фальсификации документов, облегчает формирование пакета документов при проведении розыскных мероприятий в случае побега, а с другой стороны, увеличивает объем информации, которую должны обрабатывать за день сотрудники УИС.

Обеспечить информационную безопасность способен только хорошо подготовленный специалист в области информационных технологий.

Подготовке сотрудников УИС в этом направлении уделяется достаточно много внимания, однако психологической подготовкой сотрудников для работы с информационными технологиями практически совсем не занимаются.

С введением в деятельность УИС информационных технологий у сотрудников увеличивается психологический стресс (несоответствие между нагрузкой и имеющимися ресурсами, сопровождаемое такими эмоциями, как страх, гнев, удрученность и т. д.), который подразделяется на стресс информационный и эмоциональный. Информационный стресс возникает в ситуациях информационных перегрузок, когда человек не справляется с задачей, не успевает принимать верные решения в требуемом темпе при высокой степени ответственности за свои

действия. Эмоциональный стресс появляется в ситуациях угрозы, опасности, обиды и др.

Если сотрудник не может справиться с нагрузками, то это при использовании информационных технологий является угрозой (из-за невнимательности и рассеянности) информационной безопасности.

В связи с этим для обеспечения информационной безопасности особое внимание следует уделять формированию у сотрудников УИС психологической стрессоустойчивости. Этому может способствовать обучение сотрудников методам саморегуляции, овладение которыми позволит сохранить психическое здоровье, справиться с негативными последствиями стрессов, предотвратить профессиональную деформацию. Начинать данную работу необходимо как можно раньше, еще во время обучения будущих сотрудников пенитенциарных и правоохранительных учреждений. В выигрыше останется как сотрудник, ставший высококвалифицированным специалистом, так и общество, получившее человека, который способен успешно преодолевать экстремальные ситуации в важном и опасном деле – защите правопорядка и охране спокойствия граждан.

Подытоживая вышеизложенный материал, можно сказать, что решение проблемы информационной безопасности должно носить системный характер, при этом нужно уделять внимание не только техническим и правовым сторонам защиты информации, но и психологической подготовке сотрудников.

УДК 347.45

А.С. Ласкевич

РАСТОРЖЕНИЕ КОНТРАКТОВ ПО ПОДГОТОВКЕ СПЕЦИАЛИСТОВ С ВЫСШИМ ОБРАЗОВАНИЕМ ДЛЯ ВООРУЖЕННЫХ СИЛ В СВЯЗИ С ОТКАЗОМ В ДОПУСКЕ К ГОСУДАРСТВЕННЫМ СЕКРЕТАМ ИЛИ ПРЕКРАЩЕНИЕМ УКАЗАННОГО ДОПУСКА

Подготовка специалистов с высшим образованием для Вооруженных сил неразрывно связана с допуском таких специалистов в период обучения и после окончания военного учебного заведения к государственным секретам.

Законодателем определены условия предоставления гражданам допуска к государственным секретам, основания для отказа и прекращения

указанного допуска (ст. 33, 35, 37 закона Республики Беларусь «О государственных секретах», п. 10–18 Положения о порядке предоставления допуска физическим лицам к государственным секретам, утвержденного постановлением Совета Министров Республики Беларусь от 10 апреля 2004 г. № 400).

В Положении о порядке предоставления допуска физическим лицам к государственным секретам установлено, что для предоставления допуска необходимо письменное согласие физического лица на проведение органами государственной безопасности в отношении него проверочных мероприятий и временное ограничение в связи с этим права на неприкосновенность личной жизни. После согласования заключается соответствующий договор о допуске к государственным секретам на срок его действия одной из трех форм. По истечении срока действия допуска соответствующей формы осуществляется его перерегистрация и заключается новый договор (п. 10–12).

Отношения по подготовке специалистов с высшим образованием для Вооруженных сил возникают, продолжаются и прекращаются на основании соответствующего договора, именуемого контрактом, на период обучения и на пять лет прохождения военной службы на должностях офицерского состава.

Одним из оснований для отчисления (увольнения с военной службы) и расторжения контракта является отказ военнослужащему в допуске к государственным секретам или прекращение указанного допуска (п. 174, п. 174.5, п. 176, п. 176.4, п. 211, п. 211.3 Положения о порядке прохождения военной службы, утвержденного указом Президента Республики Беларусь от 25 апреля 2005 г. № 186, ч. 4 ст. 59 закона Республики Беларусь от 5 ноября 1992 г. № 1914-XII «О воинской обязанности и воинской службе»).

При этом к условиям возмещения расходов, затраченных государством на обучение военнослужащих, отчисленных из военного учебного заведения и уволенных из рядов Вооруженных сил, установленных в гл. 23 Положения о порядке прохождения военной службы, указанное основание не относится. Это позволяет военнослужащим злоупотреблять предоставленным законодателем правом в допуске к государственным секретам.

Так, военнослужащий, получающий высшее образование либо направленный после получения такого образования согласно контракту для дальнейшего прохождения военной службы, при перерегистрации допуска (заключении нового договора о допуске к государственным секретам) выражает несогласие на проведение органами государственной безопасности в отношении него проверочных мероприятий и на временное ограничение в связи с этим права на неприкосновенность личной жизни, в соответствии с чем подлежит увольнению с военной

службы, не возмещая расходы, затраченные на его подготовку. Увольнению с военной службы может также предшествовать отказ в допуске или его прекращение до истечения срока действия.

Возмещение в таких случаях расходов за обучение позволит осуществить в полной мере принцип возвратности средств, затраченных государством на подготовку специалистов с высшим образованием для Вооруженных сил.

По нашему мнению, представляется целесообразным внесение изменений в Положение о порядке прохождения военной службы, касающихся обязанности возмещения расходов за обучение при отчислении курсанта (магистранта) из военного учебного заведения, а также при увольнении офицера, не отслужившего установленный контрактом 5-летний срок после получения образования, на основании отказа военнослужащему в допуске к государственным секретам или прекращения указанного допуска.

УДК 004.056.55

Л.В. Михайловская, Е.В. Валаханович, В.А. Липницкий

СОВРЕМЕННЫЙ ПОДХОД К ПРЕПОДАВАНИЮ ТЕМЫ «СТАНДАРТЫ ШИФРОВАНИЯ»

В настоящее время в Военной академии Республики Беларусь учебная программа для ряда специальностей факультета связи и автоматизированных систем управления включает в себя дисциплины, связанные с изучением информационной безопасности, а также методов и средств защиты информации. Для успешного освоения, например, дисциплин «Основы построения техники связи», «Кодирование и цифровая обработка сигналов» и других необходимо понимание принципов и знание основных элементов криптографического преобразования информации.

Так, введенная в текущем учебном году дисциплина «Прикладная математика», преподаваемая на кафедре высшей математики и физики Военной академии Республики Беларусь, призвана ознакомить курсантов с основными математическими методами и моделями защиты информации. В ходе изучения дисциплины излагаются основные принципы конструкции, рассматриваются вопросы, связанные с реализацией шифра, выяснением устойчивости к известным видам атак. Показаны требования безопасности и цели, преимущества и ограничения шифра, способы его расширения и возможности использования помимо действий шифрования/дешифрования.

В отличие от курса «Высшая математика» в ходе преподавания данной дисциплины курсанты осваивают основные алгебраические структуры – группы, кольца, поля и поля Галуа, основы теории чисел – структуры, необходимые для построения помехоустойчивых кодов, современных криптографических систем, систем обработки сигналов и изображений.

В процессе изучения дисциплины «Прикладная математика» на учебных моделях происходит знакомство с классическими и современными криптографическими системами защиты информации: криптосистемами Цезаря (в частности, ее аффинный вариант и вариант Хилла), RSA, Рабина, Эль Гамаля и др. В то же время учебные пособия по защите информации рекомендуют в качестве образца поточного алгоритма шифрования/дешифрования использовать старый американский стандарт шифрования DES (Data Encryption Standard), который считают устаревшим ввиду небольшой длины ключа (56 бит) и необеспечивающим выполнение задачи по защите информации от несанкционированного доступа, так как имеются возможности успешного применения метода прямого перебора ключей для его взлома.

Вследствие развития современных информационных технологий существует постоянная угроза взлома и последней версии криптосистемы DES – «тройного DES». В связи с вышеизложенным целесообразнее перейти на более современный стандарт шифрования AES (Advanced Encryption Standard), обладающий высокой степенью защиты (размер блока равен 128 бит), простой структурой и высокой производительностью. Кроме того, данный алгоритм ориентирован на программно-аппаратную реализацию, на уровне внутренней архитектуры он обладает надежностью, достаточной для того, чтобы противостоять будущим попыткам взлома. Конечно, этот переход потребует серьезных программно-методических усилий: предварительного изложения теории колец, полей Галуа как фактор-колец по максимальным идеалам, освоения определенных навыков вычислений в фактор-кольцах кольца полиномов, умения создавать компьютерные программы реализации алгоритма Евклида и расширенного алгоритма Евклида в кольце полиномов, реализации арифметических действий в фактор-кольцах кольца полиномов, процедуры обращения и возведения в степень в полях Галуа характеристики 2.

Таким образом, в целях подготовки высококвалифицированных специалистов в области защиты информации в ходе обучения необходимо применять современный алгоритм AES, обеспечивающий высокую степень защиты системы. В связи с его программно-аппаратной реализацией для более глубокого освоения изучаемого стандарта возможно использование шифрования в ряде смежных учебных дисциплин.

УДК 004:34

Л.Л. Утин, Р.А. Дидковский, В.Н. Корделюк

ПРОБЛЕМНЫЕ ВОПРОСЫ, СВЯЗАННЫЕ С ПОДГОТОВКОЙ СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ

В настоящее время защита информации является сложной организационно-технической проблемой. Для ее решения создается система защиты информации, которая нормативными правовыми актами Республики Беларусь (НПА) определяется как совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации.

Требования к созданию системы защиты информации в государственных информационных системах, а также информационных системах, содержащих информацию, распространение и (или) представление которой ограничено, определяются законодательством Республики Беларусь. Отметим, что на функционирование системы защиты информации влияет работа каждого элемента. При этом в НПА требования предъявляются ко всем элементам системы, за исключением исполнителей, которые остаются наиболее уязвимым звеном данной системы.

Права, обязанности и ограничения лиц, допущенных к государственным секретам, четко регламентированы в НПА. Однако компетентностные требования к этим лицам часто не предъявляются. Лица, допущенные к государственным секретам, могут халатно относиться к выполнению обязанностей по защите информации, содержащей государственные секреты.

По данным западных исследований, порядка 80 % нарушений связано с деятельностью собственных сотрудников. Из них более 80 % инцидентов, в которых виновны сотрудники, происходят в результате неумышленных действий. Эти статистические данные свидетельствуют, что компетентность сотрудников оказывает непосредственное влияние на вопросы защиты информации. В свою очередь, компетентность специалиста базируется на знаниях, навыках и опыте.

Классически процессы повышения уровней компетентности осуществляются следующим образом:

знания получают в учреждениях образования: университетах, институтах, учреждениях переподготовки кадров и повышения квалификации;

навыки – частично в учреждении образования, но в основном на рабочих местах или на различных курсах по изучению и освоению конкретных систем, проводимых как самими производителями систем, так и аккредитованными учебными центрами;

опыт – только в результате производственной и/или исследовательской деятельности.

Подготовка специалистов в области защиты информации сопряжена с трудностями своевременного обновления знаний об угрозах и уязвимостях информационных систем. Разрешение данной проблемы возможно путем своевременной переподготовки сотрудников.

Например, США уже в 1998 г. создали Национальный центр защиты инфраструктуры (NIPC), объединивший представителей органов власти, военных и частного сектора. Наиболее известными компаниями, проводящими обучение в области информационной безопасности в США, являются: Check Point Software Technologies, Cisco Systems, IBM Tivoli Systems Global Security Laboratory, Sun Microsystems, Symantec и др. Среди учебных центров, специализирующихся на подготовке специалистов по защите информации, можно отметить CERT, GIAC, CSI, Cisco Systems.

Помимо коммерческих компаний, подготовку специалистов в области информационной безопасности осуществляет и ряд государственных структур: аспирантура NAVAL предлагает 12 различных курсов, Агентство по защите информационных систем (Defense Information Systems Agency, DISA) – 8 курсов, Колледж управления информационными ресурсами (Information Resource Management College) – 1 курс. Агентство национальной безопасности (NSA) сформировало ряд центров послевузовского образования и подключило к ним 14 ведущих университетов США.

Серьезное внимание в США уделяется процессу подготовки исполнителей. Так, для всех пользователей информационных систем установлен необходимый минимум базовых знаний в области информационной безопасности (знание криптографии, законов по информационной безопасности, правил работы с информацией ограниченного доступа). Без овладения этим уровнем знаний они не могут быть допущены к работе, при этом весь персонал должен проходить ежегодную переподготовку.

УДК 343.985

В.Г. Хахановский

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ УЧЕБНОЙ И НАУЧНОЙ ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

В современных условиях важное значение имеет информационное обеспечение правовой системы. Информация сегодня стала мерилом множества политических, социальных, экономических и правовых процессов. Информационная безопасность является неотъемлемой составляющей национальной безопасности государства, объектами которой выступают информационные ресурсы, каналы информационного обмена и другие элементы информационной инфраструктуры страны.

Вопросы своевременного и качественного информационного обеспечения деятельности правоохранительных органов сегодня имеют особенное значение, поэтому проблема информационной безопасности становится одним из приоритетных направлений в их роботе.

Разные аспекты проблемы информационной безопасности и защиты информации исследовали такие ученые СНГ, как В.Б. Аверьянов, О.А. Баранов, И.Л. Бачила, Ю.П. Битяк, П.Л. Боровик, А.Г. Додонов, В.Е. Козлов, А.Н. Лепёхин, М.Р. Сиротич, А.В. Соснин, Р.А. Калюжный, В.А. Копилов, А.И. Марущак, М.М. Россолов, Н.Я. Швец, С.А. Янишевский и др.

Вместе с тем важную роль в обеспечении организационной, научной и практической деятельности правоохранительных органов играют ведомственные учебные заведения и научно-исследовательские учреждения, где обрабатывается значительный объем информации закрытого, конфиденциального характера. В современных условиях подготовки закрытых специальных научных разработок, преподавания специальных учебных дисциплин актуализируется проблема защиты информации от утечки.

Стремительное развитие научно-технического прогресса повлекло за собой создание компактных и высокоэффективных технических средств, которые позволяют легко подключиться к линиям телекоммуникаций с целью получения, передачи и анализа данных. Для этого может использоваться аппаратура радиотехнической, оптико-электронной, радиотепловой, лазерной, акустической, химической, магнитометрической, сейсмической и радиационной разведок. Поэтому специалисты должны в совершенстве владеть методами комплексной защиты информации.

Методы защиты информации условно разделяют на правовые, организационные и технические.

Так, правовую основу обеспечения защиты информации в Украине составляют: Конституция Украины, Концепция национальной безопасности Украины, законы Украины «Об информации», «О защите информации в информационно-телекоммуникационных системах», «О телекоммуникациях», «О государственной тайне», другие нормативно-правовые акты, а также международные соглашения в сфере информационных отношений.

Комплексный характер законодательства в сфере обеспечения информационной безопасности определяет особенную актуальность проблемы консолидации законодательства, приведения к единой нормативно-правовой базе отдельных положений, зафиксированных в разных ведомственных, отраслевых и других нормативных актах, обеспечение единства в решении проблем регулирования отношений в сфере информационной безопасности.

К организационным методам защиты информации можно отнести: определение данных с ограниченным доступом, подлежащих защите; обоснование необходимости разработки и реализации защитных мероприятий; установление перечня помещений, в которых не допускается реализация угроз и утечка секретной информации; тщательный отбор и подготовка кадров; создание подразделений защиты информации, разработка современных средств защиты информации и др.

К техническим методам защиты информации можно отнести: блокировку электроакустических преобразователей и линий связи, которые выходят за пределы выделенных помещений; блокировку каналов утечки конфиденциальной информации; резервирование особо важных компьютерных подсистем; оборудование помещений замками, установку сигнализации и т. п.

Технической защите подлежит информация с ограниченным доступом, носителями которой являются поля и сигналы, образующиеся в результате работы технических средств передачи, обработки, хранения, отображения информации, а также вспомогательных технических средств и систем.

В зависимости от физической природы возникновения информационных сигналов, среды их распространения и средств перехвата, технические каналы утечки информации можно разделить на электромагнитные, электрические и параметрические.

К электромагнитным каналам утечки информации относят те, которые образуются за счет паразитного электромагнитного излучения: элементов технических средств – носителем информации тут является электрический ток, параметры которого изменяются по законам ин-

формационного сигнала; высокочастотных генераторов – генераторы тактовой частоты, генераторы подмагничивания и стирания магнитофонов, гетеродина радиоприемников и телевизионного оборудования, генераторы контрольно-измерительных приборов; на частотах работы самовозбуждения усилителей низкой частоты технических средств.

Причинами возникновения электрических каналов утечки информации могут быть наводки электромагнитного излучения на соединительных линиях и проводниках, переход сигналов к линиям энергообеспечения и заземления.

Параметрический канал утечки информации образуется в результате воздействия внешнего высокочастотного излучения. При взаимодействии элементов технических средств связи образуется вторичное излучение, модулированное информационным сигналом.

Перехват информационных сигналов этими каналами возможен путем прямого подключения к соединительным линиям или к системам питания и заземления с помощью средств радиотехнической разведки и измерительной аппаратуры.

В последнее время все чаще применяются специализированные закладные устройства, вмонтированные в технические средства (так называемые аппаратные закладки). Полученная таким способом информация передается по радиоканалу или сначала записывается на специальное запоминающее устройство, а затем по команде передается на объект.

Перехват информации по электрическому или индукционному каналу из кабельных линий предполагает подключение аппаратуры разведки к кабелям линий связи как непосредственно, так и бесконтактно (так называемые телефонные закладки). Высокочастотные электромагнитные колебания радиопередатчиков, модулированные информативным сигналом, могут быть перехвачены портативными средствами радиоразведки.

Информационная безопасность в учебных заведениях и научных учреждениях МВД должна быть обеспечена в соответствии с общегосударственными и ведомственными нормативно-правовыми актами.

Использование технических средств обработки информации и средств связи иностранного производства (при отсутствии отечественных конкурентоспособных информационных технологий, обеспечивающих защиту информации) дает возможность удаленного доступа к аппаратным и программным средствам, создает условия для несанкционированного воздействия на их функционирование и контроля за организацией связи и содержанием пересылаемых сообщений.

Безусловно, важны и актуальны вопросы информационной безопасности. Эффективность функционирования таких конфиденциальных

информационных систем, как материалы оперативной разработки, агентурные сообщения, доверенные лица и другие при их освещении в учебном курсе должны сочетаться с взвешенным и конструктивным подходом. Поэтому организационно-технический комплекс обеспечения информационной безопасности в учебных заведениях и научных учреждениях системы МВД должен отвечать требованиям защиты служебных помещений от несанкционированного снятия информации согласно концепции технической защиты информации.

Итак, организационно-технический комплекс защиты информации в учебных заведениях и научных учреждениях должен быть обеспечен: специальным подразделением, ответственным за защиту служебной информации; оснащением учебных аудиторий, служебных помещений, лекционных залов техническими средствами обнаружения радиозакладных устройств; оснащением учебных аудиторий и служебных помещений системами защиты информации от несанкционированного снятия.

СВЕДЕНИЯ ОБ АВТОРАХ

АЛЕФИРЕНКО Виктор Михайлович – доцент кафедры проектирования информационно-компьютерных систем Белорусского государственного университета информатики и радиоэлектроники, кандидат технических наук, доцент.

БАБКИН Александр Николаевич – начальник кафедры информационной безопасности Воронежского института МВД России, кандидат технических наук, доцент.

БАБКИН Алексей Александрович – начальник кафедры информатики и математики Вологодского института права и экономики ФСИН России, кандидат педагогических наук, доцент.

БАРАНОВА Алла Саввична – доцент кафедры педагогики Минского государственного лингвистического университета, кандидат педагогических наук, доцент.

БАРАНОВСКИЙ Олег Константинович – заместитель начальника центра испытаний по науке НИИ технической защиты информации, кандидат физико-математических наук.

БАРКОВ Александр Валерьевич – ассистент кафедры технологий программирования Полоцкого государственного университета.

БАЧИЛО Иллария Лаврентьевна – заведующая сектором информационного права Института государства и права РАН, доктор юридических наук, профессор , заслуженный юрист Российской Федерации.

БЕЗНОСЮК Роман Владимирович – старший преподаватель кафедры математики и информационных технологий управления Академии права и управления ФСИН России, кандидат технических наук.

БЕКБАЕВА Мадина Самиголлаевна – доцент кафедры Академии Комитета национальной безопасности Республики Казахстан, кандидат юридических наук.

БЕЛОУСОВА Елена Сергеевна – ассистентка кафедры защиты информации Белорусского государственного университета информатики и радиоэлектроники, магистр технических наук.

БЕЛЮЖЕНКО Екатерина Витальевна – преподаватель кафедры высшей математики и физики Военной академии Республики Беларусь, магистр технических наук.

БЕНЕДИКТОВИЧ Игорь Викторович – аспирант Белорусского государственного университета информатики и радиоэлектроники.

БОБОВИЧ Николай Михайлович – доцент кафедры правовой информатики Академии МВД Республики Беларусь, кандидат технических наук, доцент.

БОЙПРАВ Ольга Владимировна – аспирантка кафедры защиты информации Белорусского государственного университета информатики и радиоэлектроники.

БОНДУРОВСКИЙ Владимир Владимирович – начальник информационно-аналитического управления ОДКБ Секретариата Совета МПА СНГ – заместитель Ответственного секретаря Парламентской ассамблеи ОДКБ, член Координационного совета Международного союза юристов, кандидат юридических наук, доцент.

БОРБОТЬКО Тимофей Валентинович – профессор кафедры защиты информации Белорусского государственного университета информатики и радиоэлектроники, доктор технических наук, профессор.

БОРЕЙКО Антон Александрович – магистрант кафедры проектирования информационно-компьютерных систем Белорусского государственного университета информатики и радиоэлектроники.

БОРОВИК Петр Леонидович – старший преподаватель кафедры правовой информатики Академии МВД Республики Беларусь, кандидат юридических наук.

БОТАХАНОВ Жасулан Болатович – заместитель начальника кафедры Академии Комитета национальной безопасности Республики Казахстан, кандидат юридических наук.

БУЛГАКОВА Елена Валерьевна – доцент кафедры информационного права, информатики и математики Российской правовой академии Министерства юстиции Российской Федерации, кандидат юридических наук, доцент.

БУРАЧЕНОК Ирина Брониславовна – старший преподаватель кафедры технологий программирования, аспирантка кафедры электронной техники и энергетики Полоцкого государственного университета.

ВАЛАХАНОВИЧ Екатерина Валентиновна – преподаватель кафедры высшей математики и физики Военной академии Республики Беларусь, магистр технических наук.

ВИДОВ Станислав Владимирович – доцент кафедры математики и информационных технологий управления Академии права и управления ФСИН России, кандидат педагогических наук.

ВОРОБЬЁВ Владимир Иванович – старший научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН, доктор технических наук, профессор.

ВУС Михаил Александрович – старший научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН, кандидат технических наук.

ВУСС Георгий Васильевич – заведующий сектором Всероссийского НИИ проблем вычислительной техники и информатизации.

ГАВРИЧЕНКО Антон Николаевич – техник-программист НИИ технической защиты информации.

ГОЛУБЕВ Алексей Геннадьевич – доцент кафедры управления и информационно-технического обеспечения деятельности УИС Самарского юридического института ФСИН России, кандидат исторических наук.

ГОРБАЧЁВ Геннадий Леонидович – старший научный сотрудник НИИ технической защиты информации.

ГУБИН Игорь Алексеевич – аспирант кафедры информатики и методики преподавания математики Воронежского государственного педагогического университета.

ДЕСНИЦКИЙ Василий Алексеевич – старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН, кандидат технических наук.

ДИДКОВСКИЙ Руслан Анатольевич – научный сотрудник НИИ Вооруженных Сил Республики Беларусь.

ДМИТРИЕВ Владимир Александрович – заместитель заведующего лаборатории проблем защиты информации Объединенного института проблем информатики НАН Беларуси, кандидат физико-математических наук.

ДОЙНИКОВА Елена Владимировна – младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН.

ДУБРОВИН Анатолий Станиславович – профессор кафедры управления и информационно-технического обеспечения факультета внебюджетного образования Воронежского института ФСИН России, доктор технических наук, доцент.

ДУШКИН Александр Викторович – начальник кафедры управления и информационно-технического обеспечения Воронежского института ФСИН России, кандидат технических наук.

ЕВНЕВИЧ Елена Людвиговна – старший научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН, кандидат физико-математических наук.

ЕЖОВА Олеся Николаевна – профессор кафедры управления и информационно-технического обеспечения деятельности УИС Самарского юридического института ФСИН России, кандидат психологических наук, доцент.

ЖАЛОВ Александр Петрович, – преподаватель кафедры правовой информатики Академии МВД Республики Беларусь.

ЖЕЛЕЗНЯК Владимир Кириллович – профессор кафедры электронной техники и энергетики Полоцкого государственного университета, доктор технических наук, профессор.

ЖУКОВА Полина Николаевна – профессор кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России, доктор физико-математических наук, доцент.

ЖУРАВЕЛЬ Вадим Васильевич – начальник отдела компьютерно-технической экспертизы лаборатории криминалистических экспертиз Государственного научно-исследовательского экспертно-криминалистического центра МВД Украины.

ЗАГУМЕННОВ Артемий Андреевич – курсант Воронежского института ФСИН России.

ЗАРУБСКИЙ Владимир Георгиевич – доцент кафедры организации охраны и конвоирования в УИС Пермского института ФСИН России, кандидат технических наук.

ИВЛИЧЕВ Павел Сергеевич – доцент кафедры экономической безопасности Рязанского филиала Московского университета МВД России, кандидат физико-математических наук.

ИВЛИЧЕВА Наталья Александровна – доцент кафедры экономической безопасности Рязанского филиала Московского университета МВД России, кандидат физико-математических наук.

КАЛИБЕРОВ Андрей Васильевич – доцент кафедры специальных дисциплин Государственного института повышения квалификации и переподготовки кадров таможенных органов Республики Беларусь.

КАМЕНЕЦКИЙ Юрий Францевич – следователь по особо важным делам отдела анализа практики предварительного расследования управления организации расследования преступлений Следственного комитета Республики Беларусь, адъюнкт научно-педагогического факультета Академии МВД, магистр экономических наук.

КАШИНСКИЙ Юлий Иосифович – директор Национального центра правовой информации Республики Беларусь, кандидат экономических наук.

КИРЬЯНОВ Александр Юрьевич – доцент кафедры математики и информационных технологий управления Академии права и управления ФСИН России, кандидат технических наук.

КЛЮЕВ Станислав Геннадьевич – старший преподаватель кафедры информационной безопасности Краснодарского университета МВД России, кандидат технических наук.

КЛЮС Вадим Валерьевич – старший преподаватель кафедры оперативно-розыскной деятельности факультета подготовки специалистов для подразделений уголовной милиции Донецкого юридического института МВД Украины, кандидат юридических наук, доцент.

КОВАЛЕВИЧ Алексей Николаевич – курсант Могилевского высшего колледжа МВД Республики Беларусь.

КОВАЛЕНКО Александр Николаевич – старший преподаватель факультета внутренних войск Военной академии Республики Беларусь.

КОМЛИКОВ Дмитрий Александрович – начальник отдела НИИ технической защиты информации, кандидат технических наук.

КОРДЕЛЮК Владимир Николаевич – научный сотрудник НИИ Вооруженных Сил Республики Беларусь.

КОТЕНКО Игорь Витальевич – заведующий лабораторией проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН, доктор технических наук, профессор.

КРАВЧЕНКО Андрей Сергеевич – преподаватель кафедры управления и информационно-технического обеспечения Воронежского института ФСИН России, кандидат технических наук.

КРУПЕНКО Светлана Евгеньевна – адъюнкт Воронежского института ФСИН России.

КРЮКОВА Эмма Петровна – ведущий научный сотрудник НИИ технической защиты информации, кандидат технических наук.

КУДИНОВ Вадим Анатольевич – начальник кафедры информационных технологий Национальной академии внутренних дел Украины, кандидат физико-математических наук, доцент.

КУЗЬМИЦКИЙ Анатолий Михайлович – преподаватель факультета внутренних войск Военной академии Республики Беларусь.

КУЛАГА Александр Григорьевич – старший преподаватель кафедры правовой информатики Академии МВД Республики Беларусь.

КУЧЕРЯВЫЙ Михаил Михайлович – руководитель Управления Федеральной службы по техническому и экспортному контролю России, кандидат политических наук.

ЛАВРЕНОВ Виктор Вячеславович – старший преподаватель кафедры правовой информатики Академии МВД Республики Беларусь.

ЛАСКЕВИЧ Александр Сергеевич – аспирант кафедры гражданского права юридического факультета Белорусского государственного университета.

ЛЕПЁХИН Александр Николаевич – начальник кафедры правовой информатики Академии МВД Республики Беларусь, кандидат юридических наук, доцент.

ЛИПНИЦКИЙ Валерий Антонович – заведующий кафедрой высшей математики и физики Военной академии Республики Беларусь, доктор технических наук, профессор.

МАКАРОВ Олег Сергеевич – профессор Института национальной безопасности Республики Беларусь, кандидат юридических наук, доцент.

МАКСИМОВИЧ Елена Павловна – ведущий научный сотрудник Объединенного института проблем информатики НАН Беларуси, кандидат физико-математических наук.

МАЛИКОВ Владимир Викторович – начальник цикла технических и специальных дисциплин Центра повышения квалификации руководящих работников и специалистов Департамента охраны МВД Республики Беларусь, кандидат технических наук, доцент.

МАТВЕЕВ Анатолий Анатольевич – начальник отдела Оперативно-аналитического центра при Президенте Республики Беларусь.

МАТЮШКОВА Галина Леонидовна – научный сотрудник Объединенного института проблем информатики НАН Беларуси.

МЕЛЬНИК Александр Филиппович – старший научный сотрудник НИИ технической защиты информации.

МИРОНЧИК Виолетта Викторовна – аспирантка кафедры защиты информации Белорусского государственного университета информатики и радиоэлектроники.

МИХАЙЛОВСКАЯ Людмила Вячеславовна – доцент кафедры высшей математики и физики Военной академии Республики Беларусь, кандидат физико-математических наук.

МОРАР Виталий Олегович – старший научный сотрудник Всероссийского НИИ МВД России, кандидат технических наук.

МОРАР Иван Олегович – юрист.

МОРОЗ Наталия Олеговна – преподаватель кафедры конституционного и административного права Академии управления при Президенте Республики Беларусь.

МЫТНИЦКИЙ Александр Андреевич – курсант Воронежского института ФСИН России.

НАСОНОВА Валентина Афанасьевна – профессор кафедры информационно-компьютерных технологий в деятельности органов внутренних дел Белгородского юридического института МВД России, кандидат физико-математических наук, доцент.

НАУМЕНКО Георгий Николаевич – заведующий сектором Объединенного института проблем информатики НАН Беларуси.

НЕСТЕРУК Филипп Геннадьевич – старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН, кандидат технических наук, доцент.

НИКИТЕНКОВ Кирилл Сергеевич – студент факультета компьютерных технологий и управления Санкт-Петербургского института информатики и автоматизации РАН.

НОВОСЕЛЬЦЕВ Виктор Иванович – профессор кафедры управления и информационно-технического обеспечения Воронежского института ФСИН России, доктор технических наук.

ОЗЁРСКИЙ Сергей Владимирович – заместитель начальника кафедры Самарского юридического института ФСИН России, кандидат физико-математических наук, доцент.

ОСИПЕНКО Анатолий Леонидович – заместитель начальника Воронежского института МВД России по научной работе, доктор юридических наук, доцент.

ПЕРЕВАЛОВ Дмитрий Васильевич – доцент кафедры оперативно-розыскной деятельности и правового обеспечения органов пограничной службы Института пограничной службы Республики Беларусь, кандидат юридических наук, доцент.

ПЕРЕКОПСКИЙ Геннадий Иванович – заместитель начальника информационно-аналитического управления ОДКБ Секретариата МПА СНГ, кандидат педагогических наук.

ПОЗНАНСКИЙ Юрий Николаевич – старший преподаватель кафедры управления органами расследования преступлений Академии управления МВД России.

ПОЛЯКОВ Александр Сергеевич – ведущий научный сотрудник Объединенного института проблем информатики НАН Беларуси, кандидат технических наук, доцент.

ПОНОМАРЁВ Максим Валерьевич – курсант Воронежского института ФСИН России.

ПОПОВ Игорь Вадимович – доцент кафедры управления и информационно-технического обеспечения деятельности УИС Самарского юридического института ФСИН России, кандидат педагогических наук.

ПУЗЫНА Сергей Викторович – магистрант Белорусского государственного университета информатики и радиоэлектроники.

ПУП Александр Александрович – аспирант кафедры гражданско-правовых дисциплин Белорусского государственного экономического университета.

РАБЦЕВИЧ Роман Владимирович – магистрант Белорусского государственного университета информатики и радиоэлектроники.

РАХАНОВ Константин Яковлевич – старший преподаватель кафедры технологий программирования Полоцкого государственного университета, кандидат технических наук.

РУДАКОВ Артур Михайлович – научный сотрудник научно-исследовательской лаборатории организационно-научного отдела, адъюнкт кафедры уголовно-исполнительного права и организации воспитательной работы с осужденными Вологодского института права и экономики ФСИН России.

РУЧКИН Владимир Николаевич – профессор кафедры информатики и вычислительной техники Рязанского государственного университета имени С.А. Есенина, доктор технических наук, профессор.

РУЧКИН Григорий Владимирович – магистрант Рязанского государственного университета имени С.А. Есенина.

РЫБАЛЬСКИЙ Олег Владимирович – профессор кафедры информационных технологий Национальной академии внутренних дел Украины, доктор технических наук, профессор.

РЫЧАГО Михаил Евгеньевич – доцент кафедры специальной техники и информационных технологий Владимирского юридического института ФСИН России, кандидат физико-математических наук, доцент.

РЯБЕНКО Денис Сергеевич – аспирант кафедры электронной техники и энергетики Полоцкого государственного университета.

САЕНКО Игорь Борисович – ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН, доктор технических наук, профессор.

САМСОНОВ Виктор Евстратьевич – старший научный сотрудник Объединенного института проблем информатики НАН Беларуси.

САХАРОВ Сергей Леонидович – доцент кафедры управления и информационно-технического обеспечения Воронежского института ФСИН России, кандидат технических наук.

СЕНАТОРОВА Наталья Борисовна – старший преподаватель кафедры Самарского юридического института ФСИН России.

СИДЕЛЬНИКОВ Павел Алексеевич – начальник инженерно-технического факультета Воронежского института ФСИН России, кандидат педагогических наук.

СКОРОБОГАТОВА Дарья Евгеньевна – адъюнкт Воронежского института ФСИН России.

СМАКОВ Евгений Юрьевич – преподаватель кафедры управления и информационно-технического обеспечения Воронежского института ФСИН России, доктор технических наук.

СМИРНОВ Александр Александрович – ведущий научный сотрудник Всероссийского НИИ МВД России, кандидат юридических наук, доцент.

СОЛОВЬЁВ Виктор Иванович – доцент кафедры компьютерных систем и сетей Восточноукраинского национального университета имени В. Даля, кандидат технических наук, доцент.

СТЕПАНЯН Арарат Баркевович – ведущий научный сотрудник Объединенного института проблем информатики НАН Беларуси, кандидат технических наук.

СТЕЦЮК Сергей Юрьевич – главный специалист Оперативно-аналитического центра при Президенте Республики Беларусь.

СУЛТАНОВ Аскар Ануарбекович – начальник научно-исследовательского управления Академии Комитета национальной безопасности Республики Казахстан, кандидат юридических наук.

СУМИН Виктор Иванович – профессор кафедры управления и информационно-технического обеспечения Воронежского института ФСИН России, доктор технических наук, профессор.

СУРИН Владимир Владимирович – начальник кафедры уголовного процесса и криминалистики Пермского института ФСИН России, кандидат юридических наук.

СУШКО Александр Евгеньевич – начальник управления по расследованию преступлений против информационной безопасности и интеллектуальной собственности ГСУ Следственного комитета Республики Беларусь.

ТРАХИМОВИЧ Евгений Валерьянович – курсант факультета милиции Академии МВД Республики Беларусь.

ТРУБЕЙ Антон Иванович – научный сотрудник научно-исследовательской лаборатории проблем защиты информации Объединенного института проблем информатики НАН Беларуси.

ТУКАЛО Алексей Николаевич – заместитель начальника кафедры оперативно-розыскной деятельности Академии МВД Республики Беларусь, кандидат юридических наук, доцент.

УТИН Леонид Львович – начальник научно-исследовательского отдела НИИ Вооруженных Сил Республики Беларусь, кандидат технических наук, доцент.

ФАДЕЕВ Антон Геннадьевич – курсант Воронежского института ФСИН России.

ФАТКИЕВА Роза Равильевна – старший научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН, кандидат технических наук.

ФЕДОРЧЕНКО Андрей Владимирович – младший научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН.

ФИСЕНКО Владимир Карпович – ведущий научный сотрудник лаборатории проблем защиты информации Объединенного института проблем информатики НАН Беларуси, кандидат технических наук, доцент.

ФОМИН Василий Васильевич – доцент Академии права и управления ФСИН России, кандидат юридических наук.

ХАБИБУЛИНА Светлана Юрьевна – заместитель декана факультета внебюджетного образования Воронежского института ФСИН России, кандидат экономических наук.

ХАХАНОВСКИЙ Валерий Георгиевич – профессор кафедры информационных технологий Национальной академии внутренних дел Украины, доктор юридических наук, профессор.

ХОРОШЕВА Анна Владимировна – доцент кафедры специальной техники и информационных технологий Владимирского юридического института ФСИН России, кандидат физико-математических наук.

ЦВЕТКОВ Владимир Владимирович – адъюнкт кафедры управления и информационно-технического обеспечения Воронежского института ФСИН России.

ЧЕЧУЛИН Андрей Алексеевич – старший научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН, кандидат технических наук.

ЧУДИЛОВСКАЯ Татьяна Геннадьевна – старший преподаватель кафедры правовой информатики Академии МВД Республики Беларусь.

ЧУМАК Владимир Валентинович – старший преподаватель кафедры административной деятельности органов внутренних дел факультета по подготовке специалистов для подразделений милиции общественной безопасности и криминальной милиции по делам детей Харьковского национального университета внутренних дел, кандидат юридических наук.

ЧУМАКОВА Анна Сергеевна – курсантка факультета милиции Академии МВД Республики Беларусь.

ЧУРЮКАНОВ Степан Александрович – аспирант Белорусского государственного университета информатики и радиоэлектроники.

ШАБАНОВ Вячеслав Борисович – заместитель начальника Академии МВД Республики Беларусь по научной работе, доктор юридических наук, профессор.

ШВЕД Надежда Александровна – главный специалист НПЦ Генеральной прокуратуры Республики Беларусь, кандидат юридических наук.

ШЕБЕЦ Оксана Романовна – старший преподаватель кафедры управления и информационно-технического обеспечения деятельности УИС Самарского юридического института ФСИН России.

ШИШКИН Владимир Михайлович – старший научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН, кандидат технических наук, доцент.

ШЛЫКОВ Сергей Александрович – преподаватель кафедры информатики и математики Вологодского института права и экономики ФСИН России.

ШУГАЙ Андрей Александрович – аспирант кафедры гражданско-правовых дисциплин Белорусского государственного экономического университета, магистр юридических наук.

ЩЁКИН Виктор Александрович – курсант Воронежского института ФСИН России.

ЩЕРБАКОВА Юлия Владимировна – адъюнкт кафедры управления и информационно-технического обеспечения Воронежского института ФСИН России.

ЭСАУЛЕНКО Александр Владимирович – начальник Управления вневедомственной охраны ГУ МВД России по Краснодарскому краю.

ЯКЖИК Дмитрий Сергеевич – начальник отдела управления по защите государственных секретов МВД Республики Беларусь.

ЯХНОВИЧ Олег Игоревич – преподаватель кафедры источниковедения Белорусского государственного университета.

СОДЕРЖАНИЕ

РАЗДЕЛ 3
СОВРЕМЕННЫЕ ПРОБЛЕМЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАЗДЕЛ 4
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

РАЗДЕЛ 5
АКТУАЛЬНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
В ДЕЯТЕЛЬНОСТИ УЧРЕЖДЕНИЙ
УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ

РАЗДЕЛ 6
ПОДГОТОВКА СПЕЦИАЛИСТОВ
В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ

Научное издание

**ТЕОРЕТИЧЕСКИЕ
И ПРИКЛАДНЫЕ АСПЕКТЫ
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ**

Материалы
Международной
научно-практической конференции
(Минск, 19 июня 2014 г.)

Редактор *С.А. Ржановская*
Компьютерная верстка *И.В. Бачилы*

Подписано в печать 09.02.2015. Формат $60\times84^{1}/_{16}$.
Бумага офсетная. Ризография. Усл. печ. л. 24,41. Уч.-изд. л. 22,14.
Тираж 100 экз. Заказ 37.

Издатель и полиграфическое исполнение:
учреждение образования
«Академия Министерства внутренних дел Республики Беларусь».
Свидетельство о ГРИИРПИ № 1/102 от 02.12.2013.
ЛП № 02330/447 от 18.12.2013.
Пр-т Машерова, 6, 220005, Минск.

ДЛЯ ЗАМЕТОК