ИНФОРМАТИЗАЦИЯ
И СВЯЗЬ
Издается с 1998 г.

ISSN 2078-8320

Журнал зарегистрирован в Министерстве РФ по делам печати, телерадиовещания и средств массовых коммуникаций

Регистрационный номер
ПИ № 77-16535

Издатель
Автономная некоммерческая организация «Редакция журнала «Информатизация и связь»

Научный редактор выпуска
М.А.Вус

Адрес редакции
105005, г. Москва,
ул. Бакунинская, д. 15

Телефон: (495) 952-18-52
e-mail: infsvz@gmail.com
www.infsv.ru

Подписка на журнал
производится в почтовых отделениях связи по Объединенному каталогу «Пресса России» том 1

Подписной индекс 83828

СОДЕРЖАНИЕ
3'2014

В.В. Бондуровский, И.Л. Бачило, М.А. Вус, М.М. Кучерявый, О.С. Макаров
ПАРЛАМЕНТСКОЕ ИЗМЕРЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ СНГ И ОДКБ НА СОВРЕМЕННОМ ЭТАПЕ 8

И.Л. Бачило, М.А. Вус, О.С. Макаров
ОБ ИЗМЕНЕНИЯХ МОДЕЛЬНОГО ЗАКОНА СНГ «ОБ ИНФОРМАТИЗАЦИИ, ИНФОРМАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ» (2005 г.) В ЕГО НОВОЙ РЕДАКЦИИ С ИЗМЕНЁННЫМ НАЗВАНИЕМ «ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» 14

Д.В. Перевалов
ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ ФОРМИРОВАНИЯ СИСТЕМЫ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ 17

А.Н. Лепёхин
О НЕКОТОРЫХ АСПЕКТАХ РАЗРАБОТКИ И РЕАЛИЗАЦИИ АДМИНИСТРАТИВНЫХ РЕГЛАМЕНТОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 27

М.М. Кучерявый, И.И. Лившиц
ПОДХОДЫ К ОЦЕНКЕ УЯЗВИМОСТЕЙ И УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ НА ПРИМЕРЕ НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЫ 30

М.В. Буйневич, О.А. Тиамийу
ПРОГРАММНАЯ АРХИТЕКТУРА СИСТЕМЫ УПРАВЛЕНИЯ ДОВЕРЕННОЙ МАРШРУТИЗАЦИЕЙ В ГЛОБАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ 35

К.Е. Израилов
МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ СРЕДСТВ АЛГОРИТМИЗАЦИИ, ИСПОЛЬЗУЕМЫХ ДЛЯ ПОИСКА УЯЗВИМОСТЕЙ 39

М.В. Харинов, В.П. Заболотский
КРИТИЧЕСКАЯ ТЕХНОЛОГИЯ КВАЗИОПТИМАЛЬНОГО МАШИННОГО ЗРЕНИЯ 43

Д.С. Черешкин
ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В НОВЫХ УСЛОВИЯХ 47

Внимание авторов!

Журнал входит в «Перечень российских рецензируемых научных журналов, в которых должны быть опубликованы основные научные результаты диссертации на соискание ученых степеней доктора и кандидата наук»

Все публикации в журнале, в том числе аспирантов, осуществляются бесплатно

Перепечатка материалов допускается только с письменного разрешения редакции

Журнал отпечатан в ООО «ОМП группа»

Адрес: 125040, Москва, ул. Нижняя, д.14, стр.1

Подписано в печать 23.09.14.
Тираж 250 экз. Усл. печ. 5.25.
Заказ № 1284.

© Журнал "Информатизация и связь", 2014

© АНО "Редакция журнала Информатизация и связь", 2014

О.С. Макаров, М.А. Вус, Д.В. Перевалов
К ВОПРОСУ РАЗРАБОТКИ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 55

ПРОЕКТ МОДЕЛЬНОГО ЗАКОНА СНГ «ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» 65

АННОТАЦИИ 76

SUMMARY 78

ИНФОРМАЦИЯ ОБ АВТОРАХ 80

КНИЖНАЯ ПОЛКА 82

САНКТ-ПЕТЕРБУРГСКАЯ КОНФЕРЕНИЦИЯ «РЕГИОНАЛЬНАЯ ИНФОРМАТИКА (РИ–2014)» 84

РЕДАКЦИОННЫЙ СОВЕТ

Председатель Редакционного Совета

ГУЛЯЕВ Ю.В. – академик РАН, член Президиума РАН, директор ФГБУН «Института радиотехники и электроники им. В.А. Котельникова» РАН.

Первый заместитель Председателя Редакционного Совета

СТАРОВОЙТОВ А.В. – доктор технических наук, профессор, Президент Федерального государственного автономного научного учреждения «Центр информационных технологий и систем органов исполнительной власти».

Заместители Председателя Редакционного Совета

ГОЛУБЕВ Ю.Н. – кандидат технических наук, вице-президент ОО Московское отделение «Качество информационных технологий в системах управления» Академии проблем качества.

СКВОРЧЕВСКИЙ А.К. –доктор технических наук, профессор, заведующий лабораторией ФГБУН Института машиноведения им. А.А. Благонравова РАН.

Члены Редакционного Совета

АБРАМОВ С.М. – доктор физико-математических наук, член-корреспондент РАН, директор ФГБУН Института программных систем им. А.К. Айламазяна РАН.

АНИСЬКИНА Н.Н. – кандидат технических наук, доцент, ректор ГБОУ ДПО «Государственная академия промышленного менеджмента им. Н.П. Пастухова».

БАЧИЛО И.Л. – доктор юридических наук, профессор, заведующая сектором информационного права Института государства и права РАН.

ВАСИЛЬКОВ Ю.В. – доктор технических наук, профессоркафедры интегрированных систем менеджмента ГБОУ ДПО «Государственная академия промышленного менеджмента им. Н.П. Пастухова».

ВОРОНЦОВА Л.В. – доктор юридических наук, профессор ФГКОУ ВПО «Академия Федеральной службы безопасности РФ».

ВУС М.А. – кандидат технических наук, старший научный сотрудник ФБУН Санкт-Петербургский институт информатики и автоматизации РАН.

ДУБИНСКИЙ Ю.М. – доктор технических наук, кандидат юридических наук, профессор, заместитель генерального директора по информационным технологиям УК «Авеню менеджмент».

ЖИЖЧЕНКО А.Б. – академик РАН, заместительАкадемика секретаря Отделения математических наук РАН.

ЗАЙЦЕВСКИЙ И.В. – доктор экономических наук, профессор, генеральный директор АНОО Центральный Российский Домзнаний Общества «Знание» России.

КОСТОГРЫЗОВ А.И. – доктор технических наук, профессор, директор-научный руководитель «Научно-исследовательский института прикладной математики и сертификации», профессор МГТУ МИРЭА и РГУ нефти и газа им. И.М.Губкина.

КУЧЕРЯВЫЙ М.М. – кандидат политических наук, доцент, руководитель Управления Федеральной службы по техническому и экспортному контролю по Северо-Западному федеральному округу.

ЛЫСЕНКО Э.А. – директор Департамента информатизации и связи Ярославской области.

МАХУТОВ Н.А. – доктор технических наук, профессор, член-корреспондент РАН, главный научный сотрудник ФГБУН Институт машиноведения им. А.А. Благонравова РАН.

ЛИХТЕНШТЕЙН В.Е. – доктор экономических наук, профессор, ведущий научный сотрудник научно-методического совета ФГУП «Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации».

ОЛЕЙНИКОВ А.Я. – доктор технических наук, профессор, главный научный сотрудник ФГБУН «Института радиотехники и электроники им. В.А. Котельникова» РАН.

ПРОТАСОВ А.А. – доктор военных наук, начальник 27 Центрального научно-исследовательского института Министерства обороны РФ, профессор Академии военных наук.

РОГОЗОВ Ю.И. – доктор технических наук, профессор, заведующий кафедрой системного анализа и телекоммуникаций Южного федерального университета.

РОСС Г.В. – доктор технических наук, доктор экономических наук, профессор, заместитель директора ФГУП «Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации» по учебно-методической работе.

РУСАКОВ А.В. – доктор химических наук, профессор, ректор Ярославского государственного университета им. П.Г. Демидова.

СВЕТИК Ф.Ф. –профессор, Председатель Правления Международного гуманитарного общественного фонда «Знание» им. академика К.В. Фролова.

СТРЕЛЬЦОВ А.А.–доктор технических наук, доктор юридических наук, профессор, главный научный сотрудник Института проблем информационной безопасности МГУ им. М.В. Ломоносова.

ТАРАСОВ Б.В. – доктор технических наук, профессор, генеральный директор Научно-производственного центра «Модуль».

ЦАРЕВ А.П. – кандидат технических наук, Президент ОО Московское отделение «Качество информационных технологий в системах управления» Академии проблем качества.

ШЕРСТЮК В.П. – кандидат физико-математических наук, член-корреспондент Академии криптографии РФ, директор Института проблем информационной безопасности МГУ им. М.В. Ломоносова.

ЮСУПОВ Р.М. – доктор технических наук, профессор, член-корреспондент РАН, директор ФБУН Санкт-Петербургский институт информатики и автоматизации РАН.

Ответственный секретарь

ДЕРГАЧЕВА Е.В. – директор АНО «Редакция журнала «Информатизация и связь».

EDITORIAL BOARD

Chairman of the Editorial Board

GULYAEV Yu.V. – Academician of RAS, member of the Presidium of RAS, Director of Kotelnikov's Institute of Radio Engineering and Electronics of RAS.

First Deputy Chairmans of the Editorial Board

STAROVOYTOV A.V.,Doctor of Technical Sciences, Professor, Director of Federal State Research Institution "Centre of Information Technologies and Systems for Executive Power Authorities" (CIT&S).

Deputy Chairmans of the Editorial Board

GOLUBEV Yu.N.– Candidate of Technical Sciences, vice president of the Moscow branch "Quality of information technologies in control systems" of the Quality ProblemsAcademy.

SKVORCHEVSKY A.K. –Doctor of technical Sciences, Professor, Head of a Laboratory of Blagonravov Research Institute for Machine Science of RAS.

Members of the Editorial Board

ABRAMOV S.M. – Doctor of Physical and Mathematical Sciences, Corresponding Member of RAS, Director of Program Systems Institute of RAS.

ANISKINA N.N. – Candidate of Technical Sciences, Associate Professor, Rector of Pastukhov State Academy of Industrial Management.

BACHILO I.L. – Doctor of Juridical Sciences, professor, Head of the Information Law Department at the Institute for State and Law of RAS.

VASILKOV Yu.V. – Doctor of Technical Sciences, Professor of Integrated Management Systems Department of Pastukhov State Academy of Industrial Management.

VORONTSOVA L.V. – Doctor of Juridical Sciences, Professor of Academy of the Federal Security Service of Russia.

VYS M.A. – Candidate of Technical Sciences, senior researcher of Applied Informatics Laboratory of the St. Petersburg Institute for Informatics and Automation of RAS.

DOUBINSKY Yu.M. – Doctor of Technical Sciences, Candidate of Juridical Sciences, Professor, Information Technology Deputy Director of "Avenue Management".

ZHIZHCHENKO A.B. – Academician of RAS, Deputy Academician Secretary of the Mathematical Sciences Department of RAS.

ZAYTSEVSKY I.V. – Doctor of Economic Sciences, Professor, General Director of Russian Central House of Knowledge of Russian Society "Knowledge".

KOSTOGRYZOV A.I. – Doctor of Technical Sciences, professor, director-supervisor of Scientific Research Institute of Applied Mathematics and certification.

KUCHERYAVY M.M.–Doctor of Political Sciences, Associate Professor, Head of the Federal Service for Technical and Export Control in the North-West Federal District.

LYSENKO E.A. – Director of Information and Communication Department of the Yaroslavl region.

LIECHTENSTEIN V.E. – Doctor of Economical Sciences, professor, Chief Researcher of the All-Russian Research Institute of Computer Science and Informatization.

MAHUTOV N.A. – Corresponding Member of RAS, Chief Researcher of Blagonravov Research Institute for Machine Science of RAS.

OLEINIKOV A.Y. – Doctor of Technical Sciences, Professor, Chief Researcher of the Kotelnikov's Institute of Radio Engineering and Electronics of RAS.

PROTASOV A.A. – Doctor of Military Sciences, head of 27-th Central Research Institute of the Ministry of Defense of the Russian Federation, professor of the Military Sciences Academy.

ROGOZOV YU.I. – Doctor of Technical Sciences, Professor, Head of the System Analysis and Telecommunications Department of the Southern Federal University.

ROSS G.V. – Doctor of Technical Sciences, Doctor of Economical Sciences, professor, Deputy Director of the All-Russian Research Institute of Computer Science and Information Technology.

RUSAKOV A.V. – Doctor of Chemistry Sciences, Professor, Rector of Demidov Yaroslavl State University.

SVETIK F.F. – Professor, Chairman of the Frolov International Humanitarian Public Fund "Knowledge".

STRELTSOV A.A. – Doctor of Technical Sciences, Doctor of Juridical Sciences, Professor, Senior Researcher of Information Security Problems Institute of the Lomonosov Moscow State University.

TARASOV B.V. – Doctor of Technical Sciences, Professor, Director General of Research and Production Center "Module".

TSAREV A.P. – Doctor of Technical Sciences, President of the Moscow branch "Quality of information technologies in control systems" of the Quality Problems Academy.

SHERSTYUK V.P. – Candidate of Physical and Mathematical Sciences, Corresponding Member of the Russian Academy of Cryptography, Director of Information Security Problems Institute of the LomonosovMoscow State University.

YUSUPOV R.M. –Doctor of Technical Sciences, Corresponding Member of RAS, Director of St Petersburg Institute for Informatics and Automation of RAS.

Executive secretary

DERGACHEVA E.V. – Director of the Editorial board" Informatization and Communication".

ВЫСОКИЕ МЕЖПАРЛАМЕНТСКИЕ НАГРАДЫ САНКТ-ПЕТЕРБУРГСКИМ УЧЁНЫМ

Постановлением Совета Межпарламентской Ассамблеи Содружества Независимых Государств (МПА СНГ) в ноябре 2013 г. орденом «Содружество» за активное участие в деятельности Межпарламентской Ассамблеи и её органов, вклад в укрепление дружбы между народами государств – участников Содружества Независимых Государств был награжден директор Санкт-Петербургского института информатики и автоматизации РАН (СПИИРАН) член-корреспондент РАН Юсупов Рафаэль Мидхатович. В апреле текущего года этим же орденом награжден старший научный сотрудник того же академического института, кандидат технических наук Вус Михаил Александрович.

Межпарламентский орден «Содружество» — высшая награда МПА СНГ, присуждаемая за заслуги перед народами в различных областях деятельности. К награждению этим орденом представляются не более двух кандидатур от государства в течение года. Среди награждённых в разные годы орденом «Содружество» видные государственные и общественные деятели, политики, учёные, деятели науки, культуры и искусства. В числе известных учёных, удостоенных ордена «Содружество», академик Национальной Академии наук Беларуси Войтович А.П. (2002) и академик Российской Академии наук Кокошин А.А. (2007); директор Центра Евро-Атлантической Безопасности МГИМО профессор Никитин А.И. (2009); академик Национальной Академии наук Казахстана Сагадиев К.А. (2010) и другие.

МПА СНГ является межгосударственным органом сотрудничества законодательных органов государств Содружества. Важнейшим направлением её деятельности является правотворческий процесс.

Учёные СПИИРАН в качестве экспертов принимают участие в работе различных экспертных групп и комиссий. С их участием разрабатывались проекты ещё первых, принятых МПА СНГ на рубеже веков модельных законодательных актов в области информатизации, оказавшие определённое влияние на становление и развитие национальных законодательств.

Когда десятилетие назад впервые высветилась во всём своём многообразии проблема международной информационной безопасности, возникла необходимость системного и адекватного парирования вызовов и угроз в стремительно развивающейся информационной сфере. Сформированный СПИИРАН интернациональный коллектив российских и белорусских учёных предпринял попытку подготовки проекта Рекомендаций по совершенствованию и гармонизации национального законодательства для государств – участников СНГ в сфере обеспечения информационной безопасности. Проект этого концептуального по своему характеру документа в 2010-2012 гг. публиковался для широкого обсуждения на страницах ряда научных изданий, что в конечном итоге предопределило успешное завершение работы над ним. Одновременно разработчиками был подготовлен и выпущен в свет Словарь-справочник понятийного аппарата модельного законодательства МПА СНГ (2012), отмеченный профессиональной премией Национального Инфофорума по информационной безопасности.

Рекомендации по совершенствованию и гармонизации национального законодательства для государств – участников СНГ в сфере обеспечения информационной безопасности были приняты на пленарном заседании МПА СНГ в 2012 г. На их основе определен комплекс законодательных инициатив в проектах межгосударственных программ сотрудничества государств-участников СНГ в сфере безопасности на период 2014–2018 гг., которые в 2013 г. утвердил Совет глав государств СНГ.

Владимир Бондуровский
начальник информационно-аналитического управления ОДКБ —
заместитель Ответственного секретаря Парламентской Ассамблеи ОДКБ

80-ЛЕТИЕ
члена-корреспондента РАН
Рафаэля Мидхатовича ЮСУПОВА

80 летний юбилей отметил член редакционного совета журнала, член-корреспондент Российской академии наук, Заслуженный деятель науки и техники Российской Федерации Рафаэль Мидхатович ЮСУПОВ.

Выпускник Казанской спецшколы ВВС с отличием окончил Военно-космическую академию имени А.Ф. Можайского и Ленинградский государственный университет, прошел путь от инженера до генерала, более четверти века возглавляет Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН).

Доктор технических наук, профессор Р.М. Юсупов является организатором, руководителем и участником крупнейших фундаментальных и прикладных исследований в области кибернетики и информатики, результаты которых явились важным вкладом в отечественную и мировую науку, образование и экономику страны, ее безопасность и развитие международных научных связей. Он является одним из основоположников отечественной научной школы по теории чувствительности.

Р.М. Юсупов — действительный член Академии военных наук России, являясь членом Научного совета при Совете Безопасности Российской Федерации, он лично принимал участие в разработке целого ряда проектов государственных документов по обеспечению информационной безопасности.

Благодаря усилиям Р.М. Юсупова, руководимый им институт стал научно-методическим центром информатизации Санкт-Петербурга. СПИИРАН является сегодня одним из немногих научных учреждений страны, в перечне основных направлений исследований которого фундаментальные основы информатизации общества и информационной безопасности.

Р.М. Юсупов награжден орденом «За заслуги перед Отечеством» IV степени, орденом «Почета», орденом «Красная звезда», медалями.

За научные достижения и педагогические заслуги Р.М. Юсупов удостоен премий Правительства России и Правительства Санкт-Петербурга в области образования, премии им. А.С. Попова Правительства Санкт-Петербурга в области электро- и радиотехники и информационных технологий (2009) и ряда других наград. Ему присуждена Международная премия им. Н. Рериха за достижения в области педагогики и просветительства (2005).

В 2013 г. за работы в области обеспечения международной информационной безопасности директор СПИИРАН член-корреспондент РАН Р.М. Юсупов награжден высшей наградой Межпарламентской ассамблеи государств-участников Содружества независимых государств — орденом «Содружество».

Редакционный совет журнала «Информатизация и связь» поздравляет своего коллегу-юбиляра и желает ему здоровья и дальнейших творческих успехов!

«Сегодня школа и институт – это место столкновения двух поколений: одно – носитель уже уходящего в прошлое понятийного мышления, для которого характерна логика; логос имеет здесь фундаментальное значение, - и клиповое сознание. В одном случае книжная культура, в другом – экранная. Чем хорошо клиповое сознание? Радостью при встрече с пустотой, фрагментами, перепрыгиванием с фрагмента на фрагмент, игрой, креативностью. И сегодня, когда преподаватели говорят студентам прочесть большой текст, а они не могут, потому что устают, скучают, засыпают, у них не хватает внимания – им это не надо! Нужно уметь коротко формулировать мысль. У тебя есть три минуты экранного времени, и за эти три минуты нужно сказать всё! Что значит мыслить? Это значит быстро мыслить! Нужен ПЕРЕСКОК! Потому что время сейчас другое».

[В.В. Александров]

От «Урала – 1» к БПЛА

Своё 75-летие отметил доктор технических наук, профессор, Заслуженный деятель науки и техники Российской Федерации, лауреат премии по информатике им. Дж. Фон Неймана и лауреат премии Правительства Российской Федерации в области науки и техники Виктор Васильевич Александров.

В.В. Александров – ленинградец, житель блокадного Ленинграда, заведующий лабораторией автоматизации научных исследований Санкт-Петербургского института информатики и автоматизации и РАН. По окончании техникума первые шаги по компьютерному моделированию и распознаванию радионавигационных сигналов постигал на ЭВМ «Урал – 1». С отличием окончил Ленинградский политехнический институт. Темой кандидатской диссертацией стала задача распознавания и классификации на ферритовых ячейках с использованием матриц Адамара.

В 1974 году В.В. Александров был приглашен заведующим лабораторией автоматизации научных исследований во вновь образуемую академическую организацию — ныне СПИИРАН, где и работает по настоящее время. Докторскую диссертацию защитил в 1978 г., академик РАЕН с 1992 г.

В.В. Александров разработал цифровые методы классификации и распознавания на основе алгоритмов быстрых преобразований Аламара-Уолша. Разработал рекомендации по хранению и сжатию изображений, передаче информации с поэтапным проявлением на приёмной стороне, быстрому поиску информации по видеозапросу, поиску на изображении заданных целей и объектов. Создал систему объектно-адаптированного анализа и иерархического представления изображения сложной структуры в целях непрерывной обработки видеоданных. Разработчик развивающейся системы в проблемно-ориентированной среде. В 1993 г. В.В. Александров был удостоен премии по информатике им. Дж. Фон Неймана.

За цикл работ по операторному и/или беспилотному управлению научно-технический совет ОАО «Московский вертолетный завод им. М.Л. Миля» включил профессора В.В. Александрова в состав авторского коллектива работы «Разработка эргономически обоснованных комплексов, повышающих эффективность эксплуатации и безопасность полетов, вертолетов». Премия Правительства Российской Федерации в области науки и техники «за разработку и создание новой техники» была присуждена в 2011 году.

Редакционный совет журнала «Информатизация и связь» поздравляет юбиляра и желает ему здоровья и дальнейших творческих успехов!

УДК 004

ПАРЛАМЕНТСКОЕ ИЗМЕРЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ СНГ И ОДКБ НА СОВРЕМЕННОМ ЭТАПЕ

В.В. Бондуровский, И.Л. Бачило, М.А. Вус, М.М. Кучерявый, О.С. Макаров

Субъекты международного права. После распада СССР на ряд независимых государств на пространстве бывшего Союза образовались региональные международные организации. В их числе Содружество Независимых Государств (СНГ) и Организация Договора о коллективной безопасности (ОДКБ). Целями СНГ — межгосударственного объединения, в соответствии с Уставом этой международной организации, является развитие равноправного и взаимовыгодного сотрудничества народов и государств, содействие широкому информационному обмену.

Созданная в целях обеспечения военно-политической безопасности, ОДКБ в настоящее время объединяет шесть независимых государств: Республику Армения, Республику Беларусь, Республику Казахстан, Кыргызскую Республику, Российскую Федерацию и Республику Таджикистан. Сегодня ОДКБ превратилась в полноформатную многофункциональную региональную структуру противодействия традиционным и новым вызовам и угрозам миру, безопасности и стабильности. Диапазон таких вызовов в последнее время не только не сужается, а, напротив, расширяется. Исходя из этого, Президент Российской Федерации ***В.В. Путин*** особо подчеркнул, что «**совместно с нашими союзниками мы должны укреплять возможности Организации Договора о коллективной безопасности**».

За годы своего существования СНГ и ОДКБ стали признанными субъектами международного права. Генеральная Ассамблея ООН приняла специальную резолюцию о сотрудничестве с региональными объединениями, действующими на постсоветском пространстве. Устав СНГ и Договор о коллективной безопасности как международные соглашения зарегистрированы в соответствии со статьёй 102 Устава ООН в её Секретариате. В 2004 г. ООН предоставила ОДКБ статус наблюдателя.

Информационная безопасность. Важнейшим результатом формирования информационного общества на рубеже веков стало возникновение глобального информационного пространства, в котором развернулась острая борьба за достижение информационного превосходства. Всемирная федерация учёных еще в 2000 г. поставила первой в списке угроз человечеству в XXI веке угрозу информационной безопасности. Информационная сфера — весьма чувствительный фактор жизнедеятельности общества. Повсеместно и объективно растут техногенные факторы и связанная с этим уязвимость.

Формирование системы международной информационной безопасности определяется уровнем политического доверия между правительствами государств с учётом принципов взаимопонимания, равноправия и согласования интересов сторон. Сегодня информационная безопасность является важнейшим компонентом национальной, региональной и международной безопасности. Проблема информационной безопасности связана с категорией суверенитета и юрисдикции государств, что с необходимостью требует согласования систем организационного и правового обеспечения информационной безопасности в контексте обеспечения национальной (региональной) и международной безопасности. Интересы международного сотрудничества требуют обеспечения совместимости национальных векторов информационного развития и приоритетных направлений обеспечения информационной безопасности.

СНГ. Первыми актами Содружества Независимых Государств, относящимися к информационной сфере, явились Соглашение «О сотрудничестве в области информации» и Рекомендательный законодательный Акт «О принципах регулирования информационных отношений в государствах МПА СНГ» (1993). В Рекомендательном Акте впервые в законодательстве СНГ было использова-

но понятие «информационная безопасность», однако его конкретное содержание при этом не раскрывалось. В 1996 г. была принята Концепция формирования информационного пространства Содружества Независимых Государств.

Межпарламентская Ассамблея государств – участников СНГ, состоящая из парламентских делегаций государств – участников, взаимодействует со всеми странами СНГ в сфере безопасности. Адаптируя международный опыт борьбы с угрозами безопасности применительно к условиям государств – участников, МПА СНГ разрабатывает для них типовые модельные законодательные акты и рекомендации. Эти документы не обладают обязательной юридической силой, однако наличие типовых моделей правового регулирования определённых отношений составляет потенциал для развития национальных систем законодательства в общем ключе. Благодаря их наличию создаётся механизм имплементации положений международно-правовых документов в национальные правовые системы государств – участников СНГ.

В международно-правовых актах СНГ понятие «информационная безопасность» впервые получило свое легальное определение в 2002 г. в Модельном законе «О международном информационном обмене» как «**состояние защищенности информационной среды общества, обеспечивающее её формирование, использование и развитие в интересах граждан, организаций, государства**». В 2006 г. Советом глав государств СНГ была принята Стратегия сотрудничества в сфере информатизации; в 2008 г. — Концепция сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности. В 2012 г. Советом глав государств СНГ принята Стратегия сотрудничества государств в построении и развитии информационного общества, а в ноябре 2013 г. подписано Соглашение «О сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности».

Комплексным планом мероприятий по реализации Концепции сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности на 2008-2010 гг. была предусмотрена разработка Рекомендаций по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности. С некоторым запозданием этот вопрос нашел своё отражение в Перспективном плане модельного законотворчества в СНГ на 2011-2015 гг.

Стремительное развитие информационной сферы обусловило отставание в выработке правовых механизмов адекватного парирования ее новых вызовов и угроз. Несмотря на то, что в СНГ и ОДКБ и до этого принимались межгосударственные документы, имеющие важнейшее значение для обеспечения информационной безопасности, следует признать, что они объективно не могли исключить негативные проявления в данной сфере. Современный уровень вызовов и угроз информационной безопасности детерминировал необходимость поиска новых подходов к комплексному нормативному правовому противодействию им.

Интернациональный коллектив российских и белорусских учёных предпринял попытку подготовки проекта Рекомендаций по совершенствованию и гармонизации национального законодательства для государств – участников СНГ в сфере обеспечения информационной безопасности. Проект этого концептуального по своему характеру документа в 2010-2012 гг. публиковался для широкого обсуждения на страницах ряда периодических научных изданий, что в конечном итоге предопределило

Защита диссертации на соискание учёной степени доктора юридических наук в Институте государства и права РАН профессором Института национальной безопасности Республики Беларусь Макаровым О.С.

успешное завершение работы над ним. В 2013 г., помимо вышеназванных Рекомендаций, тем же научным коллективом полностью была завершена работа над Рекомендациями по правовому регулированию эксплуатации открытых телекоммуникационных сетей для предупреждения их использования в террористических и иных противоправных целях.

Целью разработки Рекомендаций по совершенствованию и гармонизации законодательства в сфере информационной безопасности явилось формулирование общих подходов для государств – участников СНГ к правовому регулированию информационной безопасности. Разработчики документа предложили опереться на трактовку понятия «информационная безопасность — состояние защищенности личности, общества, государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве», использованную в Соглашении о сотрудничестве в области обеспечения международной информационной безопасности, заключённом в 2009 г. между правительствами государств – членов Шанхайской организации сотрудничества.

Документ, носящий концептуальный характер, прошел экспертное обсуждение в парламентах государств-участников и был принят на 38-м пленарном заседании МПА СНГ в 2012 г. В том же году был подготовлен и вышел в свет «Словарь-справочник понятийного аппарата модельного законодательства государств – участников СНГ, отмеченный профессиональной премией Национального ИНФОФОРУМА по информационной безопасности.

В разработанных российскими и белорусскими учёными и принятых Рекомендациях были обоснованы также предложения об изменении базового Модельного закона МПА СНГ «Об информатизации, информации и защити информации» и о разработке нового Модельного закона «Об объектах критически важных информационных технологий». Эти предложения поддержаны Советом Федерации Федерального Собрания Российской Федерации и нашли своё отражение в обновлённом перспективном плане законотворчества МПА СНГ на 2012-2015 гг. Комплекс законодательных инициатив получил своё закрепление в межгосударственных программах сотрудничества государств – участников СНГ в сфере безопасности на периоды 2014–2018 гг., которые 25 октября 2013 г. утвердил Совет глав государств СНГ.

В соответствии с результатами проведенной исследовательской работы, составившими основу принятых межгосударственных решений, 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, Модельного закона «О критически важных объектах информационно-коммуникационной инфраструктуры», изменений в Модельный закон «Об информации, информатизации и защите информации», которые обусловят выход в свет его новой редакции. Названные проекты обсуждались на научно-практической конференции «Теоретические и прикладные проблемы информационной безопасности» в Республике Беларусь (г. Минск, 2014) и в настоящее время проходят комплексную экспертизу в государствах Содружества.

ОДКБ. Договор о коллективной безопасности на постсоветском пространстве был подписан в 1992 г., однако сама ОДКБ — организация военно-технического сотрудничества появилась десятилетием позже. Концепция коллективной безопасности государств – участников Договора о коллективной безопасности представляет собой совокупность взглядов этих государств на предотвращение и устранение угрозы миру, совместную защиту от агрессии, обеспечение их суверенитета и территориальной целостности. Эта Концепция закрепляет приверженность государств – участников Договора целям предотвращения войн и вооруженных конфликтов, устранению их из системы международных отношений, созданию условий для всестороннего развития личности, обществ и государств на базе идеалов гуманизма, демократии и всеобщей безопасности.

В качестве источников военной опасности в Концепции коллективной безопасности ОДКБ указаны попытки вмешательства извне во внутренние дела государств, попытки дестабилизации их внутриполитической обстановки, международный терроризм, политика шантажа. Сегодня подобные угрозы во многом реализуются через информационную сферу. Военная, оборонная и информационная безопасность тесно взаимосвязаны, информационные технологии уже стали одним из важнейших политико-экономических и военных ресурсов.

Государства – члены ОДКБ, в соответствии с Уставом этой организации, принимают меры по развитию договорно-правовой базы, регламентирующей функционирование системы коллективной безопасности, по гармонизации национального законодательства по вопросам обороны, военного строительства и безопасности. В качестве одного из основных направлений создания системы коллективной безопасности позиционируется сближение основных положений законодательных актов в области обороны и безопасности. В 2006 г. была создана Парламентская Ассамблея (ПА ОДКБ) – орган межпарламентского сотрудничества государств – членов Организации Договора о коллективной безопасности.

Программа совместных действий государств – членов ОДКБ по формированию системы информационной безопасности была принята в 2008 г. 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.

В 2010 г. обеспечение информационной безопасности, как важное направление сотрудничества, было закреплено в Уставе ОДКБ. Статья 8 Устава ОДКБ гласит: «Государства – члены взаимодействуют в сферах охраны государственных границ, обмена информацией, информационной безопасности, защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера, а также от опасностей, возникающих при ведении или вследствие военных действий». В том же году Совет коллективной безопасности ОДКБ утвердил Положение о сотрудничестве государств – членов ОДКБ в сфере информационной безопасности. В соответствии с этим Положением в формате ОДКБ определены национальные координирующие органы в сфере информационной безопасности.

В 2011 г. Советом коллективной безопасности ОДКБ был разработан и утверждён Перечень мероприятий, направленных на формирование системы обеспечения информационной безопасности в интересах ОДКБ. В их развитие приняты План первоочередных мероприятий по формированию основ скоординированной информационной политики в интересах государств – членов ОДКБ и Перечень мероприятий, направленных на формирование системы обеспечения информационной безопасности в интересах ОДКБ.

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. Вследствие этого существует настоятельная необходимость всесторонней углубленной научной проработки принципиальных целей, задач и направлений развития сотрудничества государств по противодействию современным угрозам в информационной сфере.

Для согласования политик требуется определенность и однозначность понятийного аппарата. Органам власти и управления, субъектам хозяйственной деятельности, физическим и юридическим лицам различных государств необходимы сведения, основанные на едином понимании предметов и явлений информационного пространства, регулируемого законодательными положениями. Для эффективного взаимодействия и сотрудничества необходима развитая система терминов и понятий, их определений, её закрепление в нормативных актах и общественном обращении, а также правовое толкование понятийного аппарата в повседневной практике. В пользу актуальности постановки и решения такой задачи свидетельствует предусмотренная планами Экспертного совета Регионального содружества связи и Экспертно-консультативного совета при ПА ОДКБ разработка глоссариев в области информационной безопасности.

С учетом возрастания актуальности задач защиты секретов (и не только государственных) российскими и белорусскими специалистами были разработаны принятые ПА ОДКБ в 2010 г. Рекомендации по сближению законодательства государств – членов ОДКБ по вопросам государственной тайны. В 2011 г. вышел в свет, подготовленный СПИИРАН в рамках работы в Экспертно-консультативном совете при ПА ОДКБ, «Глоссарий основных понятий в законодательстве о государственной тайне государств – членов ОДКБ». В 2014 году СПИИРАН подготовил и выпустил в свет «Словарь-справочник по информационной безопасности для Парламентской Ассамблеи ОДКБ».

Список литературы:

1. **Вус М.А., Кучерявый М.М., Макаров О.С., Перекопский Г.И.** Для совершенствования системы информационной безопасности в ОДКБ // Власть. – 2014. – № 8. – С. 37-40.
2. **Шушин В.О.** О состоянии и перспективах сотрудничества государств – членов ОДКБ по формированию системы информационной безопасности // Законодательство государств – членов ОДКБ в сфере обеспечения информационной безопасности: опыт, проблемы и перспективы гармонизации. Материалы международной научно-практической конференции (Санкт-Петербург, 28.11.2013). – СПб:. Секретариат Совета МПА СНГ, 2014.
3. Словарь-справочник по информационной безопасности для парламентской Ассамблеи ОДКБ / Под общ. ред. **М.А. Вуса и М.М. Кучерявого** – СПб.: СПИИРАН. Изд-во «Анатолия», 2011. – 96 с.
4. **Бачило И.Л., Вус М.А., Гусев В.С., Макаров О.С.** Глоссарий основных понятий в законодательстве о государственной тайне государств – членов ОДКБ. Сборник – СПб.: СПИИРАН. Изд-во «Анатолия», 2011. – 79 с.
5. Словарь – справочник терминов и определений понятий модельного законодательства государств – участников СНГ / Под ред. **М.А. Вуса и В.В. Бондуровского** – СПб.: Изд-во «Юридический Центр-Пресс», 2012. – 360 с.

Научно-практическая конференция «Теоретические и прикладные проблемы информационной безопасности» (Республика Беларусь, г. Минск, июнь 2014 г.)

Один из парламентских отзывов на разрабатываемые законопроекты

НАЦЫЯНАЛЬНЫ СХОД
РЭСПУБЛІКІ БЕЛАРУСЬ
ПАЛАТА ПРАДСТАЎНІКОЎ
Пастаянная камісія па прамысловасці, паліўна-энергетычнаму комплексу, транспарту і сувязі
220010, г. Мінск, Дом Урада,
тэл./факс (017) 222-43-52, факс (017) 327-37-84
E-mail: prom@house.gov.by

НАЦИОНАЛЬНОЕ СОБРАНИЕ
РЕСПУБЛИКИ БЕЛАРУСЬ
ПАЛАТА ПРЕДСТАВИТЕЛЕЙ
Постоянная комиссия по промышленности, топливно-энергетическому комплексу, транспорту и связи
220010, г. Минск, Дом Правительства,
тел./факс (017) 222-43-52, факс (017) 327-37-84
E-mail: prom@house.gov.by

_____ _____

на№ _____ от _____

Генеральному секретарю Совета
Межпарламентской Ассамблеи
государств — участников СНГ

Сергееву А.И.

О рассмотрении проектов
модельных законов

Уважаемый Алексей Иванович!

По поручению Председателя Палаты представителей Национального собрания Республики Беларусь Андрейченко В.П. Постоянной комиссией Палаты представителей Национального собрания Республики Беларусь по промышленности, топливно-энергетическому комплексу, транспорту и связи в рамках ее компетенции совместно с Главным экспертно-правовым управлением Секретариата Палаты представителей Национального собрания Республики Беларусь рассмотрены проект изменений в модельный закон «Об информатизации, информации и защите информации», а также проекты концепций модельных законов «Об электронном правительстве», «О трансграничном информационном обмене электронными документами» и «О межгосударственном обмене отправлениями специальной связи».

Замечаний и предложений по указанным документам не имеется.

С уважением,

Председатель Постоянной комиссии
по промышленности, топливно-
энергетическому комплексу,
транспорту и связи

Д.И.Харитончик

Секретариат Совета МПА СНГ
3 июля 2014 г.
Вх. № 1123/23

10 Лепкович 222 6146

УДК 004; 342

Об изменениях Модельного закона СНГ «Об информатизации, информации и защите информации» (2005 г.) в его новой редакции с изменённым названием «Об информации, информатизации и обеспечении информационной безопасности»

И.Л. Бачило, М.А. Вус, О.С. Макаров

Межгосударственной программой сотрудничества государств – участников СНГ в области совместных мер по борьбе с преступностью на 2014-2018 гг., утверждённой решением Совета глав государств СНГ 25 октября 2013 г., предусмотрено внесение изменений в принятый в 2005 г. (постановлением МПА СНГ № 26-7) Модельный закон «Об информатизации, информации и защите информации». Исполнителями этой работы были определёны Санкт-Петербургский институт информатики и автоматизации РАН, Институт государства и права РАН и Институт национальной безопасности Республики Беларусь. Срок выполнения работы — 2014 г.

В процессе подготовительной работы по обоснованию изменений в названный выше закон исполнители пришли к выводу о необходимости как уточнений содержания отдельных его статей, так и изменения структуры и самого названия этого закона.

Рабочий проект обновленного закона, предусматривавший предлагаемые ниже изменения, включая и изменение названия этого закона, был обсужден на заседаниях Объединенной комиссии при МПА СНГ по гармонизации законодательства в сфере безопасности и противодействия новым вызовам и угрозам и Постоянной комиссии по вопросам обороны и безопасности МПА СНГ 17 апреля 2014 г. Комиссии МПА СНГ согласились в основном с предложенными изменениями в Модельный закон и направили его проект в парламенты государств – участников СНГ для получения экспертных заключений.

В письменных отзывах, поступивших из парламентов Республики Беларусь, Республики Казахстан, Российской Федерации и Республики Таджикистан, концептуальных замечаний и предложений по проекту предлагаемых изменений в существующий Модельный закон СНГ «Об информатизации, информации и защите информации» не имеется.

В процессе подготовки уточненного проекта нового закона с измененным названием (проекта Модельного закона «Об информации, информатизации и обеспечении информационной безопасности») его разработчиками были учтены предложения, полученные в устном порядке от членов комиссий, новые нормативно правовые материалы по тематике закона, итоги обсуждения на международной научно-практической конференции «Теоретические и прикладные проблемы информационной безопасности» (Академия МВД Республики Беларусь, июнь 2014 г.), другие материалы по проблематике совершенствования правового регулирования информационной безопасности.

В ходе работы над проектом были использованы национальные законодательные акты, в частности, Федеральный Закон Российской Федерации №149 «Об информации, информационных технологиях и защите информации» (2006 г., с учетом вносившихся в него в последующие годы изменений), законы «Об информатизации» Республики Казахстан (2007 г., в редакции 2013 г.) и Республики Беларусь (2008 г., в редакции 2014 г.). Были приняты во внимание также международно-правовые нормы, такие, например, как ратифицированный Генеральной Ассамблеей Американских государств межамериканский Модельный закон «О доступе к публичной информации» и принятый этой Ассамблеей в 2014 г. «Модельный закон об Интернете», другие международно-правовые акты.

По итогам проведенной работы, во исполнение постановлений комиссий МПА СНГ по гармонизации законодательства в сфере безопасности и противодействия новым вызовам и угрозам и по вопросам обороны и безопасности, разработчики представляют проект измене-

п.п. №	Структура действующего Модельного закона СНГ «Об информатизации, информации и защите информации» (2005 г.)	Структура проекта Модельного закона СНГ «Об информации, информатизации и обеспечении информационной безопасности» (проект 2014 г.)
1.	**Глава1. Общие положения** Ст.1. Сфера действия настоящего закона Ст.2. Основные понятия, используемые в настоящем Законе Ст.3. Законодательство об информатизации, информации и защите информации Ст. 4 Принципы правового регулирования информационных отношений.	**Глава 1. Общие положения** Ст.1 Цели и сфера действия модельного закона Ст.2. Основные термины и понятия, используемые в настоящем законе Ст.3. Субъекты отношений в сфере действия настоящего закона Ст. 4. Законодательство в области информации, информатизации и информационной безопасности С.5. Принципы правового регулирования отношений в рамках данного закона Ст. 6. Основные принципы государственной политики в области информации, информатизации и обеспечения информационной безопасности
2.	**Глава 2. Основы правового режима информации** Ст.5. Информация как объект правового регулирования Ст.6. Виды информации Ст. 7. Категории доступа к информации Ст.8. Порядок распространения информации Ст.9. Обладатель информации Ст. 10. Общедоступные сведения Ст.11. Публичное предоставление информации Ст. 12. Предоставление информации по договору. Ст. 13. Договор оказания информационных услуг Ст. 14. Документированная информация.	**Глава 2. Информация, информационные ресурсы, основы правового режима информационных ресурсов** Ст. 7. Информация, информационные ресурсы, виды и учёт информационных ресурсов Ст. 8 Основы правового режима информационных ресурсов Ст. 9. Правовой режим открытой (общедоступной) информации Ст. 10. Информация ограниченного доступа
3.	**Глава 3. Информатизация информационные системы и информационные технологии** Ст. 15. Государственная политика и полномочия государства в сфере информатизации Ст. 16. Информационная система Ст. 17. Государственные информационные системы Ст. 18. Создание и эксплуатация государственных информационных систем Ст.19. Обязательные требования к средствам обработки информации в государственных информационных системах Ст.20. Исключительные права на объекты интеллектуальной собственности, включаемые в состав государственных информационных систем Ст.21. Хранение и резервное копирование информации в государственных информационных системах Ст.22. Использование информационно-телекоммуникационных сетей.	**Глава 3. Информатизация, информационные системы и информационные технологии** Ст. 11. Государственная политика в сфере информатизации Ст. 12. Организационно-правовое обеспечение реализации государственной политики в сфере информатизации Ст. 13. Формирование и структуризация информационного пространства Ст. 14. Организационно-правовое обеспечение развития информационной инфраструктуры отрасли ИКТ Ст. 15. Организационно-правовое регулирования информационной инфраструктуры системы государственного управления Ст. 16. Взаимодействие органов государственного управления и местного самоуправления со структурами, создающими инфокоммуникационную базу ИКТ Ст. 17. Юридическое оформление отношений субъектов в процессе информатизации: договоры, соглашения, регламенты
4.	**Глава 4. Право на информацию** Ст. 23. Содержание права на информацию Ст.24. Право на информацию о деятельности органов государственной власти и органов местного самоуправления Ст. 25. Реализация права на информацию о деятельности органов государственной власти и органов местного самоуправления Ст. 26. Гарантии права на информацию	**Глава 4. Правовое регулирование обеспечения информационной безопасности и ответственности за правонарушения в процессах информатизации** Ст. 18. Государственная политика в области обеспечения информационной безопасности Ст. 19. Направления, цели и задачи обеспечения информационной безопасности Ст. 20 Методы организационно-правового регулирования обеспечения информационной безопасности Ст. 21. Обеспечение информационной безопасности критически важных объектов Ст. 22. Обеспечение безопасности инфо-коммуникационной инфраструктуры и ИКТ Ст. 23. Защита прав граждан, организаций и органов государственной власти на реализацию их законных прав, исполнение обязанностей и функций этих категорий субъектов в информационном пространстве Ст.24. Обеспечение безопасности информационной среды: открытой и общедоступной информации, информации ограниченного доступа Ст.25. Защита от распространения и использования вредной и деструктивной информации Ст . 26. Виды и формы юридической ответственности за правонарушения в области информационных отношений Ст. 27. О введении в действие настоящего Закона
5.	**Глава 5. Ограничения на доступ к информации и на распространение информации** Ст. 27. Конфиденциальная информация Ст. 28. Информация о частной жизни и информация персонального характера Ст. 29. Коммерческая тайна Ст. 30. Профессиональная тайна Ст.31. Государственная и служебная тайны Ст. 32. Ограничения на распространение информации	
6.	**Глава 6. Защита информации** Ст. 33. Государственное регулирование зашиты информации Ст. 34. Обеспечение информационной безопасности Ст. 35. Защита информации и информационных системах Ст.36. Ответственность за правонарушения в сфере защиты информации и права на информацию Ст. 37. Вступление в силу настоящего Закона	

ний в ныне существующий Модельный закон СНГ «Об информатизации, информации и защите информации», включающий:

- изменение самого названия существующего Модельного закона;
- уточнения структуры Модельного закона и содержания отдельных его статей.

Выше приведена сравнительная таблица структур проекта нового Модельного закона под названием «Об информации, информатизации и обеспечении информационной безопасности» и существующего в настоящее время Модельного закона СНГ «Об информатизации, информации и защите информации».

Структура проекта и содержание статей новой версии Модельного закона позволяют отметить его новизну с учетом следующего:

1) изменено названия закона — в предлагаемой его новой формулировке: «Об информации, информатизации и обеспечении информационной безопасности»;
2) сокращено число глав в структуре закона с изменением их названия и содержания;
3) уточнён предмет регулирования – расширена сфера применения закона в области информационно-коммуникационного взаимодействия государств в едином информационном пространстве Содружества Независимых Государств, что прослеживается по всем главам проекта предлагаемого изменённого закона;
4) частично изменён перечень и содержательные трактовки используемых в законе терминов и их определений:
   - термин информационная безопасность используется в содержательной трактовке: «состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве»;
   - обеспечение информационной безопасности — «деятельность по разработке и реализации системы мер правового, организационно-технического и организационно-экономического характера по выявлению угроз информационной безопасности, предотвращению их реализации, пресечению и ликвидации последствий реализации таких угроз в национальном и международном информационно-коммуникационном пространстве»;
   - информация официальная — «информация, исходящая от органов государственной власти и органов местного самоуправления, других государственных и негосударственных органов и организаций, создаваемая, распространяемая и используемая в соответствии с правовым статусом ее источника»; и др.

Представляемый проект исправленного и дополненного Модельного закона СНГ от 18 ноября 2005 г., именуемый теперь как Модельный закон «Об информации, информатизации и обеспечении информационной безопасности», учитывает опыт национального правового регулирования процессов использования ИКТ за последнее десятилетие в ходе информатизации и обеспечения защиты информации. Он может рассматриваться как базовый модельный акт, консолидирующий порядок формирования и использования информационно-коммуникационных технологий и информационных ресурсов государств, нацеленный на обеспечение процессов информатизации на новом этапе безопасного и более эффективного взаимодействия субъектов в едином информационном пространстве Содружества Независимых Государств.

Авторская версия проекта Модельного закона СНГ «Об информации, информатизации и обеспечении информационной безопасности» приводится ниже, на страницах 65-75 данного выпуска журнала.

УДК 342.9; 351.7

ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ ФОРМИРОВАНИЯ СИСТЕМЫ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ

Д.В. Перевалов

В современных условиях интенсивное развитие инфраструктур в различных сферах жизнедеятельности государства, в том числе информационно-коммуникационной инфраструктуры (далее – ИКИ) обуславливает увеличение числа различного рода критически важных объектов (далее – КВО), нарушение нормального функционирования или выведение из строя которых может привести к тяжким (а в ряде случаев – к необратимым) последствиям для страны (отдельных регионов) и (или) её (их) населения.

В связи с этим в большинстве государств всё больше актуализируется проблема формирования обоснованной и оптимальной системы КВО ИКИ в целях обеспечения должного и надёжного функционирования всех общественных и государственных институтов.

Вместе с тем анализ научно-практической литературы показывает, что учёными и специалистами исследуются, в основном, вопросы формирования систем КВО в отдельных областях [1, с. 39–40], [2, с. 18–198], [3, с. 5–20], [4, с. 2–14], [5, 34–66], [6, с. 50–55], [7, с. 102–104], [8, с. 8–131], [9, с. 289–304] либо отдельные аспекты такой деятельности [10, с. 42-47], [11, с. 46-48], [12, с. 6-13], [13, с. 7–35, 108–132], [14, с. 666–677], [15, с. 20–24], [16, с. 2–15]. При этом комплексных научных разработок проблемы формирования общегосударственной систем КВО ИКИ фактически не осуществляется. В связи с этим представляется актуальным и востребованным определить основные правовые и организационные аспекты её разрешения на современном этапе.

Учитывая, что нормативно ИКИ не определена, то такую инфраструктуру целесообразно рассматривать как совокупность территориально распределенных государственных и корпоративных информационных систем, сетей связи, средств коммутации и управления информационными потоками, а также организационных структур, нормативно-правовых механизмов регулирования, обеспечивающих их эффективное функционирование. При этом под объектом ИКИ представляется обоснованным понимать совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения функционирования такого объекта, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, а также персонала, который осуществляет их эксплуатацию.

В таком случае объекты ИКИ будут являться критически важными, если они:

- обеспечивают функционирование экологически опасных и (или) социально значимых производств и (или) технологических процессов, нарушение (прекращение) штатного режима которых может привести к чрезвычайной ситуации техногенного характера;

- осуществляют функции информационной системы, нарушение (прекращение) функционирования которой может привести к тяжким последствиям для национальной безопасности в политической, экономической, социальной, информационной, экологической, иных сферах;
- обеспечивают предоставление значительного объема информационных услуг, частичное или полное нарушение (прекращение) оказания которых может привести к тяжким для национальной безопасности в политической, экономической, социальной, информационной, экологической, иных сферах.

В связи изложенным КВО ИКИ могут быть разделены на две группы:

1) самостоятельный имущественный комплекс (как правило, юридическое лицо), который обеспечивает выполнение определённых информационно-коммуникационных функций (например, оператор услуг Интернета (ст.ст. 2, 3 Модельного закона СНГ «Об основах регулирования Интернета» [17]));

2) автоматизированные системы управления технологическими процессами (далее – АСУ ТП), которые являются элементами промышленных, энергетических, банковских и тому подобных объектов, и связаны с другими объектами ИКИ (например, АСУ ТП железной дороги или автоматизированная банковская система, которая автоматизирует банковские технологические процессы (платёжный, информационный и др.)).

Выделение КВО в ИКИ направлено на достижение следующих целей:

- поддержание стабильного управления государством или административно-территориальной единицей (регионом);
- поддержание устойчивого уровня экономики государства или административно-территориальной единицы (региона);
- поддержание должного уровня жизнедеятельности населения, проживающего на территории государства или административно-территориальной единицы (региона);
- создание условий безопасного функционирования ИКИ.

Особое место КВО ИКИ предопределяет их ключевую роль в обеспечении нормального функционирования практически всех важнейших сфер жизнедеятельности общества и государства – политической, экономической, социальной, экологической, военной, а также – непосредственно в информационной сфере.

Нарушение нормальной деятельности КВО ИКИ неизбежно приводит к возникновению тяжких последствий в виде:

- потери государственного управления на длительный срок (например, в результате нарушения связи между государственными органами и подчинёнными ими организациями, при осуществлении компьютерной атаки на государственные информационные системы и т.п.);
- чрезвычайных ситуаций техногенного характера (например, прекращение движения значительного числа поездов на длительный период, выброс значительного количества опасных химических веществ и заражение большой территории и т.п.);
- отказа на длительный период достаточно большого сегмента банковских платёжных систем (например, крупные сбои в работе платёжных терминалов торговых предприятий, банкоматов и т.п.) и т.д.

Подобные последствия всегда обуславливают ухудшение политической и социально-экономической обстановки в стране и дестабилизации внутригосударственной ситуации. Это приводит к причинению ущерба конкретной сфере жизнедеятельности общества и государства – подрыву авторитета государственной власти, массовой гибели или заболеванию людей, потере существенных денежных, сырьевых и иных ресурсов, вывод из использования ранее плодородных земель, утрате управления вооружёнными силами государства и т.д.

В связи с этим государство выделяет в особую область регулирования вопросы безопасности КВО ИТИ и ставит соответствующие цели, которые должны достигаться при эксплуатации таких объектов.

В области безопасности КВО ИКИ необходимо выделять **два тесно взаимосвязанных, но разных по своему содержанию направления**:

1) формирование и обеспечение безопасного функционирования системы КВО ИКИ, то есть выделение среди объектов ИКИ государства критически важных и поддержание их безопасного функционирования в соответствии с правилами и требованиями, предъявляемым к реализуемым на них информационным технологиям;

2) обеспечение безопасности КВО ИКИ, то есть осуществление правомерной деятельности работников таких объектов, их службы безопасности во взаимодействии с сотрудниками уполномоченных государственных органов (организаций) и иными юридическими и физическими лицами по реализации системы правовых, организационных, инженерно-технических, программно-аппаратных и специальных мер, направленных на охрану и защиту КВО ИКИ и обеспечивающих соблюдение интересов государства и общества (в частности, реализация специально разработанных мер, не связанных с информационными технологиями, – определение порядка доступа на территорию объекта, его физическая охрана и т.п.).

1. Основываясь на сложившихся подходах в области категорирования КВО [3, с. 5–20], [5, с. 34–66], [10, с. 42–47],[11, с. 46–48], [12, с. 6–13], [15, с. 20–24] и на результатах проведённых научных исследований [18, с. 17–160], **формирование системы КВО ИКИ и обеспечение их безопасного функционирования** должно включать в себя следующие этапы.

1 этап: выделение в социально-экономической инфраструктуре государства отраслевой ИКИ.

На данном этапе предполагается легитимная идентификация такой отраслевой инфраструктуры, как ИКИ, и предусматривается закрепление её состава (объекты, линии связи и т.п.) в соответствующих нормативных правовых актах. В настоящее время, в частности, можно говорить о том, что в рамках СНГ официально определены лишь инфраструктура железнодорожного транспорта и её состав (ст.1, Приложение 1 Технического регламента Таможенного союза «О безопасности железнодорожного транспорта» (ТР ТС 003/2011), утв. Решением Комиссии Таможенного союза от 15.07.2011 № 710 [19]), а также высокоскоростного железнодорожного транспорта (ст.1, Приложение 1 Технического регламента Таможенного союза «О безопасности высокоскоростного железнодорожного транспорта» (ТР ТС 002/2011), утв. Решением Комиссии Таможенного союза от 15.07.2011 № 710 [19]). Для ИКИ такой состав нормативно не определён.

2 этап: определение признаков критичности ИКИ.

Для того чтобы определить критичность ИКИ, требуется разработка соответствующих признаков. Например, в Российской Федерации определены следующие признаки критической инфраструктуры гидротехнических сооружений: перечень соответствующих сооружений; возможность возникновения чрезвычайной ситуации при их повреждении (ст.1 Федерального закона РФ «О безопасности гидротехнических сооружений» [20]).

Видится обоснованным в качестве признаков критичности ИКИ рассматривать:

1) наличие взаимосвязанной совокупности объектов такой инфраструктуры;

2) возможность наступления тяжких последствий для отрасли при нарушении (прекращении) нормального функционирования одного или части объектов.

Такие признаки должны найти закрепление в соответствующем законодательном акте.

3 этап: выделение из числа критических инфраструктур государства критической ИКИ.

Соответствующее отраслевое министерство или ведомство государства (например, министерство связи) в соответствии с установленными признаками выделяет ИКИ и вносят предложения правительству по её легитимизации в соответствующем нормативном акте.

4 этап: определение основного критерия выделения КВО в ИКИ.

Общие требования к объектам ИКИ для отнесения их к критически важным определяются функциональным назначением таких объектов и характером взаимодействия его с другими объектами социальной, производственной, транспортной, инженерной и иной инфраструктуры, в том числе отнесенными к критически важным.

Для выделения КВО из числа других объектов ИКИ в настоящее время могут быть использованы два способа:

1) определение недопустимого ущерба [3, с. 9–11];

2) определение важности объекта [21, с. 2–12].

Вместе с тем анализ содержания обоих способов показывает, что «определение недопустимого ущерба» фактически является составным элементом «определения важности объекта». В связи с этим в качестве основного критерия выделения КВО в ИКИ целесообразно рассматривать важность объекта, характеризующаяся уровнем возможных последствий нарушения (прекращения) его функционирования:

- утрата управления государством или административно-территориальной единицей (регионом);
- потеря управления экономикой государства или административно-территориальной единицы (региона);
- необратимое негативное изменение (или разрушение) государственного управления или экономики государства или административно-территориальной единицы (региона);
- существенное снижение безопасности жизнедеятельности населения, проживающего на территории государства или административно-территориальной единицы (региона), на длительный период времени.
- В частности, для оценки важности объекта в масштабе соответствующих групп (в частности, и в рамках ИКИ) может быть разработана система рамочных критериев, которые характеризуются следующими показателями [21, с. 2]:
  1) значимость объекта для экономики страны или административно-территориальной единицы (региона) (П1 – стоимость годового выпуска товарной продукции (млн. руб.); П2 – общая численность производственного персонала (тыс. чел.); ПЗ – балансовая стоимость основных производственных фондов (млн. руб.); П4 – доля основной продукции объекта в продукции того же вида, выпускаемой в государстве (в %);
  2) нанесение ущерба престижу государства (П5 – нарушение управляемости государства или административно-территориальной единицы (региона); П6 – нанесение ущерба авторитету государства, в том числе на международной арене; П7 – раскрытие государственных секретов, конфиденциальной научно-технической или коммерческой информации; П8 – нарушение боеготовности и боеспособности вооруженных сил; П9 – нарушение стабильности финансовой или банковской систем);
  3) возможные угрозы населению и территориям (П10 – крупномасштабное уничтожение национальных ресурсов (природных, сельскохозяйственных, продовольственных, производственных, информационных); П11 – величина территории заражения в случае аварии на объекте; П12 – численность населения, которое может

пострадать в случае аварии на объекте; П13 – нарушение систем обеспечения жизнедеятельности городов и населенных пунктов; П14 – массовые нарушения правопорядка; П15 – остановка непрерывных производств; П16 – аварии и катастрофы регионального масштаба).

Состав системы частных показателей важности объектов устанавливается методом экспертного опроса специалистов, имеющих соответствующую компетенцию.

5 этап: выделение КВО в ИКИ.

В ИКИ в соответствии с основным критерием выделяются объекты, которые являются КВО. При этом целесообразно использовать процедурный подход отнесения объектов КОИ к КВО, который включает в себя следующие стадии [18, с. 75–78, 81–94]:

1) установление оснований для отнесения объекта ИКИ к КВО;
2) принятие решения о включении объекта в перечень КВО ИКИ;
3) учёт объекта, отнесённого к КВО, в Государственном реестре КВО ИКИ;
4) исключение объекта из перечня КВО ИКИ.

Работу по выделению КВО в ИКИ осуществляет отраслевое министерство или ведомство, которое принимает соответствующие решения и закрепляет их в свих нормативных актах.

6 этап: определение отраслевых критериев категорирования КВО в ИКИ.

В ИКИ сосредоточены КВО различных групп и различного уровня (такая классификация рассматривалась выше). В связи с этим для различных КВО в ИКИ требования будут различными, так как иначе это приведёт к необоснованному завышению расходов по обеспечению безопасного функционирования и безопасности таких объектов.

Поэтому является обоснованным разделение таких объектов на категории, что позволит определить для каждой категории КВО оптимальную систему правил и требований обеспечения их безопасного функционирования, а также их безопасности.

Для определения категорий КВО ИКИ необходимо выделение соответствующих отраслевых критериев. В качестве таких критериев могут выступать тяжесть последствий, объём оказываемых услуг, количество используемых в технологическом процессе опасных веществ, величина и содержание финансовых или информационных активов и т.п. Такие критерии должны закрепляться нормативными актами отраслевого министерства или ведомства.

7 этап: категорирование КВО в ИКИ.

Для категорирования КВО в соответствии с отраслевыми критериями могут использоваться следующие общие методы [19, с. 61–68]:

- метод анализа вида последствий и критичности отказов;
- метод категорирования по группам безопасности;
- метод категорирования по уровню угроз техногенного, природного, террористического характера и степени защищенности объекта;
- метод категорирования сложных объектов.

На этом этапе уполномоченные государственные органы в области безопасного функционирования КВО ИКИ включают соответствующий объект в Государственный реестр КВО ИКИ. При этом различные категории КВО могут быть включены в различные Государственные реестры (например, госреестр КВО 1-ой категории; госреестр КВО 2-ой категории и т.д.).

8 этап: определение требований к обеспечению безопасного функционирования КВО с учётом специфики ИКИ и его категории.

Требования к обеспечению безопасного функционирования КВО ИКИ определяются в зависимости от особенностей его деятельности (например, для опасных производственных объектов такие требования определены в ст.ст. 7-10 Модельного закона СНГ «О промышленной безопасности опасных производственных объектов» [22]).Общие требования закрепляются, как правило, в законодательных актах, конкретные – в технических нормативных правовых актах.

Кроме того, объём и характер таких требований должен зависеть от категории объекта: чем ниже категория объекта, тем меньше объём требований и они более мягкие.

9 этап: проверка деятельности КВО ИКИ на соответствие требованиям к обеспечению его безопасного функционирования.

Проверка данной деятельности КВО ИКИ осуществляться, как правило, отраслевым министерством или ведомством, а также уполномоченными государственными органами в области безопасности КВО ИКИ в соответствии с их компетенцией. Такая проверка проводится посредством определения соответствия деятельности по эксплуатации объекта (его оборудования, иных систем) установленным требованиям и правилам.

В частности, проверка опасных производственных объектов осуществляется в рамках экспертизы промышленной безопасности организациями, имеющими лицензию на проведение указанной экспертизы, а также государственным органом исполнительной власти, специально уполномоченным в области промышленной безопасности (его территориальные органы и другие государственные органы исполнительной власти в соответствии с законодательством государства) в ходе государственного контроля (ст.ст. 13,16 Модельного закона СНГ «О промышленной безопасности опасных производственных объектов»).

Проверка деятельности КВО ИКИ на соответствие требованиям к обеспечению его безопасного функционирования должна осуществляться уполномоченными государственными органами в области безопасности КВО ИКИ в рамках внешнего контроля безопасного функционирования таких объектов.

Такой контроль осуществляется в определённый период (например, не реже одного раза в пять лет) либо, как правило, в следующих случаях:

- принятия такими органами решения о проведении данного вида контроля по результатам внутреннего контроля;
- принятия собственником (владельцем) в установленном порядке решения об изменении функций КВО ИКИ;
- изменения местонахождения КВО ИКИ;
- возникновения инцидента безопасности.

Если по результатам контроля безопасного функционирования КВО ИКИ выявляется несоответствие объекта требованиям, установленным законодательством в области безопасности КВО ИКИ и (или) эксплуатационной документацией, собственник (владелец) обязан в срок, установленный в соответствующих актах, принять меры по устранению выявленных несоответствий.

В случае нарушений правил и требований в области безопасности КВО ИКИ виновные лица могут быть привлечены к установленным видам ответственности. Например, нарушение правил эксплуатации компьютерной системы или сети является уголовно наказуемым деянием в соответствии со ст.292 Модельного уголовного кодекса для государств – участников СНГ [23].

10 этап: приведение деятельности КВО ИКИ в соответствие с требованиями к обеспечению его безопасного функционирования.

В случае выявления несоответствия параметров деятельности объекта установленным правилам и требованиям к его безопасному функционированию уполномоченными субъектами принимаются необходимые меры по приведению её в надлежащее состояние.

2. Содержание функционирования системы обеспечения безопасности КВО ИКИ должно включать в себя следующие компоненты:

1) формирование системы обеспечения безопасности КВО ИКИ;
2) управление системой обеспечения безопасности КВО ИКИ.

Формирование системы обеспечения безопасности КВО ИКИ предполагает последовательную реализацию таких организационных мер, как:

- определение состава системы обеспечения безопасности КВО ИКИ;
- непосредственное создание данной системы.

Основываясь на сложившихся подходах в области обеспечения безопасности субъектов хозяйствования [24, с. 7–35], [24, 3–14, 47-62] и на результатах проведённого исследования [26, с. 94–100], в состав системы обеспечения безопасности КВО ИКИ должны входить следующие элементы:

- правовая основа, которую составляют правовые нормы, группирующиеся по следующим уровням:
  - ♦ конституционный уровень – нормы конституции государства, определяющие основные положения права собственности, обеспечения экологической безопасности, деятельности государственных органов по обеспечению прав и свобод личности;
  - ♦ базовый уровень – нормы специального законодательного акта в области обеспечения безопасности КВО ИКИ, определяющие: правовой статус таких объектов; субъектов государственного управления в этой области и их функции; систему и содержание мер обеспечения безопасности КВО ИКИ, порядок их применения и др.;
  - ♦ функциональный уровень – нормы законодательных актов, постановлений правительства государства, а также предписания нормативных правовых актов уполномоченных государственных органов и собственников (владельцев) КВО ИКИ, детализирующие вопросы реализации мер обеспечения безопасности данных объектов;
  - ♦ обеспечивающий уровень – нормы актов законодательства, непосредственно не регламентирующие обеспечение безопасности КВО ИКИ, но создающие условия по реализации мер обеспечения их безопасности и определяющие полномочия государственных органов и иных организаций по реализации таких мер;
  - ♦ технико-технологический уровень – нормы различных технических стандартов, регламентирующие правила строительства, техники безопасности, информационной безопасности, иные нормы технического регулирования;
  - ♦ объекты обеспечения безопасности КВО ИКИ, из числа которых в качестве основных необходимо рассматривать:
  - ♦ интересы государства и общества;
  - ♦ интересы предприятия (организации) производственного или социального назначения, отнесённого к КВО;
- субъекты обеспечения безопасности КВО ИКИ, к которым относятся:
  - ♦ работники объекта (в том числе, его службы безопасности, подразделения информационной безопасности и т.п.), которые реализуют меры обеспечения безопасности объекта, предусмотренные локальными нормативными правовыми актами;
  - ♦ сотрудники уполномоченных государственных органов и организаций (правоохранительных органов, органов безопасности, по чрезвычайным ситуациям и т.п.), которые реализуют меры обеспечения безопасности объекта в со-

ответствии со своей компетенцией, определённой актами законодательства;

- ♦ работники организаций, осуществляющие проектирование, монтаж, наладку и техническое обслуживание средств и систем охраны;
- ♦ иные лица, в установленном законодательством порядке уполномоченные осуществлять охрану и защиту КВО ИКИ (например, адвокаты, работники привлечённых аудиторских и иных организаций);

- система мер обеспечения безопасности КВО ИКИ, основными из которых являются:
  - ♦ правовые меры – положения законодательных актов в области безопасности КВО ИКИ, требования иных актов законодательства, в том числе технических нормативных правовых актов, а также действия уполномоченных субъектов обеспечения безопасности таких объектов по их реализации;
  - ♦ организационные меры – действия уполномоченных субъектов обеспечения безопасности КВО ИКИ, направленные на организацию и поддержание системы обеспечения безопасности таких объектов;
  - ♦ инженерно-технические меры – действия уполномоченных субъектов обеспечения безопасности КВО ИКИ, направленные на поддержание функционирования соответствующих объектов (их компонентов) в определенный промежуток времени в случае выхода из строя их критических и иных элементов, а также на создание и поддержание систем физической охраны таких объектов;
  - ♦ аппаратно-программные меры – действия уполномоченных субъектов обеспечения безопасности КВО ИКИ, направленные на защиту информационных активов таких объектов, обрабатываемых и (или) хранящихся в различных информационных системах либо в отдельных комплексах программно-технических средств;
  - ♦ специальные меры – действия уполномоченных субъектов обеспечения безопасности КВО ИКИ, направленные на предупреждение, выявление и локализацию угроз безопасности таким объектам, осуществление информационно-аналитической деятельности и физическую охрану работников объекта.

Целью системы обеспечения безопасности КВО ИКИ является обеспечение должного функционирования соответствующих объектов, в том числе, в случае реализации угроз его безопасности.

При обеспечении безопасности КВО ИКИ должен достигаться баланс интересов государства и общества и интересов собственников (владельцев) таких объектов.

Непосредственное создание системы обеспечения безопасности КВО ИКИ включает в себя следующую совокупность мероприятий [26, с. 271–272]:

- установление уровней обеспечения безопасности КВО ИКИ, которые подразделяются на следующие виды:
- общий уровень, на котором меры обеспечения безопасности таких объектов реализуется работниками всех его структурных подразделений, сотрудниками уполномоченных государственных органов и организаций, иными уполномоченными лицами;
- специальный уровень, на котором соответствующие меры реализуется работниками службы безопасности объекта;
- анализ, определение и моделирование угроз безопасности КВО ИКИ и инцидентов безопасности;
- проведение первоочередных мероприятий на КВО ИКИ, основными из которых являются разработка:
- концепции обеспечения информационной безопасности объекта;
- положения о службе безопасности объекта, подразделении информационной безопасности и т.п.;
- ежегодных планов мероприятий по обеспечению безопасности объекта;
- типовых планов повышенной готовности объекта к деятельности в условиях реализации угроз;
- типовых планов действий персонала объекта при реализации угроз его безопасности и возникновении инцидентов безопасности;
- типовых планов обеспечения безопасности КВО в особых условиях.

Угрозы безопасности КВО ИКИ составляют:

1) в зависимости от источника угроз:

- природные угрозы – опасные метеорологические и гидрологические явления, опасная сейсмическая активность, опасные уровни воды, раннее образование ледостава и появление льда, пожары, иные природные явления, могущие привести к нарушению (прекращению) функционирования таких объектов или их критических элементов;
- техногенные угрозы – аварии, отказы или повреждения критических элементов рассматриваемых объектов или технических устройств на иных объектах, обеспечивающих безопасное функционирование КВО ИКИ, нарушения производственных процессов на КВО ИКИ, которые могут вызвать инциденты безопасности, иные техногенные инциденты, могущие привести к нарушению (прекращению) функционирования таких объектов;
- социальные угрозы – экстремистские, террористические или диверсионные проявления (акты), компьютерные атаки, а также иные противоправные действия в отношении КВО ИКИ, их критических

элементов и (или) их работников, недостаточные производственная дисциплина и профессиональная подготовка работников рассматриваемых объектов, иные социальные проявления, могущие привести к нарушению (прекращению) их функционирования;

2) в зависимости от сферы проявления:

- внешние угрозы – природные угрозы, а также техногенные и социальные угрозы, не связанные с деятельностью КВО ИКИ или их работников;
- внутренние угрозы – техногенные и социальные угрозы, связанные с деятельностью КВО ИКИ или их работников.

Инцидент безопасности КВО ИКИ – произошедшие в результате реализации угрозы безопасности такого объекта нарушение (прекращение) его функционирования, а также нарушение законодательства в области безопасности КВО ИКИ.

Управление системой обеспечения безопасности КВО ИКИ предусматривает последовательную реализацию следующих мер [26, с. 271]:

1) организация функционирования системы обеспечения безопасности таких объектов;
2) поддержание заданного уровня охраны и защиты этих объектов.

Организацию функционирования системы обеспечения безопасности КВО ИКИ, как элемент управления ею, необходимо рассматривать с двух сторон:

- как организационный процесс, который включает следующие стадии:
- поддержание и развитие управления системой обеспечения безопасности КВО ИКИ во всех подразделениях объекта;
- определение и поддержка исполнителей, реализующих меры обеспечения безопасности КВО ИКИ, а также оценка их деятельности;
- планирование, контроль и подведение итогов деятельности по обеспечению безопасности КВО ИКИ;
- как технологический процесс, который состоит из:
- подготовки и принятия управленческих решений в области обеспечения безопасности КВО ИКИ;
- реализации принятых управленческих решений;
- оценки реализованных решений.

Соответственно, управление системой обеспечения безопасности КВО ИКИ предусматривает совокупность организованных действий руководства объекта и его службы безопасности, обеспечивающих согласованную реализацию всеми заинтересованными субъектами соответствующих мер в целях охраны и защиты КВО ИКИ от внутренних и внешних угроз. Такое управление направлено на организацию непрерывного процесса поддержания заданного уровня охраны и защиты КВО ИКИ и должно обеспечивать своевременное, строгое и точное выполнение всеми субъектами мер обеспечения безопасности объекта, в том числе в случае возникновения инцидентов безопасности.

Поддержание заданного уровня охраны и защиты КВО ИКИ целесообразно рассматривать как деятельность, в рамках которой проводятся следующие мероприятия:

- оценка достаточности реализуемых мер обеспечения безопасности КВО ИКИ;
- определение и введение на КВО ИКИ соответствующих режимов функционирования:
- повседневный режим – действует на объекте, когда угрозы его безопасности отсутствуют;
- режим повышенной готовности – вводится на объекте в случае возникновения угроз его безопасности;
- чрезвычайный режим – вводится на объекте в случае реализации угроз его безопасности и возникновения инцидентов безопасности;
- определения порядка введения в действие соответствующих типовых планов;
- определение порядка взаимодействия с уполномоченными государственными органами и организаций, иными субъектами обеспечения безопасности КВО ИКИ.
- Как и при формировании и обеспечении безопасного функционирования системы КВО ИКИ, так и при обеспечении их безопасности все субъекты, осуществляющие деятельность в этой сфере (собственники (владельцы) таких объектов, уполномоченные государственные органы, привлекаемые юридические и физические лица) должны действовать в пределах своей компетенции, которую составляют следующие элементы.

1. Задачи, то есть отдельные положения, которые в силу своей особой значимости требуют безусловного исполнения их заинтересованными предприятиями, организациями, государственными органами, иными юридическими и физическими лицами.

Основными задачами обеспечения безопасного функционирования КВО ИКИ являются:

- создание условий для осуществления уставной деятельности (технологического процесса) такого объекта;
- поддержание штатного функционирования КВО ИКИ;
- осуществление контроля за надлежащим соблюдением работниками КВО ИКИ правил и требований их безопасного функционирования.

Основными задачами обеспечения безопасности КВО ИКИ являются:

- выявление и ликвидация угроз безопасному функционированию такого объекта;
- поддержание функционирования КВО ИКИ или его критического элемента постоянно или опреде-

ленный промежуток времени в случае реализации угроз его безопасности;

- полное или частичное возмещение вреда, причиненного интересам государства и общества, интересам объекта в результате нарушения (прекращения) его функционирования.

2. Объём полномочий таких субъектов и их работников и сотрудников, то есть совокупность их прав и обязанностей, обеспечивающих возможность решения установленных задач.

Основными полномочиями уполномоченных субъектов, реализуемыми ими в пределах их компетенции при обеспечении безопасного функционирования КВО ИКИ, являются:

- разработка и реализация мероприятий по обеспечению безопасного функционирования таких объектов;
- осуществление государственного контроля и (или) надзора в области безопасного функционирования КВО ИКИ;
- предоставление по требованию уполномоченных государственных органов в области безопасности КВО ИКИ имеющейся информации по вопросам функционирования данных объектов;
- по требованию уполномоченных государственных органов в области безопасности КВО ИКИ оказание им необходимой помощи в реализации мер обеспечения безопасного функционирования КВО ИКИ.

При обеспечении безопасности КВО ИКИ уполномоченные субъекты в пределах своей компетенции обладают следующими полномочиями:

- реализовывать необходимые правовые, организационные, инженерно-технические, аппаратно-программные, специальные и иные меры обеспечения безопасности КВО ИКИ;
- создавать подразделения по охране и защите таких объектов (службы безопасности, подразделения информационной безопасности и т.п.);
- самостоятельно определять формы и методы охраны и защиты этих объектов;
- приостанавливать эксплуатацию КВО ИКИ или его критических элементов самостоятельно или по предписанию уполномоченного государственного органа в области безопасности КВО ИКИ или его должностных лиц в случае инцидента безопасности, а также в случае обнаружения вновь открывшихся обстоятельств, влияющих на безопасное функционирование таких объектов.

3. Подведомственность, которая определяет сферу реализации полномочий заинтересованными юридическими и физическими лицами.

Подведомственность уполномоченных субъектов в области безопасности КВО ИКИ распределяется в зависимости от задач, которые они решают:

1) собственники (владельцы) реализуют свои полномочия исключительно в отношении КВО ИКИ, принадлежащих им (которыми они владеют);

2) уполномоченные государственные органы в области безопасности КВО ИКИ реализуют полномочия по двум направлениям:

- при осуществлении и (или) надзора в области безопасного функционирования таких объектов;
- при реализации функции обеспечения безопасности этих объектов;

3) привлекаемые юридические и физические лица реализуют полномочия при осуществлении вспомогательных функций в области обеспечения безопасного функционирования и обеспечения безопасности КВО ИКИ (например, адвокаты, работники привлечённых аудиторских организаций или коммерческих организаций, специализирующихся на оказании услуг по наладке охранных систем, и т.п.).

Для снижения уровня угроз безопасности КВО ИКИ создается государственная система реагирования на инциденты безопасности таких объектов.

В рамках этой системы наиболее эффективным является создание Национального центра реагирования на инциденты безопасности КВО ИКИ (далее – НЦРИБ). В состав такого центра должен входить Национальный центр реагирования на компьютерные инциденты. Порядок НЦРБИ определяется уполномоченным государственным органом в области обеспечения безопасности КВО ИКИ.

В случае возникновения инцидента безопасности КВО ИКИ вводится режим чрезвычайной ситуации и реализуется типовой план действий работников такого объекта при возникновении инцидентов безопасности.

В рамках режима чрезвычайной ситуации работники КВО ИКИ реализуют соответствующие меры безопасности, направленные на ликвидацию инцидентов безопасности и поддержание функционирования объекта.

Для установления причин и условий возникновения инцидентов безопасности, выработки мер по недопущению их повторного возникновения проводится расследование инцидентов безопасности. Расследование инцидентов безопасности проводится в соответствии с положениями действующего законодательства государства.

О возникновении инцидента безопасности КВО ИКИ, его последствиях, принятых мерах и результатах расследования информируется НЦРБИ.

Конкретный перечень сведений, подлежащих представлению в НЦРБИ, и порядок их предоставления устанавливает уполномоченный государственный орган в области обеспечения безопасности КВО ИКИ.

Сведения, содержащиеся в государственной системе реагирования на инциденты безопасности КВО ИКИ, относятся к информации ограниченного распространения. Порядок доступа к сведениям, содержащимся в такой госу-

дарственной системе, определяется уполномоченным государственным органом в области безопасности КВО ИКИ.

Изложенное позволяет сделать следующие выводы.

1. Проблема формирование системы КВО ИКИ, обеспечение её безопасного функционирования и безопасности указанных объектов является важной и актуальной в современный период.

При этом в области безопасности КВО ИКИ необходимо выделять два тесно взаимосвязанных, но разных по своему содержанию направления:

1) формирование и обеспечение безопасного функционирования системы КВО ИКИ;
2) обеспечение безопасности КВО ИКИ.

2. Формирование и обеспечение безопасного функционирования системы КВО ИКИ должно включать в себя следующие этапы:

1 этап: выделение в социально-экономической инфраструктуре государстве отраслевой ИКИ;

2 этап: определение признаков критичности ИКИ;

3 этап: выделение из числа критических инфраструктур государства критической ИКИ;

4 этап: определение основного критерия выделения КВО в ИКИ;

5 этап: выделение КВО в КОИ;

6 этап: определение отраслевых критериев категорирования КВО в ИКИ;

7 этап: категорирование КВО в КОИ;

8 этап: определение требований к обеспечению безопасного функционирования КВО с учётом специфики ИКИ и его категории;

9 этап: проверка деятельности КВО ИКИ на соответствие требованиям к обеспечению его безопасного функционирования;

10 этап: приведение деятельности КВО ИКИ в соответствие с требованиями к обеспечению его безопасного функционирования.

3. Функционирование системы обеспечения безопасности КВО ИКИ включает в себя следующие компоненты:

1) формирование системы обеспечения безопасности КВО ИКИ;
2) управление системой обеспечения безопасности КВО ИКИ.

Содержание компонентного состава функционирования системы обеспечения безопасности КВО ИКИ отражает последовательную реализацию соответствующих организационных мер:

1) в процессе формирования системы обеспечения безопасности КВО ИКИ:
   - определение состава системы обеспечения безопасности КВО ИКИ;
   - непосредственное создание данной системы;

2) при управлении системой обеспечения безопасности КВО ИКИ:
   - организация функционирования системы обеспечения безопасности КВО ИКИ;
   - поддержание заданного уровня охраны и защиты КВО ИКИ.

4. Все компоненты формирования системы КВО ИКИ, обеспечения её безопасного функционирования и безопасности указанных объектов должны найти своё закрепление в законодательных и подзаконных нормативных правовых актах, а также в локальных актах КВО ИКИ.

Список литературы:

1. **Барановский О.К.** Актуальные вопросы технической защиты информации в системах физической защиты объектов критической инфраструктуры // Технологии безопасности. – 2012. – № 3. – С. 39-40.
2. **Козлитин А.М.** Развитие теории и методов оценки рисков для обеспечения промышленной безопасности объектов нефтегазового комплекса: автореф. дис. ... д–ра. тех. наук: 05.26.03; Уфим. гос. нефтяной техн. ун-т. – Уфа, 2006. – 44 с.
3. **Черешкин Д.С. и др.** Концепция категорирования потенциально опасных объектов национальной транспортной инфраструктуры // Труды Ин-та систем. анализа Рос. Академии Наук. – 2007. – Т. 31. – С. 5–20.
4. **Косицин И.А.** Правовые и организационные основы охраны особо важных объектов подразделениями вневедомственной охраны при органах внутренних дел: автореф. дис. ... канд. юрид. наук: 12.00.14; Омск. Акад. МВД Рос. Федерации. – Омск, 2001. – 19 с.
5. **Кузьмин В.В.** Правовое регулирование защиты критически важных для национальной безопасности объектов инфраструктуры населения страны от угроз техногенного и природного характера: дис. ... канд. юрид. наук: 05.26.02 ; С.-Петерб. гос. ун-т ГПС МЧС России. – СПб, 2009. – 127 с.
6. **Моторный И.Д.** Современный терроризм и оценка диверсионно-террористической уязвимости гражданских объектов: монография. – М.: Изд-ль Шумилова И.И., 2004. – 106 с.
7. **Наумович Л.В., Кучинский П.В.** Роль информационной составляющей критически важных объектов в обеспечении национальной безопасности // ЭлектроникаИнфо. – 2012. – № 2. – С. 102-104.
8. **Трофименко Ю.В. и др.**Обеспечение защищённости автомобильных мостов от актов незаконного вмешательства: учеб. пособие; под. ред. Ю.В. Трофименко. – М.: МАДИ, 2014. – 172 с.
9. **Полякова Т.А.** Правовое обеспечение информационной безопасности при построении информационного общества в России: дис. ... д–ра. юрид. наук: 12.00.14; Рос. правовая акад. Мин. юст. Рос. Федерации. – М., 2008. – 438 с.
10. **Вус М.А., Кучерявый М.М., Шакин Д.Н.** Методологические проблемы обеспечения информационной

безопасности критически важных объектов топливно-энергетического комплекса Российской Федерации// Информатизация и связь. – 2012. – № 7. – С. 42-47.

11. **Гражданкин А.И.** Критически важные для национальной безопасности опасные производственные объекты. Показатели, критерии и порядок их категорирования // Безопасность труда в промышленности. – 2005. – № 5. – С. 46-48.
12. **Пучков В.А. и др.** Использование категорирования в обеспечении безопасности критических инфраструктур национального масштаба // Труды Ин-та систем. анализа Рос. Академии Наук. – 2009. – Т. 41. – С. 6–13.
13. **Назаркин М.В.** Теоретические и прикладные проблемы обеспечения безопасности высокорисковых объектов: монография – М.: Всерос. науч.-исслед. ин-т МВД России, 2009. – 260 с.
14. **Мелех О.В., Максимович Е.П., Фисенко В.К.** Классификация критически важных объектов информатизации по требованиям физической защиты с использованием методов кластерного анализа // Искусственный интеллект. – 2010. – № 4. – С. 666–677.
15. **Панин О.** Категорирование объектов для создания эффективных систем физической защиты // Безопасность. Достоверность. Информация. – 2007. – № 1(70). – С. 20-24.
16. **Юдин Г.Г.** Правовые и организационные основы обеспечения безопасности потенциально важных объектов: теория и практика: автореф. дис. ... канд. юрид. наук: 12.00.11; Акад. упр. МВД Рос. Федерации. – М., 2009. – 22 с.
17. Модельный закон об основах регулирования Интернета: Постановление Межпарламентской Ассамблеи государств – участников СНГ, 16 мая 2011 г., № 36-9 // Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. – 2011. – № 51. – С. 191 – 198.
18. Актуальные направления совершенствования государственного управления и повышения эффективности работы государственных органов по противодействию терроризму и обеспечению информационной безопасности в Республике Беларусь. Задание 3. (шифр «Антитеррор-КВО»): отчёт о НИР по Государственной программе на 2011–2013 гг. «Научное обеспечение повышения эффективности работы государственных органов по укреплению обороноспособности и безопасности Республики Беларусь, уровня национальной безопасности и защищенности населения и территорий от чрезвычайных ситуаций природного и техногенного характера (ГПНИ «Научное обеспечение безопасности и защиты от чрезвычайных ситуаций»)» (заключ.): в 3 ч. / С.В. Матусевич, С.А. Михалёнок, Д.В. Перевалов, Д.В. Титлов, А.А. Тепляков / Ин-т нац. безопасности Респ. Беларусь; рук. задания Д.В. Перевалов. – Минск, 2013. – Ч. 3: «Антитеррор-КВО». – Ч. 1: Основные результаты. – 200 с. – Инв. № 111920.
19. О принятии технических регламентов Таможенного союза «О безопасности железнодорожного подвижного состава», «О безопасности высокоскоростного железнодорожного транспорта» и «О безопасности инфраструктуры железнодорожного транспорта»: Решение Комиссии Таможенного союза, 15 июля 2011 г., № 710 // Консультант Плюс: Беларусь. Технология 3000 [Электронный ресурс] / ООО «ЮрСпектр». – Минск, 2014.
20. О безопасности гидротехнических сооружений: федер. закон Рос. Федерации, 21 июля 1997 г., № 117-ФЗ // Собрание законодательства РФ. – 1997. – № 30. – Ст. 3589.
21. Методический подход к отнесению объектов к категории критически важных. – М.: ФГУ ВНИИ ГОЧС (ФЦ) МЧС России, 2006. – 50 с.
22. Модельный закон о промышленной безопасности опасных производственных объектов: Постановление Межпарламентской Ассамблеи государств – участников СНГ, 06 дек. 1997 г., № 10-5 // Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. – 1998. – № 16. – С. 90 – 108.
23. Модельный уголовный кодекс для государств – участников Содружества Независимых Государств: Постановление Межпарламентской Ассамблеи государств – участников СНГ, 17 февр. 1996 г., № 7-5 // Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. – 1996. – № 10. – Приложение.
24. **Ярочкин В.И.** Система безопасности фирмы /М.: Ось 89, 2003. – 352 с.
25. **Мак-Мак В.П.** Служба безопасности предприятия. Организационно-управленческие и правовые аспекты деятельности /М.: «Мир безопасности», 1999. – 160 с.
26. **Матусевич С.В., Михаленок С.А., Перевалов Д.В., Тепляков А.А., Титлов Д.В. под руководством Перевалова Д.В.** Актуальные направления совершенствования государственного управления и повышения эффективности работы государственных органов по противодействию терроризму и обеспечению информационной безопасности в Республике Беларусь. Задание 3. (шифр «Антитеррор-КВО»): отчёт о НИР по Государственной программе на 2011-2013 гг. «Научное обеспечение повышения эффективности работы государственных органов по укреплению обороноспособности и безопасности Республики Беларусь, уровня национальной безопасности и защищенности населения и территорий от чрезвычайных ситуаций природного и техногенного характера (ГПНИ «Научное обеспечение безопасности и защиты от чрезвычайных ситуаций»)» (заключительный): в 3 ч.– Минск, 2013. – 677 с. – Инв. №№ 111920, 111921, 112174.

УДК 342.9; 351.7

О НЕКОТОРЫХ АСПЕКТАХ РАЗРАБОТКИ И РЕАЛИЗАЦИИ АДМИНИСТРАТИВНЫХ РЕГЛАМЕНТОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.Н. Лепёхин

Современные вызовы и угрозы предопределяют обеспечение информационной безопасности важной стратегической задачей государства, интересы которого предполагают реализацию механизмов защиты от внутренних и внешних угроз различных объектов информационно-коммуникационной инфраструктуры и, в первую очередь, объектов, отнесенных к критически важным.

В сфере информатизации к критически важным объектам относят объекты:

- осуществляющие функции информационной системы, нарушение (прекращение) функционирования которой может привести к значительным негативным последствиям для национальной безопасности в политической, экономической, социальной, информационной, экологической, иных сферах;
- обеспечивающие предоставление значительного объема информационных услуг, частичное или полное прекращение оказания которых может привести к значительным негативным последствиям для национальной безопасности в политической, экономической, социальной, информационной, экологической, иных сферах.

Основным критерием отнесения объекта информационно-коммуникационной инфраструктуры к критически важному является уровень возможных последствий нарушения (прекращения) его функционирования:

- утрата государственного управления страной или административно-территориальной единицей;
- потеря управления экономикой страны или административно-территориальной единицы;
- необратимое негативное изменение (или разрушение) государственного управления или экономики страны или административно-территориальной единицы;
- существенное снижение безопасности жизнедеятельности населения, проживающего на территории административно-территориальной единицы или страны, на длительный период времени.

Наличие в любом государстве критически важных объектов информатизации обуславливает разработку определенных регламентов административных процедур, осуществляемых уполномоченными органами в сфере обеспечения информационной безопасности государства для упорядочения деятельности государственных органов и заинтересованных субъектов в данной сфере. Указанная работа проводится и в рамках Содружества Независимых Государств, в рамках разработки модельного регламента административных процедур.

При подготовке проекта регламента непосредственно использованы основополагающие положения принятых ранее Модельного информационного кодекса для государств – участников СНГ, модельных законов «Об информации, информатизации и защите информации» «О международном информационном обмене», Рекомендаций по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности, и разрабатываемого проекта модельного закона «О критически важных объектах информационно-коммуникационной инфраструктуры», а также учтены 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 России 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».

Разработка проекта регламента осуществлялась параллельно с разработкой проекта модельного закона «О критически важных объектах информационно-коммуникационной инфраструктуры», Стратегии обеспечения информационной безопасности государств – участников СНГ и ряда проектов других модельных актов в данной сфере. В связи с этим проект регламента должен стать составной частью целостного пакета концептуальных и нормативно-правовых предложений в сфере обеспечения информационной безопасности государств – участников СНГ.

Основной целью разработки модельного регламента являлось формирование механизма реализации полномочий государственных органов, прав и законных интересов заинтересованных субъектов в сфере эксплуатации критически важных объектов в рамках обеспечения информационной безопасности и нормального функционирования критически важных объектов информационно-коммуникационной инфраструктуры.

Основными задачами при этом являются:

- установление единого подхода к перечню административных процедур и уровней их реализации с учетом основных положений законодательства в области безопасности критически важных объектов информационно-коммуникационной инфраструктур государств – участников СНГ;
- формирование общего перечня (для государств – участников СНГ) документов и (или) сведений, представляемых в уполномоченный орган для осуществления административной процедуры;
- выработка механизма реализации административных процедур с учетом требований законодательства о критически важных объектах и особенностей информационно-коммуникационной инфраструктуры в государствах – участниках СНГ;
- разработка единой и скоординированной системы правовых, организационных, инженерно-технических, программно-аппаратных и специальных мер обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры в государствах – участниках СНГ, обеспечивающей безопасный ввод в эксплуатацию, безопасную эксплуатацию и безопасный вывод из эксплуатации соответствующих объектов;
- определение органа, уполномоченного на проведение административной процедуры и сроков ее осуществления.

Предметом правового регулирования в рамках рассматриваемого проекта регламента являются правовые и организационно-управленческие отношения, связанные формированием механизма реализации полномочий государственных органов, а также прав и законных интересов заинтересованных субъектов в сфере эксплуатации критически важных объектов.

Необходимость разработки проекта регламента обусловлена, во-первых, ростом числа критически важных объектов в системе объектов информационно-коммуникационной инфраструктуры государств – участников СНГ; во-вторых, целесообразностью разработки механизма реализаций полномочий государственных органов и заинтересованных субъектов в данной сфере; в-третьих, отсутствием в большинстве государств – участников СНГ нормативно закреплённых основ деятельности по обеспечению нормального функционирования критически важных объектам информационно-коммуникационной инфраструктуры; в-четвертых, важностью установления общих подходов к содержанию административных процедур, перечню органов их осуществляющих и ожидаемых результатов их реализации.

Таким образом, принятие проекта регламента позволит создать эффективный организационно-правовой механизм реализации полномочий государственных органов в сфере эксплуатации критически важных объектов, обеспечивающий формирование и развитие системы обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры, направленный на:

- согласование единых подходов по разработке перечня административных процедур и их содержания;
- определение компетентных государственных органов уполномоченных на реализацию административных процедур в сфере обеспечения информационной безопасности государств-участников СНГ;
- гармонизацию национальных законов и нормативных актов в области информационной

безопасности в целях формирования единого информационного пространства и расширения интеграции государств – участников СНГ в данной сфере.

Список литературы:

1. Закон Республики Беларусь от 28.10.2008 № 433-З (ред. от 13.07.2012) «Об основах административных процедур».
2. Указ Президента Республики Беларусь от 26.04.2010 № 200 (ред. от 24.07.2014) «Об административных процедурах, осуществляемых государственными органами и иными организациями по заявлениям граждан».
3. Постановление Правительства РФ от 16.05.2011 № 373 (ред. от 23.01.2014) «О разработке и утверждении административных регламентов исполнения государственных функций и административных регламентов предоставления государственных услуг».
4. Постановление Правительства РФ от 19.01.2005 № 30 (ред. от 06.09.2012) «О Типовом регламенте взаимодействия федеральных органов исполнительной власти».
5. **Лепёхин А.Н** К вопросу предупреждения использования открытых телекоммуникационных систем в террористических и иных противоправных целях / Вус М.А., Лепёхин А.Н., Перевалов Д.В. // Информатизация и связь. 2013, № 1. С.22-25.
6. **Душакова Л.А.** Некоторые аспекты правового регулирования государственных услуг // Вестник Пермского университета. Юридические науки. Выпуск № 2 / 2011 С.106-109.
7. **Яцкин А.В.** Правовое регулирование разработки административных регламентов // Журнал рос. Права.2006.№10 С.3-17.

УДК 004.056

ПОДХОДЫ К ОЦЕНКЕ УЯЗВИМОСТЕЙ И УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ НА ПРИМЕРЕ НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЫ

М.М. Кучерявый, И.И. Лившиц

Введение

В статье рассматриваются угрозы НПС на примере характерного критичного инцидента – прерывания обслуживания российских банков платежными системами Visa и MasterCard в 2014 г. Логичной реакцией на этот инцидент стало принятие Федерального закона о создании Национальной системы платежных карт с целью поддержания бесперебойности денежных переводов и гарантии их безопасности [1], и расширение сферы уже действовавшего ранее Федерального закона «О национальной платежной системе»[2].

В Российской Федерации хорошо известны требования современных международных стандартов ISO серии 27000 (системы менеджмента информационной безопасности, СМИБ) – актуальные версии стандартов требования [3], управления рисками [4] и словарь [5]. Необходимо отметить, что ряд стандартов ISO в Российской Федерации приняты в аутентичных ГОСТ Р содержательных трактовках, например ГОСТ Р ИСО/МЭК 27001-2006. Соответственно, представляется полезным провести краткий анализ рисков НПС (с учетом известных угроз и уязвимостей) и проанализировать меры, которые могут быть предприняты для исключения повторения подобных инцидентов в будущем или существенного «смягчения» негативных последствий в том случае, если внешние факторы риска снова проявятся. Анализ рисков предлагается выполнить на основании современной методической базы: международных стандартов ISO [3 – 5] и стандартов БР ИББС версии 2014 г. [6, 7].

Актуальные стандарты ISO серии 27000

На дату подготовки публикации действует система стандартов ISO серии 27000 [5]:

- **Требования** (см. стандарт [5] п. 4.3), например ISO/IEC 27001 Information security management systems — Requirements [3];
- **Основные руководства** (см. [5] п. 4.4), например, ISO/IEC 27005 Information security risk management [4];
- **Руководства для определенных отраслей** (см. [5] п. 4.5), например, ISO/IEC TR 27015 Information security management guidelines for financial services.

Для целей данной публикации будут приняты во внимание 3 основные стандарта ISO серии 27000 [3 – 5], необходимые для правильного проектирования, создания и оценки СМИБ. Тем не менее, при формировании требований, разработке, внедрении и оценки реальных СМИБ (или адекватных моделей СМИБ) рекомендуется применять соответствующие отраслевые руководства, в том числе и с целью создания интегрированных систем менеджмента [8 – 9].

Актуальные стандарты комплекса БР ИББС

Распоряжением Банка России от 17.05.2014 № Р-399 с 1 июня 2014 г. введены 5-я редакция стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014 [6] и 4-я редакция стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014» СТО БР ИББС-1.2-2014 [7].

Отметим ряд необходимых в контексте данной публикации терминов и определений в стандарте [6] и обратим внимание на применимость использования этих терминов:

- «**Оценка риска нарушения информационной безопасности**» (3.53). Данный термин встречается только в разделе 3 («Термины и определения»), но далее в процессах анализа ИБ и обеспечения ИБ в ЖЦ, во всех фазах цикла PDCA в стандарте не встречается.
- «**План работ по обеспечению информационной безопасности»** (3.58). Данный термин встречается только в разделе 3 («Термины и определения»), далее в процессах анализа ИБ и обеспечения ИБ в ЖЦ, во всех фазах цикла PDCA в стандарте не встречается.
- «**Аудит информационной безопасности; аудит ИБ**» (3.64). Данный термин встречается в разделах 8 («СМИБ») и 9 («Проверка и оценка ИБ организаций БС»). Стандарт устанавливает в п. 8.1.4 требования только в фазе «Проверка» цикла PDCA, но не упоминает предшествующие 2 фазы цикла – «Планируй» и «Делай».

Далее необходимо рассмотреть перечень требований стандарта [6] к СИБ в аспекте определения модели угроз по основным (для целей рассматриваемой публикации) областям. Можно выделить общие требования:

1. по обеспечению ИБ АБС на стадиях ЖЦ (п. 7.3):
   - Выполнение работ на всех стадиях ЖЦ АБС в части вопросов обеспечения ИБ должно осуществляться по согласованию и под контролем службы ИБ (7.3.2);
   - На стадии эксплуатации АБС должны быть определены, выполняться, регистрироваться и контролироваться процедуры, необходимые для обеспечения восстановления всех реализованных функций по обеспечению ИБ (7.3.10).
2. по обеспечению ИБ платежных технологических процессов (п. 7.8.):
   - Должны быть определены, выполняться, регистрироваться и контролироваться процедуры восстановления всех реализованных программно-техническими средствами функций по обеспечению ИБ платежной информации (7.8.11).

Для результативного процесса оценки рисков (на примере НПС) важно определить численные показатели ИБ (метрики), которые позволят оценить количественно текущий уровень обеспечения ИБ, соответственно, дополнительно рассмотрены некоторые показатели ИБ, приведенные в стандарте [7]. Например, в Таблице 4 (СИБ) установлено соответствие:

- для структурного элемента СТО БР ИББС-1.0 (п. 7.3) – групповой показатель ИБ М2 «Обеспечение ИБ на стадиях жизненного цикла АБС», для этого показателя в Приложении Б даны примеры метрик, например М 2.2 – М 2.11 (бесперебойность).
- для структурного элемента СТО БР ИББС-1.0 (п. 7.8) установлено соответствие – групповой показатель М7 «Обеспечение ИБ банковских платежных технологических процессов», для этого показателя в Приложении Б даны примеры метрик, например М 7.6 – М 7.22 (защита от искажений, фальсификации и уничтожения).

Анализ угроз и уязвимостей в соответствии с требованиями ISO

Из приведенного выше краткого анализа требований современного комплекса БР ИББС очевидно, что содержащиеся требования в стандарте [6] и, соответствующие показатели ИБ, приведенные в стандарте [6] не в полной

Таблица 1.

Перечень уязвимостей и угроз НПС в соответствии с ISO/IEC 27005:2011

Уязвимость	Угроза	Категория	Примечания
Единичная точка отказа	Отказ телекоммуникационного оборудования	Категория D (преднамеренно)	Область вне разумного контроля регуляторов РФ
Изъяны планов непрерывности			
Потеря необходимых сервисов			
Нехватка процедур выявления риска и оценки	Злоупотребление правами		Область возможного контроля регуляторов РФ
Недостатки в контрактах третьих лиц			

мере содержат методики обеспечения ИБ для НПС. Причин сложившегося положения несколько: – субъектный состав НПС значительно шире области применения комплекса БР ИББС, не полностью реализована поддержка цикла PDCA применительно к СМИБ, функционально ограниченная оценка риска нарушения ИБ. Соответственно, для целей достоверного, точного, воспроизводимого и объективного анализа угроз и уязвимостей НПС необходимо дополнительно применять требования стандартов ISO серии 27000 [3 – 5].

Анализ угроз и уязвимостей НПС предлагается провести с точном соответствии с методикой, изложенной в стандарте [4], рассматривая для формирования перечня угроз приложение «**C**», а для формирования перечня уязвимостей – приложение «**D**». Фрагмент анализа НПС для 2 наиболее явно проявившихся угроз и уязвимостей представлен в Таблице 1.

Дополнительно должен быть принят во внимание комплекс угроз касательно возможности приостановления технической поддержки со стороны крупнейших зарубежных ИТ-поставщиков (Oracle, HP и IBM) [10, 11]. На уровне Банка России эта угроза получила подтверждение (например, возможность отзыва лицензий на ПО), как отметил заместитель начальника главного управления безопасности и защиты информации ЦБ Артем Сычев. По данным ряда экспертов, доля зарубежного ПО в российских банках высока – в Сбербанке она составляет примерно 50%, в ВТБ – до 40%, в Промсвязьбанке около 30% [10]. В тоже время, требования современного бизнеса к ИБ постоянно изменяются, и как подтверждение этого факта инициировано очередное изменение Федерального закона «О национальной платежной системе» [1], в частности, предполагается, что будет изменена норма закона об обеспечительных взносах в ЦБ и конкретика о размере депозитов, сроках их перечисления и пр. Также опубликована информация на портале Cnews о «санкционных» распоряжениях президента США и приостановке работы Red Hat над проектами в 20 российских компаниях.

Оценка результативности СМИБ для НПС

На основании анализа угроз и уязвимостей на базе стандартов ISO серии 27000 возможно предложить способ оценки результативности СМИБ для НПС. Данный способ ориентирован на формирование численных оценок, которые могут быть сопоставлены с заранее заданным «эталонным» уровнем (**baseline**) и основан на иерархической структуре требований к СМИБ (для упрощения может применяться модель СМИБ), предоставлять возможность оценки как отдельных подсистем СМИБ, так и общей оценки результативности СМИБ с учетом весовых коэффициентов (уровня значимости) [9, 12]. Отметим, что уровни значимости (весовые коэффициенты) предполагается определять экспертным методом с использованием известного и хорошо зарекомендовавшего метода анализа иерархии (МАИ), предложенного Т. Саати. Важно, что МАИ позволяет выполнять не только статическую оценку, но и моделирование на основании динамических функций [9]. Данный способ может быть применим при проведении любого типа аудитов СМИБ, в частности – внутренних (аудиты 1-й стороной) и внешних (аудиты 2-й и 3-й стороной).

Предложенный способ использует количественные метрики оценки результативности СМИБ с целью представления этой оценки (равно как и представление оценок при моделировании – в хронологическом порядке) для анализа со стороны руководства с установленной периодичностью и планирования мероприятий по постоянному улучшению СМИБ. В модели используются следующие шкалы зрелости СМИБ (Таблица 2).

Общая оценка результативности СМИБ определяется по формуле (1):

$$P_{СМИБ} = \prod_{i=1}^{i=k_{ПС}} \alpha_i P_{ПС\ i} \qquad (1)$$

где:

$P_{СМИБ}$ – Общая оценка результативности модели СМИБ

$P_{ПС\ i}$ – Оценка результативности *i*-подсистемы в модели СМИБ

Таблица 2.

Шкалы зрелости

№	Уровень	Описание зрелости СМИБ	Основные характеристики СМИБ	Значение $P_{СМИБ}$
	Уровень 0	СМИБ отсутствует	Реализация отдельных требований	$0{,}1 \geq P_{СМИБ} > 0$
	Уровень 1	Определенная СМИБ	Реализация всех требований СМИБ документирована	$0{,}25 \geq P_{СМИБ} > 0{,}1$
	Уровень 2	Управляемая СМИБ	СМИБ документирована Поддерживается цикл PDCA	$0{,}5 \geq P_{СМИБ} > 0{,}25$
	Уровень 3	Установленная СМИБ	Реализация всех требований СМИБ сертифицирована	$0{,}75 \geq P_{СМИБ} > 0{,}5$
	Уровень 4	Предсказуемая СМИБ	СМИБ сертифицирована Управление по целям	$0{,}8 \geq P_{СМИБ} > 0{,}75$
	Уровень 5	Оптимизируемая СМИБ	СМИБ прошла несколько циклов сертификации Определены цели улучшения Управление эффективностью	$P_{СМИБ} > 0{,}8$

Таблица 3.

Перечень подсистем СМИБ

Код подсистемы	Описание подсистем оценки	Разделы ISO 27001
	Исполнение требований внешних нормативных документов	4.1, A.18
	Исполнение требований внутренних нормативных документов	4.1, 7.5, A.5, A.6
	Исполнение требований к обеспечению ИБ основных процессов	8, A.12, A.14, A.15
	Исполнение требований постоянного улучшения	10.2
	Исполнение требований к аудитам	9.2
	Исполнение требований корректирующих действий	10.1
	Исполнение требований анализа со стороны высшего руководства	9.3
	Исполнение требований по целям	6.2, 8.1
	Исполнение требований к персоналу	5.1, 7.2, 7.3, 7.4, A.7

$k_{пс}$ – Количество подсистем в модели СМИБ

α_i – весовой коэффициент *i*-подсистемы в модели СМИБ

В модели используются 9 функциональных подсистем СМИБ, выбор которых основан на требованиях стандарта [3], определенными ограничениями МАИ [9] и практикой выполненных проектов [8, 12] (Таблица 3).

Оценка результативности каждой подсистемы в СМИБ определяется по формуле (2):

$$P_{ПС\ i} = \prod_{j=1}^{j=m_{ИБ}} \beta_j M_{ИБ\ j}$$

где:

$P_{ПС\ j}$ – Оценка результативности *i* - подсистемы в модели СМИБ

$m_{ИБ}$ – Количество метрик ИБ, учитываемых в *i* - подсистеме модели СМИБ

$M_{ИБ\ j}$ – Метрика ИБ, учитываемая в *i* - подсистеме в модели СМИБ

β_i – весовой коэффициент *j* - метрики ИБ, учитываемой в *i* - подсистеме модели СМИБ

В модели используется иерархическая структура СМИБ, которая позволяет гибко формировать (изменять) состав и количество метрик ИБ, учитываемых при оценке результативности каждой подсистемы в модели СМИБ. Пример формирования перечня метрик ИБ для подсистемы 3 представлен ниже (Таблица 4).

Заключение

На основании рассмотренных современных стандартов в области ИБ – комплекса БР ИББС и ISO серии 27000 применительно к анализу угроз и уязвимостей НПС в аспекте известного инцидента с Visa и MasterCard, представляется возможным предложить следующие выводы:

1. Недостаточное внимание к проблеме обеспечения ИБ при полном охвате стадий ЖЦ может привести к дальнейшему появлению инцидентов (подобных Visa и MasterCard), т.к. важнейшие вопросы непрерывности и поддержания доступности процессингового ядра оказались вне зоны какого-либо контроля пользователей, организаций и уполномоченных регуляторов в Российской Федерации.
2. Применение для оценки результативности СМИБ для НПС только комплекса БР ИББС объективно недостаточно в силу ряда объективных причин, для обеспечения адекватного анализа современных угроз и уязвимостей НПС необходимо базироваться на современных стандартах ISO серии 27000.

Таблица 4.

Метрики ИБ оценки исполнения требований к обеспечению ИБ основных процессов

Код метрики	Описание метрики	Пример метрики
	Доступность базовых ИТ систем (режим сопровождения 5 х 8), в мес.	99,99 % или 1 мин. 48 сек. простоя
	Доступность критичных ИТ систем (режим сопровождения 7 х 24), в мес.	99,99 % или 4 мин. 19 сек. простоя
	Доля инцидентов ИБ в общем объеме зарегистрированных инцидентов, в мес.	10 %
	Количество внутренних инцидентов ИБ, в мес.	85 %
	Количество внешних инцидентов ИБ, в мес.	15 %
	Выполнение плана внутренних аудитов ИБ в срок	100 %
	Результативность выполнения корректирующих действий	100 %
	Количество выявленных несоответствий ИБ	0 %
	Количество повторно выявленных несоответствий ИБ	0 %

3. Численные методы оценки результативности СМИБ, основанные на требованиях стандартов ISO серии 27000, позволят обеспечить достоверный и оперативный контроль за текущим уровнем ИБ по отношению к НПС (как совокупности активов), а также предложить меры для исключения повторения инцидентов в будущем или существенного «смягчения» негативных последствий в том случае, если внешние факторы риска снова проявятся.

Список литературы:

1. Федеральный закон от 05.05.2014 N 112-ФЗ «О внесении изменений в Федеральный закон «О национальной платежной системе» и отдельные законодательные акты Российской Федерации».
2. Федеральный закон от 27 июня 2011 года N 161-ФЗ «О национальной платежной системе».
3. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements.
4. ISO/IEC 27005 Information technology — Security techniques — Information security risk Management.
5. ISO/IEC 27000:2014 Information technology — Security techniques — Information security management systems — Overview and vocabulary.
6. СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
7. СТО БР ИББС-1.2-2014 «Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014».
8. **Лившиц И.И.** Подходы к решению проблемы учета потерь в интегрированных системах менеджмента // Информатизация и связь. – 2013. – №1. . – С. 55 - 60.
9. **Лившиц И.И.** Применение моделей СМИБ для оценки защищенности интегрированных систем менеджмента // Тр. СПИИРАН. – 2013. – вып. 8(31) . – С. 147-163.
10. «Oracle и Microsoft могут прекратить поддержку попавших под санкции банков», Интернет ресурс «РБК Дейли» (дата обращения 01.05.2014).
11. «Visa и MasterCard снова в законе», Интернет ресурс «Газета «Коммерсантъ» № 93 (дата обращения 02.06.2014).
12. **Лившиц И.И.** Подходы к синтезу модели оценки защищенности персональных данных в соответствии с требованиями стандарта ISO/IEC 27001:2005 // Тр. СПИИРАН. – 2012. – Вып. 23. – С. 80-92.

УДК 004.728; 004.715

ПРОГРАММНАЯ АРХИТЕКТУРА СИСТЕМЫ УПРАВЛЕНИЯ ДОВЕРЕННОЙ МАРШРУТИЗАЦИЕЙ В ГЛОБАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

М.В. Буйневич, О.А. Тиамийу

Передача конфиденциальной информации между компьютерами, принадлежащим различным сетям, по глобальной телекоммуникационной сети является небезопасной, так как существует риск несанкционированного доступа (НСД) к этой информации в процессе ее следования от отправителя к получателю. Количество и разнообразие атак на телекоммуникационную инфраструктуру нарастает с каждым днем и уже с трудом поддается какой-либо систематизации и классификации [1]. С неким асимметричным опозданием, но также бурно, развиваются технологии защиты.

Еще в начале 80-х гг. прошлого века Международная Организация по Стандартизации (ISO) и Международный Консультативный Комитет по Телеграфии и Телефонии (МККТТ) признали необходимость создания модели защищенной от НСД сети, которая могла бы помочь создавать безопасные реализации взаимодействующих сетей. В тесном сотрудничестве была разработана эталонная модель «Взаимодействия Открытых Систем» (ВОС), которая в дальнейшем была описана в рекомендациях X.200 (МККТТ) и ISO 7498.

ГОСТ Р ИСО 7498-2-99 определяет архитектуру безопасности для модели ВОС, дополняя базовую справочную модель, определенную в ГОСТ Р ИСО 7498-1-99. Этот документ является введением в архитектуру безопасности Интернета и включает краткое описание набора общеархитектурных и специальных механизмов защиты, а также таблицу, которая связывает последние со средствами защиты. Список этих механизмов является не полным, а те, которые представлены, как правило, совершенно не детализированы.

Научный и чисто практический интерес в контексте безопасности глобальной телекоммуникационной сети, по мнению авторов, представляет механизм управления маршрутизацией – применение правил в процессе маршрутизации по выбору или исключению конкретных сетей, звеньев данных или ретрансляторов. Согласно пп. 5.3.7.1 – 5.3.7.1 ГОСТ «маршруты могут выбираться либо динамически, либо путем такого предварительного распределения, которое использует только физически защищенные подсети, ретрансляторы или звенья данных»; «при обнаружении постоянных попыток манипуляции данными оконечные системы могут передать поставщику сетевой услуги команду на установление соединения через другой маршрут»; «инициатор соединения может установить запрет на использование маршрутов, что требует исключения из маршрута заданных подсетей, звеньев данных или ретрансляторов».

Такое «предварительное распределение, запрет на использование маршрутов и установление соединения через другой маршрут» поглощается понятием доверенная маршрутизация, под которой понимается процесс планирования передачи информационных потоков по вычисленному маршруту через (доверенные) узлы, исключающие возможность подмены, модификации или внедрения информации в проходящие через них потоки данных [2]. С позиций общеархитектурных механизмов защиты она реализует, так называемую, доверительную функциональность, согласно которой: «Любая функциональность, непосредственно обеспечивающая механизмы защиты или доступ к ним, должна быть заслуживающей доверия» (см. п. 5.4.1.1).

Анализ современных международных и российских стандартов в области обеспечения безопасности и устойчивого функционирования сетей связи, выполненный по заказу Минкомсвязи РФ в ходе соответствующей научно-исследовательской работы [3], показал, что управление маршрутизацией в контексте доверительной функцио-

нальности даже не упоминается как сетевой механизм защиты информации. Будучи малоизученной научным сообществом, доверенная маршрутизация практически не используется для борьбы с сетевыми атаками, несмотря на потенциальную возможность обеспечения безопасной передачи конфиденциальных данных через глобальную телекоммуникационную сеть.

В этой связи авторами предпринята попытка и образован научно-технический задел в части разработки метода, реализующего доверенную маршрутизацию [2, 4]. В результате проведенных изысканий и исследований определена последовательность этапов ее реализации, а именно: определение топологии сети; идентификация доверенных узлов; составление доверенных маршрутов; получение доступа к дистанционному управлению маршрутизирующим оборудованием; гарантированная передача данных путем их принудительной маршрутизации; контроль прохождения трафика и состояния «вырожденной» сети. Проанализирована возможность и ограничения использования стека стандартных протоколов на предмет реализации того или иного этапа доверенной маршрутизации, а также разработаны новые необходимые алгоритмы.

Так, сетевая топология может быть определена в результате использования алгоритма трассировки с помощью опций IP-пакета или алгоритма доступа к маршрутно-адресным таблицам с помощью протокола BGP или SNMP. Некоторыми способами идентификации маршрутизирующего оборудования являются использование стандартных утилит таких как traceroute, nmap, ping и т.п. Для составления доверенных маршрутов может использоваться модифицированный одним их авторов алгоритм Дейкстры. Протоколы BGP и OSPF в совокупности позволяют построить «картину» маршрутов от отправителя к адресату и получить список всех транзитных узлов.

Необходимая взаимообусловленность и объективная «разношерстность» алгоритмов и приемов, реализующих оригинальный метод доверенной маршрутизации, указывает на то, что его реализацию невозможно выполнить в пределах отдельных составляющих с простым последующим объединением. Требуется общая система управления, реализующая идею доверенной маршрутизации и позволяющая согласовать в пространстве и во времени все необходимые компоненты.

Вопросы ее организации и функционирования изложим в терминах программной архитектуры, под которой понимается представление системы управления в виде взаимодействующих на разных уровнях программных модулей. В подтверждение права на такой подход процитируем пп. 5.4.1.2 – 5.4.1.3 ГОСТ Р ИСО: «Как правило, такие (используемые для гарантии включения ... доверительных функциональностей в соответствующие аппаратные и программные средства) процедуры дорогостоящи и сложны в реализации. Эти проблемы могут быть минимизированы путем выбора архитектуры, позволяющей реализовать функции защиты в модулях, которые могут быть выполнены отдельно от функций, не связанных с защитой, и защищены от них».

Наиболее близкими по функционалу к системе управления доверенной маршрутизацией являются системы управления сетью (от англ. Network Management System, NMS), под которыми понимаются централизованные программные системы, которые собирают данные о состоянии узлов и коммуникационных устройств сети, а также данные о трафике, циркулирующем в сети. Эти системы не только осуществляют мониторинг и анализ сети, но и выполняют в автоматическом или полуавтоматическом режиме действия по управлению сетью – включение и отключение портов устройств, изменение параметров мостов, адресных таблиц мостов, коммутаторов и маршрутизаторов и т.п.

Изучение принципов построения и функционирования современных NMS позволяет придти к заключению, что у системы управления доверенной маршрутизацией должна быть распределенная двухуровневая архитектура, включающая в себя 3 основных компонента: менеджер доверенной маршрутизации (МДМ) – программное средство, выполняющее отслеживание и управление группой устройств в телекоммуникационной сети; агенты доверенной маршрутизации (АДМ) – программное обеспечение, запускаемое на управляемых устройствах (в нашем случае – на маршрутизаторах); канал управления и контроля (КУК) – программное обеспечение организации канала информационного взаимодействия между менеджером и агентами (до их внедрения – операционными системами маршрутизатора).

Создание КУК необходимо, поскольку стандартные каналы управления (через консоль, удалённый терминал telnet или файл настроек) имеют ряд недостатков: они могут оказаться недоступными при изменениях в системе аутентификации (например, смене пароля или уровней доступа); факт управления по ним легко может быть обнаружен; они имеют ограничения по функциональности, поскольку не предназначены для управления модулями операционной системы маршрутизаторов. Поскольку информационное взаимодействие менеджера с агентами требует использования протокола связи, то среди широко используемых можно выбрать ICMP, как служебный и поэтому, обычно, не просматриваемый. К тому же его прохождение, как правило, не ограничивается.

Так как маршрутизирующее оборудование «подвластно» собственной операционной системе, которая и управляет проходящим трафиком, то для его перенаправления по доверенному маршруту необходимо, чтобы они управлялись МДМ посредством внедренного АДМ. Поэтому должна существовать возможность встраивания АДМ в операционную систему маршрутизирующего оборудования. Подобная технология «имплантации» известна – примеры таких «агентов» (halluxwater, stuccomontana, genie, gourmettrough, souffletrough, jetplow, sierramontana,

headwater, feedtrough и др.) можно найти у производителей Cisco, Juniper или Huawei. Эти «имплантаты» модифицируют операционную систему сетевого устройства и позволяют удаленно манипулировать трафиком через Интернет-соединение. Они достаточно стойкие и выживают при обновлении или замене операционной системы – некоторые даже после физической замены флэш-карты маршрутизирующего оборудования [5 – 7].

МДМ, удаленно управляющий маршрутизирующими оборудованием через АДМ по КУК, должен быть установлен на подключенной к контролируемой фрагменту сети рабочей станции управления информационной безопасностью, где могут решаться и другие задачи в интересах доверенной маршрутизации, как-то: определение конкретного маршрута прохождения трафика; осуществление контроля прохождения трафика; выявление транзитных маршрутизаторов, находящихся вне контролируемого сегмента сети; осуществление сбора информации о маршрутно-адресных таблицах маршрутизаторов; хранение в базе и обработка данных о маршрутах; осуществление географической привязки транзитных маршрутизаторов; реализация графического интерфейса, отображающего результаты определения конкретного маршрута прохождения трафика, – которые также могут быть представлены соответствующими программными модулями.

Рассмотрим функционал этих основных компонентов на конкретном примере – задаче трассировки потоков между заданными маршрутизаторами. От МДМ по КУК поступает команда на получение маршрута до заданного IP-адреса; в АДМ активизируется соответствующий программный модуль. Трассировка маршрута с помощью опций IP может быть основана на использовании параметра «запись маршрута» поля опции IP-пакета и предназначена для получения информации об активном маршруте прохождения информационного потока (трафика), то есть списка IP-адресов всех транзитных маршрутизаторов, расположенных от АДМ до заданного адресата (удаленного АДМ). Если отправитель включает в пакет параметр «запись маршрута», то в пакете сохраняется IP-адрес каждого транзитного маршрутизатора, участвующего в доставке пакета. Таким образом, вместе с пакетом получатель принимает список всех транзитных маршрутизаторов, «посещенных» пакетом. Формируется и отправляется на заданный маршрутизатор (удаленный АДМ) пакет, который в свою очередь формирует и отправляет еще один пакет. После получения пакета заданного маршрутизатора, АДМ производит предварительную обработку данных о прохождении трафика и полученную информацию по КУК отправляет к МДМ.

Другой пример – получение доступа к маршрутно-адресным таблицам заданного маршрутизатора. От КУ по КУК поступает команда на открытие BGP-сессии с выбранным маршрутизатором; в АДМ активизируется соответствующий программный модуль, который открывает BGP-сессию с указанным в команде маршрутизатором путем отсылки стандартного BGP-OPEN сообщения, и в случае успешного открытия, маршрутизатор начинает обмен своими маршрутно-адресным таблицам с АДМ. АДМ может поддерживать одновременно BGP-сессии с несколькими маршрутизаторами, что позволяет в режиме реального времени получать от разных маршрутизаторов их маршрутно-адресные таблицы или изменения, произошедшие в них. По команде от МДМ АДМ разрывает BGP-сессию с указанным в команде маршрутизатором, для чего достаточно прекратить отсылку KEEPALIVE-сообщений BGP-маршрутизатору.

Авторами осуществлено функциональное моделирование большинства задач, решаемых методом доверенной маршрутизации. Набор разработанных приемов и алгоритмов позволяет безопасно передавать информацию от отправителя к получателю, динамически формировать маршруты между ними, использовать защищенные каналы для контроля над маршрутизирующим оборудованием, внедряя АДМ в его операционные системы, что в совокупности гарантирует работоспособность метода доверенной маршрутизации. Метод можно реализовать, практически используя только стандартные инструменты и стандартные процедуры, но, безусловно, в определенной технологической цепочке. В этих условиях важность разработки программной архитектуры системы управления доверенной маршрутизацией в глобальных телекоммуникационных сетях трудно переоценить, особенно учитывая состояние с безопасностью передачи данных по общедоступным сетям типа Интернет.

Список литературы:

1. **Буйневич М.В.** Систематизация компьютерных атак на телекоммуникационные сети в контексте модели нарушителя // Вестник Санкт-Петербургского университета МВД России. – 2005. – № 3(27-2). – С. 306–315.
2. **Буйневич М.В., Магон А.Е., Ширяев Д.М.** Анализ возможности безопасного масштабирования телекоммуникационной структуры АСУ путем принудительной маршрутизации трафика стандартными средствами // Вопросы современной науки и практики. Университет им. В.И. Вернадского.– 2008. – № 3(13). – Том 2. – Серия «Технические науки». – С. 161–164.
3. **Буйневич, М. В., Владыко А.Г., Доценко С.М., Симонина О.А.,** под. общ. ред. Доценко С.М. Организационно-техническое обеспечение устойчивости функционирования и безопасности сети связи общего пользования. СПб.: Изд-во СПбГУТ, 2013.– 142 с.

4. **О.А. Тиамийу** Обеспечение конфиденциальности трафика путем его маршрутизации от источника // Новые информационные технологии и системы: труды X Междунар. научно-техн. конф. (г. Пенза, 27–29 ноября 2012 г.). – Пенза: Изд-во ПГУ, 2012. – С. 153–156.
5. **Kim Zetter** (2013, December 30). NSA Hackers Get the «Ungettable» With Rich Catalog of Custom Tools. Wired [Online]. Available: http://www.wired.com/2013/12/nsa-hackingcatalogue/ [2014, June 8].
6. **Engineering Evil** (2014, January 2). The Actual NSA`s Spy Catalog. EEV Independent Data Library Linking Compromised Leadership [Online]. Available: http://engineeringevil.com/2014/01/02/nsas-spy-catalog/#comments [2014, June 8].
7. **Bruce Schneier** (2013, December). More about the NSA's Tailored Access Operations Unit. Schneier on Security [Online]. Available: https://www.schneier. com/blog/archives/2013/12/more_about_the.html [2014, June 8].

УДК 004.42

МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ СРЕДСТВ АЛГОРИТМИЗАЦИИ, ИСПОЛЬЗУЕМЫХ ДЛЯ ПОИСКА УЯЗВИМОСТЕЙ

К.Е. Израилов

Введение

Применение любых средств достижения какой-либо цели неизменно связано с задачей их выбора. Не исключением является и выбор средства алгоритмизации машинного кода (далее – МК), используемого для поиска уязвимостей. Здесь под средством понимается как некий инструмент (например, программа дизассемблирования), так и определенный способ (такой как ручной анализ МК). При этом логично использование средства алгоритмизации, позволяющего достигать цель наиболее эффективно. Выбор усложняется тем, что понятие эффективности для упомянутых средств является комплексным и не может быть вычислено тривиальным способом – необходимо создание специальной методики оценки эффективности.

1. Выбор метода

Средство алгоритмизации (далее Средство) является достаточно сложным объектом для оценки, поскольку конечный результат его применения – алгоритмы МК – не может быть однозначно оценен количественным (или качественным) значением. При этом, на эффективность Средства логично должны влиять и факторы самого процесса его использования, такие как, например, скорость работы и трудоемкость. Определенную сложность вносит и специфичность цели применения Средства, далекая от их главного предназначения – алгоритмизация МК кода редко используется для поиска уязвимостей, хотя порой и является единственным решением [1, 2].

Оценка затрудняется и тем, что использование Средств может осуществляться лишь узконаправленными специалистами (далее – Специалист), не имеющими широкого распространения. Охарактеризуем последних, как людей, детально разбирающихся в области информационной безопасности, владеющих серьезными навыками программирования на разно-уровневых языках и обладающих высоким уровнем аналитического мышления. Таким образом, необходимо применение класса методов экспертной оценки, основанных на информации неколичественного характера, которые могут быть проведены лишь высококвалифицированным экспертом (далее – Экспертом), обладающим достаточными знаниями на уровне Специалиста, способным и умеющим делать обоснованные заключения (оценки).

Введем обобщенное понятие эффективности, как некой меры достижения цели, определяемой по совокупности разно-важных критериев. Одно Средство будет иметь эффективность больше другого в случае, если получение с его помощью алгоритмов МК по совокупности критериев более предпочтительно, учитывая целевую функцию – поиск уязвимостей. Некоторые показатели критериев имеют абсолютные значения, некоторые же оцениваются субъективно. При этом часть из них трудно ранжируема и подходит лишь для парного сравнения. Многие показатели являются взаимно противоречивыми – улучшение одного из них приводит к ухудшению другого.

С учетом выбранного класса методов экспертной оценки и на основании введенного понятия эффективности удовлетворительным решением для оценки Средств является (из известных) только Метод Анализа Иерархий (далее – МАИ) [3]. МАИ (создателем которого является Т.Л. Саати) представляет собой математический инструмент системного анализа, используемый экспертами для выбора «правильного» решения сложной проблемы в условиях отсутствия объективных (численных) способов сравнения элементов оцениваемой системы [4].

Порядок применения метода состоит из построения иерархии модели проблемы, определения приоритетов элементов, синтеза глобальных приоритетов альтерна-

тив и принятия решения. Классическая модель иерархии состоит из трех уровней. Верхний уровень является главной целью выбора, нижний – множеством вариантов (альтернатив) достижения цели, а средний – критериями, влияющими на достижение цели альтернативами. При этом средний может быть разбит на отдельные подуровни критериев.

Применим МАИ к текущей задачей. В нашем случае главной целью считается выбор средства алгоритмизации МК – оно автоматически будет иметь наивысшую эффективность. Альтернативы представляют собой существующие Средства, среди которых необходимо сделать выбор. Критерии же определяют те характеристики Средств, которые напрямую влияют на их эффективность. Одноуровневость множества критериев является достаточной. Назначив приоритеты ко всем элементам иерархии и проведя согласно МАИ математические операции свертки, будут получены глобальные приоритеты альтернатив; выбор максимального значения даст искомое Средство, обладающее максимальной эффективностью.

Описанная проблема выбора среди средств алгоритмизации обладает неоспоримой новизной, так как не имеет готовых решений. Это приводит к необходимости разработки соответствующей методики оценки эффективности на базе МАИ (далее – Методики) практически «с нуля», а не поиску и модификации существующих.

2. Методика оценки

Для создания полноценной Методики на основе МАИ необходимо задать, определить альтернативы, ввести критерии и вычислить их приоритеты. Получение локальных приоритетов альтернатив будет происходить в процессе применения Методики, а вычисление глобальных – на заключительном этапе с помощью линейной свертки. Как будет показано далее, Методика может применяться как для оценки отдельных средств, так и их классов.

2.1. Шаги

Методика состоит из следующих шагов.

1. Выбор альтернатив. На первом шаге необходимо проанализировать существующие на данный момент средства алгоритмизации и отобрать те, из которых необходимо выбрать наиболее эффективное. В общем случае, альтернативы должны состоять из всех известных на текущий момент Средств.

2. Определение локальных приоритетов. Используя заданные в Методике критерии и выбранные на первом шаге альтернативы, необходимо провести оценки каждой альтернативы по критериям, произведя вычисление их локальных приоритетов. В случае объективной оценки альтернативы по критерию, ее локальному приоритету назначается соответствующее значение; факт наличия у Средства некой характеристики также является объективной оценкой – логической (булевой), принимающей значения «истина» или «ложь». При наличии только субъективной оценки применяется метод попарных сравнений с использованием шкалы относительной важности.

3. Вычисление глобальных приоритетов. Глобальные приоритеты альтернатив вычисляются с помощью локальной свертки всех приоритетов Иерархии, а именно заданных изначально приоритетов критериев и определенных в процессе локальных приоритетов альтернатив по каждому критерию. В результате каждой альтернативе будет назначен ее глобальный приоритет, учитывающий как важность каждого из критериев эффективности средства алгоритмизации, так и соответствие Средства этому критерию.

4. Выбор искомой альтернативы. Заключительным этапом является выбор альтернативы по наибольшему глобальному приоритету – то есть Средства с наивысшей эффективностью.

Шаги 2–4 достаточно технологичны и могут быть осуществлены с помощью подходящих программ, например, «СППР «Выбор» [5]. Дискуссионными являются выбор и обоснование альтернатив и критериев оценки.

2.2. Альтернативы

Как было уже указано, альтернативами считаются средства алгоритмизации, отобранные для проведения оценки. В качестве разумного упрощения можно в качестве альтернатив использовать классы Средств. В случае, если Средство может быть отнесено сразу к нескольким классам, будем считать, что каждому классу соответствует лишь часть функционала этого Средства. Пример такого деления Средств на классы, указанные в порядке их специализации для решения задачи поиска уязвимостей в МК приведен ниже.

Ручной способ. Такое средство алгоритмизации можно считать наипростейшим с точки зрения технологий и наисложнейшим по трудозатратам, поскольку оно применяется без каких-либо программных инструментов, а лишь за счет физического и умственного труда Специалиста. Суть способа сводится к анализу ассемблерного кода, осознанию принципов его работы и ручному созданию алгоритмов. Ярким примером является ручной анализ МК низкоуровневыми программистами и «хакерами» с последующей документацией алгоритмов.

Визуализатор блок-схем. Данное Средство является развитием ручного способа, добавляющее в него инструмент автоматического создания графического изображения алгоритмов. Примером могут служить достаточно редкие дизассемблеры МК, включающие в себя графический визуализатор (иногда и редактор) получаемого кода в виде блок-схем, такие как AsmEditor, Visustin. Также к данному классу можно отнести как классические среды программирования на различных диалектах ассемблера со встроенным визуализатором, так и достаточно простые утилиты генерации графов по ассемблерному коду.

Интерактивный визуализатор блок-схем. Следующим развитием визуализаторов можно считать добавление возможности управления процессом их создания, то

есть наличие интерактивности. Это может быть достигнуто, например, возможностью изменения ассемблерного кода с параллельным перестроением графов алгоритмов или настройкой критериев выбора элемента блок-схемы в случае альтернативных вариантов. Наиболее известным представителем данного класса можно считать интерактивный дизассемблер – продукт IDA Pro. Помимо основной своей задачи, он синхронно строит блок-схемы ассемблерных функций, позволяет добавлять метаинформацию и видоизменять блок-схемы путем сокрытия несущественных элементов и др.

Декомпилятор в язык программирования. Отдельным направлением – реверс-инжинирингом – в инструментальных Средствах можно считать утилиты декомпиляции. Их основным назначением служит попытка получения исходного кода по имеющемуся МК или хотя бы создание его аналога. В качестве примера работающих декомпиляторов можно указать следующие: Boomerang, C4Decompiler, DDC, Rec Studio 4 и SmartDec. Отдельно выделим упомянутый ранее продукт IDA Pro, поскольку имеющийся в его расширенной версии плагин Hex-Rays как раз и предназначен для получения исходного кода по МК, дизассемблированному в нем же.

Интерактивный декомпилятор в язык программирования. Внесение элемента коммерциализации (и связанного с ней расширения области применения) в разработку декомпиляторов привело к появлению возможности управления процессом получения исходного кода, то есть к их интерактивизации. Это позволило улучшить человеко-восприятие алгоритмов декомпилированного кода из-за увеличения гибкости самого процесса без ухудшения каких либо других мер оцениваемой эффективности. Из всех упомянутых декомпиляторов необходимым и достаточным набором интерактивных возможностей обладает лишь продукт IDA Pro с плагином Hex-Ray, который будем считать единственным примером данного класса Средств.

Декомпилятор в алгоритмический язык. Приближением средств декомпиляции к заданной предметной области являются утилиты, на выходе которых создается некий псевдокод, предназначенный именно для описания алгоритмов, а никак не для восстановления исходного кода с последующей перекомпиляцией. На данный момент остаются плохо развитыми не только теория создания таких Средств, но даже и сам псевдокод представления алгоритмов. Хотя существующих известных инструментальных Средств данного класса не существует, тем не менее, примером можно считать двухэтапное применение декомпиляторов с отдельным преобразованием кода на их выходном языке программировании в псевдокод.

Интерактивный декомпилятор в алгоритмический язык. Последним элементом в списке средств алгоритмизации, построенном в порядке их специализации для решения задачи поиска уязвимостей, являются утилиты декомпиляции в язык описания алгоритмов, позволяющие управлять самим процессом. В отличие от декомпиляторов в язык программирования, они стремятся предоставлять лишь необходимую, лаконичную и сформированную нужным образом информацию об алгоритмах. При этом они являются более гибкими по сравнению с двухэтапными средствами, состоящими из раздельно работающих утилит. Наличие же в выходном коде пометок о потенциальных уязвимостях повышает их поисковые возможности. К данному классу может быть отнесена только разработанная автором Утилита [6].

2.3. Критерии

Важнейшим этапом в создании Методики является выбор критериев оценки, поскольку их необходимость и достаточность позволит определить эффективность достижение цели альтернативами наиболее точно. Применительно к текущей задаче оценки введем следующие 10 критериев.

1. Скорость работы. Чрезмерная продолжительность применения Средства может свести на нет другие преимущества, например, достоверность восстанавливаемых алгоритмов (и, как следствие, найденных уязвимостей). Это в полной мере относится к ручному способу алгоритмизации кода, который может давать удовлетворительные результаты только за длительные периоды времени. Для отдельного Средства критерий имеет объективную оценку – время работы на шаблонных примерах, а для класса– субъективную, основанную на сравнении принципов их работы.

2. Трудоемкость. Чрезмерная сложность в использовании Средства резко усиливает влияние человеческого фактора на качество выполняемой работы. В рамках данного критерия, графические программные Средства зачастую выигрывают у консольных. Критерий имеет субъективную оценку, основанную на сравнении трудоемкостей использования Средств.

3. Представление алгоритмов. Конечным результатом работы Средства является алгоритм; при этом его вид никак не специфицирован и определяется концепцией самого Средства. Удачный выбор алгоритмического представления напрямую влияет на его человеко-восприятие, поэтому критерий имеет субъективную оценку. Сравнение Средств по этому критерию даст явно лучшие результаты для блок-графов и псевдо-языков алгоритмов по сравнению с не предназначенными для этого представлениями.

4. Информация об уязвимостях. Наличие в алгоритмах, восстановленных Средством, дополнительной информации об уязвимостях, напрямую влияет на успешность их поиска. Например, пометки о потенциальных уязвимостях в алгоритмах кода позволят Специалистам обнаружить уязвимости с большей вероятностью и за более короткое время. Критерий имеет логическую оценку, основанную на наличии соответствующего функционала.

5. Поддерживаемые процессоры. Использование Средства, поддерживающего целое семейство процессоров МК, более разумно, чем «заточенного» лишь под один тип, так как Средство и сделанные наработки будут при-

менимы и в случае исследования МК той же исходной программы, но откомпилированной для другого процессора. Критерий имеет объективную оценку, основанную на количестве поддерживаемых процессоров МК.

6. Применимость для различных типов уязвимостей. Уязвимости можно разделить на типы по структурному уровню их нахождения в коде: вычислительный – ошибки в реализации МК, алгоритмический – в логике работы алгоритмов, и архитектурный – ошибки в программной архитектуре в целом. И если уязвимости первого типа утрачивают свою актуальность из-за наличия большого количества автоматизированных средств их проверки и поиска, то поиск уязвимостей второго типа до сих пор является высокоприоритетным. Ошибки же в архитектуре так и вовсе оставлены без внимания, что обосновывается как высокой степенью их субъективной характеризации, так и малым количеством выявляемых на практике, хотя последствия от реализации данного типа в разы превосходят остальные. Критерий имеет объективную оценку, основанную на количестве «искомых» типов уязвимостей.

7. Актуальность средства. Каким бы быстроработающим, малотрудоемким с удачной нотацией представления алгоритмов не было Средство, однако моральное и техническое устаревание не позволит ему конкурировать с современными «собратьями». Критерий имеет объективно-субъективную оценку и может быть оценен по наличию технической и методической поддержки Средства производителем, дистрибьюторами и/или «коммьюнити».

8. Достоверность результатов. Алгоритмы, получаемые средством, должны соответствовать тем, что реализованы с помощью МК. Данный критерий является очевидным, но трудно-оцениваемым. Тем не менее, наличие работоспособного набора тестов и возможность их проверки положительно влияет на эффективность Средства. Таким образом, критерий имеет логическую оценку, основанную на наличии тестировании Средства.

9. Экономическая целесообразность. К сожалению, полный расчет стоимости владения Средства является отдельной, достаточно сложной технико-экономический задачей, поэтому будем оценивать критерий субъективно, основываясь на дешевизне Средства. В этом случае бесплатно-распространяемые Средства будут иметь приоритет по сравнению с коммерческими.

10. Распространенность. Данный критерий, соответствующий популярности, имеет важное значение для оценки, поскольку так или иначе влияет на большинство других путем их «усиления». Ведь популярный продукт априори лучше поддерживается производителем, имеет дополнительное внешнее тестирование и поддержку современных процессоров. Критерий имеет субъективную оценку, основанную на множестве факторов влияния на известность: реклама, наличие демо- и онлайн-версий, упоминание в «блогосфере» и выступлениях на конференциях, ссылки в научных статьях и т.п.

Заключение

Разработанная Методика позволяет сделать выбор наиболее эффективного для поиска уязвимостей средства алгоритмизации МК из предлагаемого класса на основании объективных и субъективных оценок по сформулированным критериям. Система последних может быть легко модифицирована под задачу оценки эффективности любых средств, обрабатывающих МК, путем изъятия специализированных критериев под номерами 3, 4 и 6.

Было проведено экспресс-применение разработанной Методики на группе из двух алгоритмизирующих средств. Для приоритетов сформулированных критериев были определены следующие значения: скорость работы – 0.077, трудоемкость – 0.081, представление алгоритма – 0.185, информация об уязвимостях – 0.129, поддерживаемые процессоры – 0.047, применимость для различных типов уязвимостей – 0.163, актуальность – 0.03, достоверность результатов – 0.17, экономическая целесообразность – 0.042, распространенность – 0.077. Применение Методики с данными приоритетами для Утилиты и ее ближайшего конкурента – IDA Pro (включая плагин HeyRay) – дало значение глобальных приоритетов 0.541 против 0.459, что доказывает практическую ценность Утилиты, как средства алгоритмизации МК, используемого для поиска уязвимостей.

Список литературы:

1. **Израилов К.Е.** Алгоритмизация машинного кода телекоммуникационных устройств как стратегическое средство обеспечения информационной безопасности // Национальная безопасность и стратегическое планирование. – 2013. – № 2 (2). – С. 28–36.
2. **Buinevich M., Izrailov K.** Method and utility for recovering code algorithms of telecommunication devices for vulnerability search // The 16th International Conference on Advanced Communications Technology (ICACT-2014), Bongpyeong-myeon, Korea (South), on February 16-19, 2014. P. 172-176.
3. **Саати Т.Л.** Принятие Решений. Метод анализа иерархий / Т. Л. Саати. – М.: Радио и связь, 1993. – 278 с.
4. **Буйневич М.В., Татаринов А.А.** Метод военно-экономического анализа вариантов проектируемых образцов автоматизированных систем // Автоматизация процессов управления. – 2009. – № 2. – С. 14–18.
5. Программа «СППР «Выбор» // Официальный сайт. URL: http://www.ciritas.ru/product.php?id=10 (дата обращения: 01.09.2014)
6. **Буйневич М.В.,** Израилов К.Е. Автоматизированное средство алгоритмизации машинного кода телекоммуникационных устройств // Телекоммуникации. – 2013. – № 6. – С. 2–9.

УДК 621.391

КРИТИЧЕСКАЯ ТЕХНОЛОГИЯ КВАЗИОПТИМАЛЬНОГО МАШИННОГО ЗРЕНИЯ

М.В. Харинов, В.П. Заболотский

Введение

В ближайшие годы ожидается появление прорывных наукоемких технологий в области машинного обучения, компенсирующих современное отставание теории от практики извлечения, представления и автоматической обработки информации цифровых сигналов. Судя по авторитетному заявлению американского агентства по перспективным оборонным научно-исследовательским разработкам DARPA (Defense Advanced Research Projects Agency), критической проблемой создания искусственного интеллекта является унификация программ машинного обучения, которая будет решена к 2017 году в результате выполнения очередной исследовательской программы PAML (Probabilistic Programming for Advanced Machine Learning). Современное состояние теории и практики компьютерной обработки сигналов, в частности, изображений, позволяет выполнить задачу за счет развитой автоматизации первичного этапа иерархического упорядочения и классификации исходных данных. В области машинного зрения для этого необходимо решить проблему автоматичекого выделения объектов на цифровых изображениях, именуемую «проблемой сегментации». Проблема возникает при распознавании цифровых изображений на первоначальной стадии «приведения данных к удобному для распознавания виду» (И.Б. Гуревич, 1985, [1]), «локализации объектов» (Ю.В. Визильтер и др., 2011, [2]), извлечения и упорядочения «глобально-локальной информации» (С.В. Абламейко и др., 2009, [3]), «квазиоптимальной разметки» изображения (П.А. Мельников и др., 2012, [4]). Суть проблемы состоит в недостаточной формализации понятия «объектов», которые компьютер «видит» или выделяет на изображении для последующего анализа признаков и идентификации.

В настоящее время, в СПИИРАН разработаны фундаментальные основы технологии *квазиоптимального* иерархического разбиения цифрового изображения на вложенные изображения «объектов», которые вычисляются из формального условия оптимального качества целевой последовательности разбиений. Общетеоретической основой технологии является формализация понятия информации, кодированной в цифровом сигнале, и количества бит информации в элементе сигнала (Р.М. Юсупов, 1973 г., [5]). В практике вычислений технология опирается на оригинальную систему счисления [6], разработанную и применяемую пока только в СПИИРАН, а также на аппарат динамических деревьев Слэйтора-Тарьяна [7]. Динамические деревья для обработки изображений впервые применены в СПИИРАН [8], и в настоящее время начинают интенсивно внедряться за рубежом [9], так как не имеют альтернатив по затратам памяти и быстродействию вычислений с иерархией произвольных разбиений изображения на вложенные изображения. Упомянутая система счисления является основой модели сигнала, порождающего собственную цифровую память, в которой независимо от предусмотренных искажений сигнала формируется его инвариантный образ [6] и оценивается целочисленное количество информации в пикселе изображения [10]. В 2008 г. модель запатентована в приложении к задачам стеганографии (патенты РФ №№ 2006119273 и 2006119146). На современном этапе она усиливается за счет аналитически обоснованных алгоритмов, разработанных в 2012-2014 гг., и обобщается на обратные задачи анализа и распознавания изображений.

Обобщенная задача сегментации изображения

Неопределенность унифицированного понятия объекта на изображении препятствует созданию эффективных программ компьютерного распознавания цифровых изображений. При этом под «объектами» обычно имеются в виду фрагменты изображения, интуитивно выделяемые в этом качестве человеком. Эффективные решения, которые создаются за счет трудоемкого эвристического программирования и предварительного обучения, как

правило, предназначены для анализа изображений с заранее известными объектами (текстовых, снимков лиц и др.), что необходимо для практических нужд, но заведомо ограничивает возможности распознавания объектов.

В обсуждаемой технологии машинного зрения отмеченная трудность формализации выделения объектов на изображении обходится за счет постановки задачи, в которой понятия «изображение» и «объект» не разграничиваются между собой. При этом элементами изображения служат не отдельные пиксели, а множества пикселей изображения, которые, в общем случае, составляют связные *сегменты* изображения, а также *кластеры* из несмежных сегментов. Тезис о том, что исходное изображение состоит из изображений означает, что оно обладает структурой, которая предполагается иерархической. При этом иерархия объектов, вложенных один в другой, задается некоторым установленным алгоритмом разделения изображения надвое и отражает неоднозначность интерпретации исходного изображения. *Тривиальные* сегменты или кластеры из одинаковых пикселей являются минимальными изображениями и считаются неделимыми.

Особенностью сегментации в обобщенной постановке является то, что она не ограничивается простым итеративным разделением исходного изображения на вложенные изображения объектов, а предполагает элементы автоматического распознавания. В результате сегментации, помимо самого разбиения изображения на объекты, для каждого из объектов автоматически генерируется его целочисленное обозначение, имя, посредством которого объекты различаются между собой, что визуализируется в наглядном представлении, если значения пикселей заменяются на соответствующие обозначения объектов. При этом важным требованием к автоматической разметке является ее робастность к определенным яркостным искажениям изображения и изменению его масштаба, а также иерархическая структура, адекватная иерархической структуре объектов.

Для эффективного разделения изображения из n пикселей на объекты решается задача оптимизации качества разбиения, которое оценивается по величине суммарной квадратичной ошибки E или среднеквадратичного отклонения $\sigma = \sqrt{\frac{E}{3n}}$ изображения от своего *кусочно-постоянного приближения* с усредненными по кластерам значениями пикселей [11].

Обобщенная задача оптимизации приближений изображения

Для выделения и распознавания объектов на цифровых изображениях за счет оптимизации качества приближений изображения традиционно применяются: метод K–средних [11, 12], метод Оцу [13, 14], а также метод Уорда и модель Мамфорда-Шаха [15–18]. При этом уделяется недостаточно внимания реальной минимизации целевой функции, что связано со сложностью точного вычисления оптимальных приближений. В [18] рассмотрен эффект минимизации целевой функции и получены оптимальные приближения для стандартных изображений минимального размера. Выяснилось, что модель Мамфорда-Шаха сегментарной аппроксимации изображения, хотя и выигрывает по качеству приближений в сравнении с другими методами слияния сегментов, но при малом числе сегментов дает среднеквадратичное отклонение, которое примерно в полтора раза превышает минимально достижимое. Причина становится понятной в сравнении модели Мамфорда-Шаха с методом Уорда [15], в котором минимизация не ограничивается слиянием смежных сегментов, но с ростом числа кластеров квадратично падает скорость обработки. Метод Оцу кластеризации пикселей изображения при малом числе кластеров обеспечивает точное решение, но с увеличением числа кластеров утрачивает эффективность из-за экспоненциального падения скорости обработки. Кроме того, метод Оцу не имеет очевидного обобщения на случай цветовых и многоспектральных изображений.

В целом, эксперименты показали, что оптимальные приближения изображения порождают ряд вычислительные проблем — генерации, сохранения в оперативной памяти, преобразования и анализа. Основная причина заключается в том, что последовательность оптимальных приближений не является иерархической. Поэтому в [19] предложен способ аппроксимации оптимальных приближений иерархическими квазиоптимальными приближениями изображения, для которых перечисленные проблемы снимаются, если вычисления реализуются в терминах деревьев Слэйтора-Тарьяна [7-8].

В развиваемой технологии оптимизационная задача ставится и решается в обобщенной постановке, в которой целевым результатом является не единственное оптимизированное приближение при заранее заданном числе кластеров, как, например, в методе K–средних, а вся последовательность квазиоптимальных приближений при каждом числе кластеров. При этом квазиоптимальные приближения, помимо близкого к оптимальному качества сохраняют некоторые другие свойства оптимальных приближений, например, в зависимости от числа кластеров описываются выпуклой последовательностью значений суммарной квадратичной ошибки [20].

Аналитическое обоснование

Следует обратить внимание, что массовая разработка программ компьютерного зрения для обнаружения и распознавания конкретных объектов нередко сопровождается отступлениями от точного выполнения расчетов согласно теоретическим рекомендациям, что позволяет учесть особенности конкретных изображений, но не способствует созданию унифицированных решений. Так, например, принято считать, что классический общеупотребительный метод K–средних, разработанный много лет назад, вероятно, еще для арифмометров, обеспечива-

ет минимизацию среднеквадратичной ошибки σ. Однако, согласно элементарным формулам [21] для строгого соответствия алгоритма указанному функционалу необходимо сравнивать расстояния до центров кластеров с коэффициентом $\alpha < 1$, который описывает количества пикселей n_1 и n_2 в донорском и акцепторном кластерах:

$$\alpha \equiv \sqrt{\frac{n_2(n_1-1)}{n_1(n_2+1)}}. \qquad (1)$$

При операциях с несколькими пикселями единица в выражении (1) заменяется на число пикселей, коэффициент α существенно отличается от 1, и указанная неточность интерпретации приводит к ошибочным вычислениям. Аналогичное несоответствие алгоритма и целевого функционала имеет место в наиболее популярной версии FLSA модели Мамфорда–Шаха [18], где, по нашему опыту, оно приводит к неоправданному усложнению вычислений. В остроумном методе кластеризации [22] автор, руководствуясь эвристическими соображениями, упускает возможность построения на основе своего метода альтернативы методу Оцу [20], которая, в отличие от последнего, применима не только для серых, но также и для цветовых изображений.

Для разработки алгоритмов аппроксимации изображения квазиоптимальными приближениями изображения мы получили аналитическое выражение, которое в общем виде описывает изменение суммарной квадратичной ошибки при слиянии нескольких кластеров.

Если исходное или вложенное изображение является результатом слияния j вложенных кластеров, то интегральное квадратичное отклонение E_0 значений пикселей этого изображения от среднего значения получается суммированием интегральных квадратичных отклонений E_p для вложенных кластеров и некоторой неотрицательной добавки, характеризующей средний взвешенный разброс квадратов евклидовых попарных расстояний $\left\|I_p - I_q\right\|^2$ между центрами I_p, I_q кластеров p и q из n_p и n_q пикселей в цветовом RGB пространстве [21]:

$$E_0 = \sum_{p=1}^{j} E_p + \frac{1}{2} \cdot \frac{\sum_{p=1}^{j}\sum_{q=1}^{j} n_p n_q \left\|I_p - I_q\right\|^2}{n}, \qquad (2)$$

где $E = \sum_{p=1}^{j} E_p$ — суммарная квадратичная ошибка для разбиения изображения на j кластеров, E_0 — суммарная квадратичная ошибка для разбиения изображения с единственным кластером, $n = \sum_{p=1}^{j} n_p$, — число пикселей в рассматриваемом изображении.

Если в качестве j вложенных кластеров иметь в виду тривиальные кластеры, на которые распадается изображение, то сумма E_p, очевидно, обращается в 0. Если в качестве тривиальных кластеров рассматриваются отдельные пиксели, то в выписанной формуле следует также положить $n_p = n_q = 1$ и $j = n$. Тогда она, с точностью до множителя, совпадает с выражением для дисперсии значений пикселей, которое активно применяется в [23-25] для теоретической и практической разработки методов кластеризации. Таким образом, формула (2) обобщает аналогичную формулу [23-25] на случай тривиальных кластеров из нескольких или многих пикселей.

Для случая $j = 2$ пары вложенных кластеров, из (2) получаются выражения для приращений суммарной квадратичной ошибки при трех операциях с кластерами пикселей [21]: операции слияния пары кластеров, операции коррекции кластеров посредством реклассификации подмножества пикселей из одного кластера в другой и операции дробления кластера за счет выделения подмножества пикселей в отдельный кластер. Приращение суммарной квадратичной ошибки при слиянии сегментов служит критерием слияния и минимизируется в версии [20, 21] модели сегментации Мамфорда-Шаха [16], и либо с дополнительным множителем, либо с аддитивной добавкой, используется в ее версиях [17, 18]. Аналитическое выражение для приращения суммарной квадратичной ошибки при коррекции кластеров продуктивно тем, что позволяет вывести классический метод K-средних (*K-means*) и обобщенный метод «*K-meanless*» [23], который в версии [21], наряду с операциями с отдельными пикселями, предусматривает операции с наборами пикселей. Выражение для приращения суммарной квадратичной ошибки при дроблении кластера применяется в алгоритмах генерации квазиоптимальных приближений изображения [20]. Таким образом, по сравнению с моделью Мамфорда-Шаха, в развиваемой технологии утроено число базовых операций с множествами пикселей изображения, что обеспечивает достоверную оптимизацию качества приближений изображения по суммарной квадратичной ошибке или среднеквадратичному отклонению приближения от изображения.

В целом, система элементарных формул [21] обеспечивает разработку и развитие алгоритмов достоверной оптимизации качества приближений изображения, и, что не менее важно, позволяет уточнить интерпретацию классических методов [11-18], потенциал которых в приложении к цифровым изображениям еще далеко не исчерпан.

Заключение

Обобщенная постановка и решение задач сегментации и аппроксимации цифрового изображения иерархической последовательностью квазиоптимальных приближений в задачах распознавания актуальны для создания унифицированных алгоритмов автоматического выделения объектов. Помимо автоматизации распознавания цифровых изображений, обсуждаемые решения полезны также для: а) развития стеганографических приложений; б) автоматической обработки оцифрованных звуковых и пр. сигналов; в) фильтрации и подавления шумов; г) минимизации потерь в задачах сжатия сигналов; д) оптимизации порядка передачи информации и др.

Еще 35-40 лет назад типичной задачей при расчетах на ЭВМ являлось сжатие данных без потерь, которой занималось множество программистов для решения конкретных проблем хранения и передачи информации. В настоящее время, этой задачей продолжает заниматься узкий круг профессионалов, а остальные специалисты пользуются готовыми программами. Вполне вероятно, что автоматическое выделение объектов на цифровых изображениях окажется следующей проблемой, для которой будут найдены общеупотребительные решения.

Список литературы:

1. **Gurevich I. B. and Yashina V.V.** Descriptive approach to image analysis: image formalization space // Pattern Recogn. Image Anal.: Adv. Math. Theory Appl. 2012. Vol. 22, №.4, — P. 495–518.
2. **Визильтер Ю.В., Желтов С.Ю.** Проблемы технического зрения в современных авиационных системах // Механика, управление и информатика. – 2011. – №6. – С. 11–44.
3. **Абламейко С.В., Недзьведь А.М., Белоцерковский А.М., Руцкая Е.А.** Сегментация трехмерных изображений компьютерной томографии на основе глобально-локальной информации // Вестник Белорусского госуниверситета. Сер. 1, Физика. Математика. Информатика. – 2009. – № 1. – С. 58-64.
4. **Мельников П.А., Копылов А.В**. Алгоритм поиска квазиоптимальной разметки для обработки изображений с построчным комбинированием переменных // Известия Тульского государственного университета. Естественные науки. – 2012. – № 1. – С. 119-129.
5. **Юсупов Р.М.** Теоретические основы прикладной кибернетики. Вып.1. Элементы теории информации. – Л.: ВИКА им. А.Ф.Можайского, 1973. — 110 с.
6. **Харинов М.В**. Запоминание и адаптивная обработка информации цифровых изображений / Под ред. Р.М. Юсупова. — СПб.: Изд-во С.Петерб. ун-та, – 2006. – 138 с
7. **Sleator D.D., Tarjan R.E**. Self-Adjusting Binary Search Trees // Journal of the ACM Vol. 32 (3), 1985. — pp. 652–686.
8. **Харинов М.**В. Разработка динамических структур данных системы автоматизированного распознавания изображений /руков. В.В. Александров/ Автореф. Дис. канд. технич. наук. — СПб. 1993. — 20с.
9. **Nock R., Nielsen F.** Statistical Region Merging // IEEE Trans. Pattern Anal. Mach. Intell. Vol. 26(11), 2004. — pp. 1452–1458.
10. **Заболотский В.П., Харинов М.В.** Стеганографическая защита документов на основе модели запоминания информации изображения // Информация и связь. – 2010. – № 1. – С. 77-81.
11. **Айвазян С.А., Бухштабер В.М., Енюков И.С., Мешалкин Л.Д.** Прикладная статистика: Классификация и снижение размерности. М.: Финансы и статистика, 1989. — 607 с.
12. **Jain A.K.** Data Clustering: 50 Years Beyond K–Means // Pattern Recognition Letters, Vol. 31, No. 8, 2010. — pp. 651–666.
13. **Otsu N.** A Threshold Selection Method from Gray–Level Histograms // IEEE Transactions on systems, MAN, and CYBERNETICS, Vol. SMC–9, №. 1, 1979. — pp. 62–66.
14. **Ping-Sung Liao, Tse-Sheng Chen, Pau-Choo Chung** A Fast Algorithm for Multilevel Thresholding // J. Inf. Sci. Eng. Vol. 17 (5), 2001. — pp. 713–727.
15. **Ward J.H., Jr.** Hierarchical grouping to optimize an objective function. // J. Am. Stat. Assoc. 1963. Vol. 58, Issue 301, — pp. 236-244.
16. **Mumford D., Shah J.** Boundary detection by minimizing functionals, I // Proc. IEEE Comput. Vision Patt. Recogn. Conf., San Francisco, 1985.— pp. 22–26.
17. **Robinson B.J., Redding N.J., Crisp D.J.** Implementation of a fast algorithm for segmenting SAR imagery // Scientific and Technical Report, Australia: Defense Science and Technology Organization, Australia, 01 January 2002. — 42 p.
18. **Koepfler G., Lopez C., Morel J.** A Multiscale Algorithm for Image Segmentation by Variational Method // SIAM Journal on Numerical Analysis, Vol. 31, No 1, 1994.— pp. 282–299.
19. **Kharinov M.V.** Image Segmentation Method by Merging and Correction of Sets of Pixels // Pattern Recognition and Image Analysis: Advances in Mathematical Theory and Applications / Vol. 23. No 3, 2013. — pp. 393-401., Pleiades Publishing, Ltd.
20. **Харинов М.В.** Альтернатива иерархическому методу оцу для цветового изображения // Вестник Бурятского государственного университета. Математика и информатика. – 2014. – №9(2). – С. 64-72.
21. **Харинов М.В.** Обобщение трех подходов к оптимальной сегментации цифрового изображения // Труды СПИИРАН. – 2013. – Вып. 2(25) . – С. 294–316.
22. **Arifin A. Z., Asano A.** Image segmentation by histogram thresholding using hierarchical cluster analysis // Pattern Recognition Letters. 2006. Vol. 27. №. 13. – P. 1515-1521.
23. **Dvoenko S.D.** Meanless k-means as k-meanless clustering with the bi-partial approach // Pattern Recognition and Information Processing (PRIP'2014) / Proc. of the 12th Int. Conf., Minsk, 2014. — pp. 50–54.
24. **Dvoenko S.D.** Clustering of a set of objects// Pattern Recognition and Information Processing (PRIP-2007) / Proc. of the 9th Int. Conf., Minsk, 2007. Vol. 1. — pp. 93–97.
25. **Двоенко С.Д.** Неиерархический дивизимный алгоритм кластеризации // Автоматика и телемеханика. – 1999. – №4. – С. 117–124.

УДК 004

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В НОВЫХ УСЛОВИЯХ

Д.С. Черешкин

Введение

Вопросы, обсуждаемые в статье и предлагаемые методы их решения, явились результатом нескольких, порою полемических, порою примирительных, но всегда очень плодотворных их обсуждений с чл.-корр. РАН Р.М. Юсуповым, способным как обоснованно возразить, так и с удовольствием согласиться с собеседником. Надеюсь, что изложенное ниже в большой мере отражает наше мнение по рассматриваемой проблеме.

Начало третьего тысячелетия, с точки зрения значимости и усложнения проблем обеспечения безопасности информации, используемой нашей цивилизацией практически во всех сферах деятельности, можно охарактеризовать однозначно — состояние с решением в стране этой проблемы все более определяет состояние общей безопасности государства. Этот вывод определяют следующие факторы. Первый — постоянный рост уровня применения информационно-телекоммуникационных технологий (ИТТ) и средств их реализаций в большинстве стран в управлении, экономике, социальной сфере и т.д. в виде различного рода автоматизированных информационных систем. Второй — рост численности населения земного шара, использующих возможности Интернета и ИТТ при решении множества своих жизненных задач. Третий фактор — появление кибероружия и рассмотрение его некоторыми политиками в качестве реального средства решения многих сложных международных политических и социальных проблем.

Можно сказать, что два первых фактора обеспечили появление и быстрое развитие того, что на Западе называют мировым киберпространством, а у нас — критической информационной инфраструктурой.

Соответственно, если есть общее для всех пользователей и никем не контролируемое и управляемое информационное пространство, свободно доступное для всех образующих его систем, элементов и пользователей, в котором существуют возможности для связи с любой его точкой и имеется интеллектуальное оружие, также ориентированное на использование этих возможностей, то не грех и применить его для разрешения спорной ситуации. Если при этом учесть, что применение этого оружия не связано с шумом орудийной канонады или разрывами бомб, а определение источника его применения часто является сложной задачей, но становится понятным интерес ряда стран, например, США к разработке стратегий использования кибероружия.

При этом кибероружие, а это различные виды внедрения в работающие автоматизированные системы противника — вирусы, «черви», трояны, программные «закладки», высокочастотное облучение и т.д. сегодня рассматривается как средство разрушения производства за счет прямого внедрения и нарушения управляемых процессов в АСУ ТП, АСУП и АСУ любых критически важных объектов (КВО) любой сферы или вывода из строя систем государственного управления путем разрушения используемых в них информационных массивов.

Сегодня это уже не ужастики научной фантастики, а реальные факты. Например, разрушение оборудования по обогащению урана атомного завода в Иране путем запуска в АСУ ТП завода специально созданного червя Stuxnet, вывод из строя АСУ энергоснабжения и ряда других в результате кибер-атаки на информационную инфраструктуру Эстонии.

Как следствие, появление нового комплекса угроз нарушения информационной безопасности – кибер-угроз требует существенной коррекции ряда положений принятых в России директивных документов, например, Доктрины информационной безопасности и других, утвержденных до 2000 г.

1. Состояние обеспечения информационной безопасности

Проблема обеспечения информационной безопасности в новых условиях вышла на первое место в большин-

стве принятых во многих странах (США, Англия, страны ЕС, Бразилия, Китай и др.) Стратегиях кибернетической безопасности. В нашей стране подготовлены три базовых документа — проект «Концепция Стратегии обеспечения кибербезопасности Российской Федерации» (подготовлен в Совете Федерации), «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» (с 16 июля 2012 г. размещен на официальном сайте Совета Безопасности) и Проект Федерального Закона «О безопасности критической информационной инфраструктуры Российской Федерации» (подготовлен ФСБ России).

Необходимо отметить, что основные положения проекта Закона практически совпадают с положениями, изложенными в известных директивных материалах США. Это позволяет считать, что такие положения универсальны.

Целесообразно привести принятые в проекте названного Федерального Закона определения понятий:

Безопасность критической информационной инфраструктуры Российской Федерации – состояние объектов критической информационной инфраструктуры в целом, при котором возникновение на них компьютерных инцидентов не приведет к потере управления экономикой и/или обеспечения обороноспособности, безопасности и правопорядка в Российской Федерации, в субъекте Российской Федерации или административно-территориальной единице, ее необратимому негативному изменению (разрушению) либо существенному снижению уровня безопасности, жизнедеятельности населения.

Информационные ресурсы Российской Федерации – информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом.

Компьютерная атака – целенаправленное воздействие на информационные ресурсы программно-техническими средствами, осуществляемое в целях нарушения безопасности информации в этих ресурсах.

Компьютерный инцидент – факт нарушения (или прекращения) функционирования объекта критической информационной инфраструктуры Российской Федерации, в том числе вызванной компьютерной атакой.

Предлагается следующая схема исследования — на основании анализа разнообразных отечественных и зарубежных материалов, в том числе и нормативных (проект российского Федерального закона и такого же рода документы США) выделим основные кибер-угрозы и направления их парирования; рассмотрим предлагаемые пути реализации направлений; определим те вопросы, которые требуют проведения научных исследований.

В настоящее время все кибер-атаки на критическую информационную инфраструктуру (КИИ) и входящие в нее КВО имеют характерную особенность — они оказывают прямое воздействие на автоматизированную систему объекта с целью нарушения её деятельности, приводящее к нарушению нормального режима функционирования, вплоть до полного или частичного разрушения системы.

К таким угрозам относятся:

- заражение системы вирусами нового типа — вирусами-разрушителями;
- модификация и/или существенное изменение (разрушение) процедур управления объектом;
- хищение и/или разрушение хранимой в системе информации;
- использование существующих уязвимостей в структуре и составе системы, выполняемых процедурах, реализуемых системой в процессе управления;
- использование специальных возможностей и уязвимостей импортного программного обеспечения и оборудования (закладки, трояны и т.д.);
- удаленное частотное воздействие на автоматизированную систему управления (самолеты, скоростные поезда).

Существует два метода реализации перечисленных угроз, первый и основной — прямое несанкционированное проникновение (внешнее и/или внутреннее) в систему с целью её разрушения или модификации управляющих воздействий на объект; второй — неправомерные действия персонала (ошибки, преднамеренные действия).

Реализация первого метода может быть проведена как в результате внешнего электронного воздействия (электронный взлом системы защиты) на входы и сетевые коммуникации в системе, так и внутреннего — преднамеренные действия персонала на любой элемент системы.

Необходимо отметить, что наиболее уязвимыми элементами КИИ являются различного типа автоматизированные информационные системы (наиболее уязвимы и наиболее интересны для нападения — системы КВО, чаще всего АСУ ТП), телекоммуникации и системы связи.

Направления развития систем обеспечения кибербезопасности

В качестве перспективных направлений развития систем обеспечения кибербезопасности (или безопасности КИИ) выделены:

- создание системы государственной поддержки, включая необходимые государственные структуры и регламентации обеспечения безопасности КИИ;
- создание общенациональной системы мониторинга всех попыток и реализованных нарушений нормального режима функционирования КИИ для выявления имеющихся потенциальных угроз и способов их парирования;

- переход к опережающему реагированию на внешние и внутренние возмущения (кибер-атаки) за счет разработки новых методов и средств решения задач обеспечения безопасности КИИ;
- переход на приоритетное применение электронных, телекоммуникационных средств, программно-аппаратных и проектных решений, в особенности в АСУ ТП, отечественной разработки и производства.

Очевидно, что необходимо отметить важные, но очень сложные направления, подробное рассмотрение которых потребовало бы слишком много места и выхода за пределы настоящей статьи.

К таким направлениям должны быть отнесены:

- вопросы создания новых средств защиты уязвимостей объектов кибернападения;
- «человеческий фактор» и его воздействие на безопасность;
- вопросы активного участия России в международной деятельности по разработке и принятию международных соглашений по запрещению проведению кибер-атак на объекты критической информационной инфраструктуры любой страны как средства политического воздействия.

Рассмотрим, как организованы работы по всем перечисленным выше направлениям в наиболее «продвинутой» в обеспечении кибербезопасности КИИ стране — США и в России.

Для реализации задач первого перспективного направления развития систем обеспечения кибербезопасности в США создана структура, обеспечиваемая финансированием, разработкой и принятием нормативных актов и постановлений. Необходимо отметить, что в соответствии с Президентской директивой №63 (PPD-63) от мая 1998 г. в США была начата разработка национального плана обеспечения безопасности информационных систем (критической информационной инфраструктуры, включая КВО этой инфраструктуры). В этом плане предусматривалась задача создания соответствующей организационной структуры, которая и была решена.

В США общее руководство всеми проблемами обеспечения безопасности КИИ страны, включая и кибербезопасность, осуществляется Советом Национальной Безопасности (СНБ) и Министерством внутренней безопасности (МВБ), обеспечивающими координацию всей деятельности по обеспечению внутренней безопасности, созданы и функционируют специализированные организации. В целом, таких организаций к настоящему времени более сорока. В структуре МВБ было создано спецподразделение Кибернетической безопасности (National Cyber Security Division – NCSD), главным элементом которого является Центр экстренного реагирования на компьютерные происшествия в США (U.S. Computer Emergency Response Team – US CERT), основной задачей которого является мониторинг имевших место кибер-атак.

Таким образом, в США создана специализированная организационная инфраструктура, ориентированная сегодня на решение задач обеспечения кибербезопасности всех критических инфраструктур, включающих в себя и соответствующие КВО.

Очень важным фактором успешной деятельности всех перечисленных выше, а также и многих других организаций в США является разработанные и утвержденные на высшем уровне директивные материалы, определяющие задачи обеспечения кибербезопасности КИИ и, соответственно, решающих эти задачи организаций.

Наряду с подготовкой и принятием директив в США большое внимание уделено разработке нового комплекса национальных и поддержке разработок Международных стандартов по обеспечению безопасности КВО. Основное место среди стандартов занимает комплекс ISA SP99.

Также следует отметить разработанный NIST (National Institute of Standards and Technology) стандарт NIST SPS00=82 «Guide to Industrial Control Systems (ICS) Security/ Recommendation of the National Institute of Standards and Technology». В этом руководстве, выпущенном в июне 2011 г., рассмотрены проблемы защиты АСУ ТП и выбора необходимого для этого стандарта.

Очевидно, что использование широкой гаммы стандартов позволяет более активно и успешно решать проблемы обеспечения безопасности КИИ в США.

По сравнению с США и четко следующими за ними странами ЕС состояние с решением проблем обеспечения безопасности КИИ в России не столь блестяще и успешно. Практически отсутствует ориентированная на решение таких проблем организационная инфраструктура.

Российская федеральная нормативная база по обеспечению безопасности включает в себя:

- Федеральный Закон «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 143-ФЗ;
- «Доктрина информационной безопасности Российской Федерации» — утверждена Президентом РФ 09.09.2000, № Пр-1895;
- «Стратегия национальной безопасности Российской Федерации до 2020 года» — утверждена Президентом Российской Федерации 12.05.2009, № 557(4);
- Федеральный Закон «О безопасности» от 28.12.2010 №390-ФЗ;
- Федеральный Закон РФ «О транспортной безопасности» от 09.03.2009 №16-ФЗ;
- Проект Федерального Закона «О безопасности критической информационной инфраструктуры Российской Федерации» — подготовлен ФСБ России;
- Проект Концепции кибербезопасности Российской Федерации» — подготовлен Советом Федерации.

- Также существует нормативная база исключительно по обеспечению безопасности КВО, в состав которой входят следующие документы:
- «Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий» — документ Совета Безопасности Российской Федерации от 08.11.2005;
- «О мерах по обеспечению безопасности критически важных для национальной безопасности объектов инфраструктуры и населения от угроз техногенного, природного характера и террористических проявлений» — Протокол от 13.11.2003 № 14 Заседания Совета безопасности и Президиума Госсовета Российской Федерации;
- «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры российской Федерации» — утверждены 16.07.2012;
- «Базовая модель угроз безопасности в ключевых системах информационной инфраструктуры» — утверждена ФСТЭК России 18.05.2007;
- «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры» — утверждена ФСТЭК России 18.05.2007;
- «Общие требования по обеспечению безопасности в ключевых системах информационной инфраструктуры» — документ утверждён ФСТЭК России 18.05.2007;
- «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» — документ утверждён 19.11.2007.

Специализированные федеральные стандарты в России приняты отдельными ведомствами, но подробная информация о них отсутствует.

Как видно из сказанного, необходимая нормативная база в России существует. Однако более тщательный анализ имеющихся специализированных материалов позволяет сделать ряд выводов:

Для реализации всех нормативных требований, наряду с Федеральными законами должны быть разработаны и приняты соответствующие регламенты и методические материалы, которых практически нет;

Не детализировано, кем, как и каким образом должны обеспечиваться устанавливаемые требования, кто – государство или бизнес – должен финансировать их выполнение, кто и как устанавливает критерии выполнения и их нормативные значения, контролирует выполнение требований;

Подготовленные проекты документов в большей степени отражают ведомственные интересы и слабо учитывают интересы общества, что отражается и в том, что широкого общественного обсуждения этих документов не проводилось.

В целом по первому направлению можно отметить определенное отставание России в решении проблем обеспечения кибербезопасности КИИ.

Второе перспективное направление развития систем обеспечения кибербезопасности рассматривает создание общенациональной системы мониторинга всех попыток и реализованных нарушений нормального режима функционирования КВО для выявления имеющихся потенциальных угроз и способов их парирования. Целесообразно привести определение системы мониторинга, как оно дано в проекте Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».

Единая государственная система обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки уровня реальной защищенности ее элементов – централизованная, иерархическая, территориально распределенная структура, включающая силы и средства обнаружения и предупреждения компьютерных атак, а также органы управления различных уровней, в полномочия которых входят вопросы обеспечения автоматизированных систем управления КВО и иных элементов критической информационной инфраструктуры.

Практически подобное же определение принято и в США.

Специалисты как США, так и России считают, что основой перехода к новому принципу построения системы кибербезопасности – принципу опережающего реагирования на внешние и внутренние возмущения (кибератаки), является создание системы мониторинга всех нападений на КИИ страны, включая входящие в нее КВО и, одновременно способную фиксировать все случаи отклонения от нормативного режима функционирования используемых объектами защиты автоматизированных систем. Следует отметить, что при создании системы мониторинга должны быть объединены усилия всех государственных структур – военных и разведывательных ведомств и обеспечиваться тесное взаимодействие с корпоративными структурами – владельцами КВО.

Планы создания системы мониторинга такого же типа и с подобными целями в России предусмотрены в имеющихся нормативных документах.

Национальная система мониторинга информационной безопасности США сформирована на базе объединения существовавших ведомственных систем – разведорганизаций, военного ведомства, других систем и Центров.

Общую координацию функционированием всего комплекса систем и Центров (далее Комплекс мониторинга информационной безопасности США) осуществляет

Центр экстренного реагирования на компьютерные происшествия в США (U.S. Computer Emergency Response Team – US CERT), входящий в состав спецподразделения Кибернетической безопасности МВБ (National Cyber Security Division – NCSD).

Таким образом, можно считать, что Комплекс мониторинга информационной безопасности США максимально охватывает все области национальной инфраструктуры, включая КВО, и обеспечивает решение задач, как обнаружения компьютерных воздействий – кибер-атак, так и выработку возможных мер по их парированию.

Для обеспечения эффективного функционирования Комплекса мониторинга информационной безопасности США на всех ключевых информационных системах установлены программно-аппаратные устройства обнаружения вторжений.

Для выполнения поставленных перед Комплексом мониторинга информационной безопасности США задач был разработан план проведения научно-исследовательских и опытно-конструкторских работ по решению проблем обеспечения информационной безопасности распределенных компьютерных сетей и распределенных вычислений. Координацию проводимых исследований осуществляет Институт защиты информационной инфраструктуры (Institute for Information Infrastructure Protection).

В нашей стране создание системы мониторинга безопасности информационной инфраструктуры, в том числе КВО, было инициировано Указом Президента России от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». Конкретные действия по реализации данного Указа предусматриваются принятыми и подготовленными федеральными документами.

Рассмотрим предложенные пути создания Российской Системы непрерывного мониторинга (далее Система мониторинга) информационной безопасности объектов КИИ (принятое в России определение киберпространства).

Принято, что Российская Система мониторинга, в соответствии с приведенным ранее определением, будет являться централизованной, иерархической, территориально распределенной структурой, включающей силы и средства обнаружения и предупреждения компьютерных атак, а также органы управления различных уровней, в полномочия которых входят вопросы обеспечения автоматизированных систем управления КВО и иных элементов КИИ. В составе Системы мониторинга предполагается создание и ввод в эксплуатацию Ситуационного Центра Системы и Ситуационных центров регионального и ведомственного уровней (второй и третий этапы реализации «Основных направлений....» – 2014-2020 гг.). На втором этапе также должен быть разработан регламент функционирования Системы мониторинга, определяющий взаимодействие КВО с Системой и органами, ответственными за обеспечение безопасности

Система мониторинга должна обеспечивать в части безопасности автоматизированных систем КВО критической инфраструктуры:

- выявление признаков проведения компьютерных атак, определение их источников, методов осуществления и направленности;
- организацию и осуществление взаимодействия на национальном и межгосударственном уровнях в области обнаружения компьютерных атак и установления их источников;
- научные исследования в области создания средств и методов обнаружения, предупреждения и ликвидации последствий компьютерных атак;
- осуществление мероприятий по оперативному реагированию на компьютерные инциденты;
- поиск и выявление компьютерных атак, а также ликвидацию последствий компьютерных инцидентов;
- сбор и анализ сведений о выявленных уязвимостях программного обеспечения и оборудования, а также средствах и способах проведения компьютерных атак;
- организацию и осуществление международного обмена информацией о выявленных угрозах, обмена лучшими практиками выявления и устранения уязвимостей и реагирования на компьютерные инциденты;
- оценку реального уровня защищенности информационных систем и информационно-телекоммуникационных сетей.

На основании сравнения основных положений и функций Системы мониторинга РФ и Комплекса мониторинга информационной безопасности КВО, созданного в США, можно сделать некоторые заключения, например:

- в США структура и состав Комплекса более сложны, Комплекс объединяет системы и центры мониторинга компьютерных атак, функционирующие в МО, разведывательных агентствах, федеральном правительстве, ряде Министерств, что позволяет Комплексу иметь информацию по более широкому кругу объектов;
- в США в МВБ создан управляющий орган и специальный Центр, выполняющие функцию координатора Комплекса;
- США начали создавать Комплекс мониторинга информационной безопасности в начале 2000 гг., однако, сегодня в США существует мнение, что проблемы обеспечения кибербезопасности в стране еще не решены и это требует достаточно больших усилий как со стороны государства, так и со стороны бизнеса и общества.

Можно надеяться, что создатели отечественной Системы учтут опыт США и постараются устранить те ее отличия от Комплекса, которые делают его априори более эффективным.

Третье перспективное направление развития систем обеспечения кибербезопасности ориентировано на переход к опережающему реагированию на внешние и внутренние возмущения (кибер-атаки) за счет разработки новых методов и средств решения задач обеспечения безопасности КВО, что связано с появлением новых видов угроз (кибер-атаки), новых целей, на которые они ориентированы, и тенденцией к постоянному увеличению их числа, разнообразия и повышенной опасности.

В новых условиях возможной реализации кибер-атак на все автоматизированные системы объектов КИИ, современная система обеспечения кибер-безопасности КВО должна работать на принципе «предвидения опасности», а не на основе традиционного – принципа реагирования «после уже случившегося». Все специалисты – американские и российские считают, что для этого должны быть реализованы, **во-первых**, тщательный мониторинг уже имевших место нападений, **во-вторых**, для выявления и анализа существующих и возможных кибер-атак управление в системе должно строится на основе управления рисками возникновения чрезвычайной ситуации на объекте при невыполнении нормативных требований и, **в-третьих**, создание и широкомасштабное применение новых методов и средств защиты известных уязвимостей автоматизированных систем КВО.

Поскольку вопросы и проблемы создания системы мониторинга были рассмотрены ранее, то здесь лишь ограничимся утверждением, что без такой системы обеспечение принципа опережения опасности кибер-атак невозможно.

Важным условием создания эффективных систем кибербезопасности КВО является повсеместный переход на управление рисками возникновения чрезвычайной ситуации на объекте. Этот метод давно известен и особенно эффективен при управлении в условиях возможности воздействия на объект множества слабо определенных потенциальных угроз. Метод позволяет вычислить оценки рисков реализации угроз в данной критической точке объекта при невыполнении комплекса нормативных требований по обеспечению безопасности – защиты – критической точки. Несмотря на известные преимущества этот метод ни в США, ни в России широко не используется. Это связано с малым числом методических разработок как в теоретическом, так и в практическом плане.

В США проблеме широкого использования управления по рискам посвящен приказ Президента США от 12 февраля 2013 г. «Executive Order 13636: Improving Critical Infrastructure Cybersecurity», в котором поставлена задача разработки документа, представляющего организациям, ответственным за кибербезопасность КВО критической инфраструктуры, единый подход для управления рисками безопасностью. Документ должен обеспечивать приоритетность, гибкость, воспроизводимость, производительность и экономическую эффективность единого подхода. Разработчиком документа явился NISN – National Institute of Standards and Technology.

Документ с названием «Cybersecurity Framework» (далее – Фрейворк) представляет собой общий язык для описания, понимания и управлениями как внешними, так и внутренними рисками кибербезопасности (или, как это принято в наших документах – информационной безопасности). Документ рассчитан на применение предлагаемого подхода организациями любого уровня – от отдельного подразделения до картеля. Предполагается, что он может быть использован для стандартизации процедур проведения оценок рисков, выделения наиболее опасных воздействий и соответствующих активных мероприятий по их парированию и обеспечению кибербезопасности объекта защиты.

Необходимо отметить, что в Распоряжении Президента США было указано, что утверждению документа должно предшествовать широкое обсуждение проекта экспертами и специалистами, поскольку предполагается его обязательное применение не только в государственных, но и в корпоративных КВО.

К сожалению, достоверная информация о практическом применении управления по рискам в действующих автоматизированных системах управления обеспечением безопасности КВО, а, тем более, обеспечения в них кибербезопасности отсутствует. Известно, что ряд НИИ разрабатывали системы управления по рискам, но точных данных по их внедрению нет. Во всяком случае, разработок в общегосударственном масштабе методических и регламентирующих документов типа «Cybersecurity Framework» в нашей стране не проводилось.

Все это позволяет утверждать, что и по этому перспективному направлению повышения эффективности систем обеспечения безопасности КВО наша страна также отстает от США.

Четвертое перспективное направление развития систем обеспечения кибербезопасности – переход на приоритетное применение электронных, телекоммуникационных средств, программно-аппаратных и проектных решений, в особенности в АСУ ТП, отечественной разработки и производства жизненно важно именно для нашей страны. Перспективность и значимость этого направления очевидна, существенные уязвимости автоматизированных систем КВО связаны именно с тем, что в таких системах используются зарубежные программные и аппаратные средства, проектные решения. Уже известны случаи использования известных уязвимостей базовой для АСУ ТП операционной системы Windows XT как пути реализации кибер-атак. Такие же уязвимости имеются и в таких, например, элементах АСУ ТП как SCADA. Опасность указанных уязвимостей, а также элементов телекоммуникационных систем, усугубляется тем, что применение для их защиты каких либо средств их защиты невозможна. Это связано с тем, что все эти устройства и программные средства являются интеллек-

туальной собственностью зарубежных фирм и какое либо их изменение запрещено. При этом регламентное обслуживание всего зарубежного оборудования выполняется только фирмами – производителями, контроль за действиями которых практически невозможен.

Данная проблема рассматривается в имеющихся директивных документах как одна из важнейших и в них предлагается принять меры на уровне государства по ее решению.

Рассмотрим основные отраженные в документах известные проблемы и предлагаемые для их решения мероприятия.

Основной источник (до 75-80%) потенциальных кибер-угроз – это пресловутый «человеческий фактор», т.е. те непредумышленные и враждебные действия персонала, которые способствуют возможности реализации или сами являются кибер-атаками. Как показывает практика, что в США, что в России эти действия имеют одну причину – низкие профессиональная подготовленность и дисциплина в области обеспечения информационной безопасности всех специалистов, занятых проектированием, руководством и эксплуатацией автоматизированных систем, обеспечивающих функционирование КВО.

Решение этой проблемы требует изменения системы подготовки специалистов в области обеспечения всех аспектов безопасности КИИ– безопасности используемых проектных решений, информационной безопасности автоматизированных систем, применения известных методов защиты, методов оценки уязвимостей системы и их ликвидации или защиты. Причем, такая подготовленность необходима не только для молодых специалистов, но и для руководящего состава объекта.

Другая важная проблема – отсутствие полной гаммы регламентирующих документов, определяющих конкретные действия всех работающих в системах управления КИИ по предотвращению и ликвидации последствий кибер-атак. При этом уже приняты и/или подготовлены основные директивные документы, определяющие государственную политику обеспечения кибербезопасности. Кстати, именно то, что в США регламенты, обеспечивающие реализацию положений директивных документов, готовятся и принимаются с минимальной задержкой по времени, и являются нашим существенным отличием от них.

Соответственно, мероприятие, определяющее решение данной проблемы — подготовка и принятие необходимых регламентов обеспечения безопасности автоматизированных систем КВО.

Третья проблема — использование элементов и проектных решений зарубежных производителей, в особенности в АСУ ТП, что часто ограничивает возможности применения решений и элементов обеспечения безопасности автоматизированных систем КВО. Решение этой проблемы – переход на создание и применение электроники и проектных решений отечественной разработки.

И, наконец, последняя проблема, ради которой и была проведена вся предыдущая аналитика — необходимость проведения широкомасштабных научных исследований по таким сложным вопросам как, например, проблема доверительности и восстанавливаемости программного обеспечения и технических средств реализации информационно-телекоммуникационных технологий, проблема создания новых комплексных антивирусных комплексов и средств индикации реализации кибер-атак, проблема разработки и создания типовых автоматизированных систем обеспечения комплексной безопасности КВО информационной инфраструктуры, объединенных с системой мониторинга возможных компьютерных инцидентов.

Для решения этой проблемы в директивных документах предусматривается разработка и финансирование плана научных исследований.

Заключение

В заключении можно сделать ряд выводов.

В настоящее время, в условиях постоянного роста количества и сложности потенциальных угроз нарушения нормального режима функционирования объектов КИИ, состояние работ по созданию и применению современных систем по обеспечению безопасности таких объектов в России, по сравнению с США, имеет значительное отставание практически по всем направлениям.

Причин для этого несколько:

- недостаточное количество директивных и регламентирующих документов федерального, ведомственного и объектового уровня;
- отсутствие стабильной государственной и ведомственной поддержки научным исследованиям проблем обеспечения безопасности КИИ;
- отсутствие необходимых стандартов, определяющих требования и условия обеспечения безопасности объектов КИИ;
- недостаточное внимание со стороны руководства КВО к обеспечению безопасности, повышению уровня дисциплины сотрудников при выполнении имеющихся нормативных требований по безопасности;
- низкий уровень профессиональной подготовки специалистов среднего и высшего уровня управления объектов КИИ;
- отсутствие четко установленной и утвержденной организационной структуры на общегосударственном уровне, обеспечивающей управление всеми работами и процессами, определяющими обеспечение безопасности объектов КИИ и, как следствие, «размывание» ответственности между различными ведомствами как бы ответственными, но каждое только за «свой» раздел.

Можно надеяться, что большинство отмеченных недостатков будет устранено в ближайшее время, поскольку проблема обеспечения комплексной безопасности КВО в условиях роста кибер-угроз становится все более и более значимой и требующей ускоренного решения.

Список литературы:

1. White Paper/ The Clinton Administration`s Policy on Critical Infrastructure Protection: Presidential decision Directive 63. May 22, 1998.
2. ESET: новый червь Win32/Stuxnet атакует промышленные компании/ Источник: http//www.esetnot32ru/ company/press/ index.php?id=7952#
3. Обзор инцидентов информационной безопасности АСУ ТП зарубежных государств. Источник: http//www.securitylab.analitics/398184.php
4. **Митрейкин А.** Некоторые аспекты обеспечения безопасности АСУ ТП в ТЭК России // «Информационные ресурсы России». №4, 2011г
5. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (16 июля 2012 года). Источник: http://www.belvpo.com/en/13419.html
6. Федеральный Закон Российской Федерации «О транспортной безопасности» от 09.03.2009 №16-ФЗ.
7. **Гриняев С.** США развертывает национальную систему информационной безопасности. – М. Изд. Центр стратегических оценок и прогнозов. 2000.
8. Распоряжение Правительства РФ от 23.03.2006 №411 с «Об утверждении перечня критически важных объектов Российской Федерации».
9. **Чернобровцев А.** Информационная безопасность промышленных предприятий.
10. Источник — http//www.osp.ru/news/articles/2013/44/1308544/
11. **Паганини П.** SCADA и безопасность стратегической инфраструктуры.
12. Источник — http//articles/antivirus/ua/cjntent/scada-i-,tzopasnost-strate
13. **Баскаков А.В.** Проблемы обеспечения непрерывности безопасности бизнеса на уровне АСУ ТП. Источник:http//journal.itmane.ru/node/1015
14. **Пашков В.** Информационная безопасность США
15. Источник – http//pentagonus.ru/publ/informacionnaja_bezopasnost_ssha
16. **Лукацкий А.** Обзор мировых стандартов МБ АСУ ТП и советы по их применимости в российских условиях. Изд. CISCO
17. **Кононов А.А., Стиславский А.Б., Цыгичко В.Н.** Управление рисками нарушения транспортной безопасности. – М. Изд. As Trust. 2008г.
18. Improving Critical Infrastructure Cybersecurity, Executive Order 13636. Preliminary Cybersecurity Framework.
19. Проект Федерального Закона «О безопасности критической информационной инфраструктуры Российской Федерации».
20. European Commission. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 7.2.2013 Brussels.
21. Федеральный Закон Российской Федерации «О безопасности» от 28.12.2010 № 390-ФЗ.
22. **Фролов А., Фролов Г.** Методы и средства защиты от компьютерных вирусов.
23. Источник – http//www.frolov-lib.ru/antivirus/articles_pl
24. www.kasperski.ru
25. Internet World Stats. Usage and population statistics.
26. Источник – http//www/internetworldstats.org.
27. **Бедрицкий А.** Международные договоренности по киберпространству: возможен ли консенсус? Источник — http//www.perspektivy/ info// oykumena/amerika/mezdunarodno

УДК 004

К ВОПРОСУ РАЗРАБОТКИ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

О.С. Макаров, М.А. Вус, Д.В. Перевалов

Материал для настоящей статьи сформировался в ходе работы авторов над подготовкой проекта изменений в существующий базовый информационный закон государств – участников СНГ при подготовке законопроекта Модельный закон «Об информации, информатизации и обеспечении информационной безопасности». Не все элементы изложенного ниже подхода к формированию правовых норм, регулирующих отношения по поводу обеспечения информационной безопасности, нашли своё отражение в итоговой рабочей версии будущего законопроекта, но они находятся в русле единой концептуальной позиции группы разработчиков и, как представляется, заслуживают отдельного внимания.

Понятие и содержание информационной безопасности. По мнению авторов, теоретическая основа формирования правовых норм, регулирующих отношения по поводу обеспечения информационной безопасности может базироваться на подходе, в рамках которого информационная безопасность представляется как социальное явление, в основе которого лежат интересы субъектов общественных отношений, каковыми являются человек, общество и государство.

«Информационная безопасность» является комплексной категорией, интегрирующей в себе технологическую, социальную и юридическую информационную безопасность и существующей в результате взаимосвязи указанных составляющих. Информационная безопасность субъекта отношений возникает и существует при условии, что вся совокупность реализуемых информационных прав и интересов данного субъекта находится в определенной степени защищенности. С правовой точки зрения информационная безопасность может рассматриваться как публично-правовой институт, следовательно, под термином «информационная безопасность» предлагается понимать общее для всех субъектов отношений состояние, характеризуемое балансом их интересов и устойчивостью.

Исходя из обозначенного посыла, информационная безопасность обладает уникальным набором идентификационных признаков:

- является состоянием, характеризующим защищенность определенной совокупности прав и интересов субъектов отношений от деструктивного воздействия определенных факторов (угроз);
- проявляется только при одновременном обеспечении заданного уровня безопасности всех реализуемых субъектом прав и интересов;
- защищаемые права и интересы представляют собой динамично развивающуюся систему;
- технологической основой развития прав и интересов являются процессы информатизации.

Результатом обеспечения информационной безопасности является создание таких условий, при которых на заданный вектор и темп развития информационных отношений не оказывают деструктивного влияния никакие внешние и внутренние факторы. Информационная безопасность не является самоцелью, а лишь обеспечивает устойчивость развития информационных отношений.

На основании изложенного, информационной безопасностью может рассматриваться как отвечающее комплексу сбалансированных интересов личности, общества и государства состояние общественных отношений по поводу информационных ресурсов, информационных технологий, информационной инфраструктуры и информационной среды в целом в условиях воздействия на них внутренних и внешних угроз.

В науке сформирована доминирующая концепция системно-структурного построения информационной безопасности, позволяющая определить ее категориальное содержание: права и интересы субъектов отношений; угрозы реализации выделенных интересов; меры противодействия угрозам обеспечения безопасности интересов.

Можно выделить следующие права и интересы субъектов информационных отношений:

- право на пользование результатами информатизации;
- свобода получения, хранения и распространения полной и достоверной информации;
- свобода мысли и слова;
- свобода массовой информации;
- свобода выражения мнений и убеждений;
- право на защиту охраняемой информации;
- право на защиту от незаконного вмешательства в личную жизнь;
- право на защиту персональных данных;
- право интеллектуальной собственности;
- право на защиту от деструктивного информационного воздействия на сознание;
- право на информационное участие граждан в государственном правлении;
- право на получение, хранение и распространение полной, достоверной и своевременной информации о деятельности государственных органов, общественных объединений;
- право на сохранение и развитие духовных и нравственных ценностей;
- право на деятельность институтов гражданского общества и возможность свободного распространения в обществе информации о данной деятельности;
- права на доступ к объектам информационной инфраструктуры;
- право на получение актуальной и достоверной информации о состоянии окружающей среды, демографической и социальной обстановке, социальных, экономических и политических процессах;
- право на защиту от пропаганды насильственного изменения конституционного строя, войны, социальной, национальной, религиозной и расовой вражды или розни;
- право на защиту от информации, пропагандирующей насилие, антиобщественное поведение и оскорбляющей моральные и культурные устои общества;
- право на защиту граждан от информационных воздействий, угрожающих их жизни и здоровью, а также нарушающих и ограничивающих их права и свободы.

Интересы государства нацелены на:

- системное информационное обеспечение реализации государственной политики, способствующее повышению эффективности и безопасности функционирования государственных институтов;
- информационное обеспечение международного сотрудничества, способствующее расширению присутствия государства на мировом экономическом рынке и рынке интеллектуальных продуктов, его не дискриминационному, равноправному участию в мировых информационных отношениях и информационном обмене, информационному обеспечению внешней политики;
- обеспечение инновационного развития, способствующее созданию современных информационных технологий, производства средств информатизации, развитию национальной индустрии информационных услуг;
- построение и безопасное развитие информационной инфраструктуры, создающие технологическую основу управления государствами (в мирное время, в чрезвычайных ситуациях и в военное время) и способствующее их взаимодействию в рамках региональных и международных организаций в информационной сфере;
- обеспечение надежности и устойчивости функционирования критически важных объектов информационно-телекоммуникационной инфраструктуры (КВОИ);
- сохранность государственных секретов;
- эффективная реализацию отношений в информационной сфере, соблюдение законов информационного общества: уважение интеллектуальной собственности, прав на доступ к информации, порядка не дискриминационного информационного обмена.

Корреспондирующей интересу категорией, противовесом, образующим состояние безопасности, является угроза безопасности. Необходимо выделить ряд актуальных характеристик угроз в информационной сфере:

- специфика информационной сферы такова, что негативные последствия реализации угроз информационной безопасности проявляются в других сферах жизнедеятельности личности, общества и государства и влияют на национальную безопасность в политической, экономической и иных сферах;
- особенность концептуальной архитектуры информационной безопасности (интересы — угрозы — меры) состоит в том, что основные угрозы часто направлены не непосредственно на общечеловеческие интересы, а воздействуют на способы их реализации (то есть специальные интересы);
- объективная закономерность, выражающаяся в том, что отказ от информатизации, а также недостаточный темп развития указанного процесса сами по себе рассматриваются как источники угроз национальной безопасности.

На современном этапе развития информационного общества сформировался комплекс актуальных угроз информационной безопасности государств – участников СНГ:

- доминирование ряда стран в мировом информационном пространстве, в сфере производства аппа-

ратных и программных средств и, соответственно, отставание ряда государств в развитии информационной инфраструктуры и систем обеспечения информационной безопасности;
- деструктивное информационное воздействие на личность, общество и государство, оказываемое посредством средств массовой информации, передачи данных в открытых телекоммуникационных сетях;
- нарушение безопасного, стабильного и устойчивого функционирования критически важных информационных инфраструктур;
- несанкционированный доступ к охраняемой информации;
- рост различных видов преступлений против информационной безопасности, включая преступления, совершаемые с использованием информационно-коммуникационных технологий.

Институт угроз является теоретической социально-политической конструкцией. В правовом поле угрозы представлены в форме составов правонарушений. Можно выделить правонарушения, непосредственно направленные на информационные интересы взаимодействующих субъектов и иные правонарушения, совершаемые с использованием информационных технологий.

Правонарушения, посягающие на информационные права и интересы личности:
- разглашение личной или семейной тайны, персональных данных, тайны голосования, тайны усыновления, врачебной, налоговой и иной охраняемой законом тайны;
- незаконные собирание либо распространение сведений о частной жизни лица;
- распространение заведомо ложных, позорящих другое лицо измышлений;
- унижение чести и достоинства личности, выраженное в неприличной форме;
- угроза причинения вреда правам и интересам лица, в том числе угроза убийства или причинения другого вреда здоровью, уничтожения имущества;
- нарушение прав лица на распространение и получение информации, в том числе, преследование за критику, отказ в предоставлении информации;
- нарушение авторских, смежных, изобретательских, патентных и иных прав на информацию.

Правонарушения, посягающие на информационные права и интересы общества:
- распространение информации, направленное на возбуждение расовой, национальной, религиозной вражды или розни, на унижение национальной чести и достоинства;
- разглашение коммерческой, банковской, следственной и иной охраняемой законом тайны;
- неправомерный отказ в доступе к информации либо неправомерное ограничение такого доступа;
- установление незаконных мер ограничения доступа к информации или к информационно-коммуникационной системе;
- воспрепятствование законной профессиональной деятельности журналиста;
- незаконное использование либо разглашение конфиденциальных сведений, охраняемых законом;
- дискредитация деловой репутации хозяйственного общества;
- распространение ложной информации о товарах и услугах;
- нарушения порядка распространения информации в период выборов и референдумов;
- нарушения установленного порядка распространения продукции средств массовой информации, религиозной информации, информации о нацистской символике или атрибутике;
- изготовление и (или) распространение, а равно хранение с целью распространения экстремистских материалов;
- незаконное ограничение свободы массовой информации;
- распространение информации, запрещённой к распространению, в том числе порнографических материалов, материалов, пропагандирующих культ насилия и жестокости;
- оскорбление или порочение государственных и других национальных языков;
- похищение либо собирание незаконным способом сведений, составляющих коммерческую или банковскую тайну;
- сокрытие либо умышленное искажение сведений, обязательных для публичного распространения, в том числе информации о загрязнении окружающей среды;
- несообщение информации об опасности для жизни людей;
- угроза совершением акта терроризма;
- заведомо ложное сообщение, в том силе об опасности;
- изменение, уничтожение, или блокирование информации, хранящейся в компьютерной системе, сети или на машинных носителях;
- разработка, использование либо распространение вредоносных компьютерных программ;
- призывы к организации или проведению массовых беспорядков, к незаконным организации или проведению массовых мероприятий;
- нарушение порядка распространения рекламы;
- распространение ложной информации о товарах и услугах;

- нарушение требований законодательства по ограничению доступа пользователей интернет-услуг к информации, запрещенной к распространению в соответствии с законодательными актами;
- нарушение порядка документирования информации и её использования, в том числе, получения и использования материалов скрытой аудио- и видеозаписи, кино- и фотосъемок;
- нарушение правил хранения документированной информации;
- неправомерное ограничение права на распространение информации, в том числе массовой информации;
- распространение информации при отсутствии возможности отказаться от её получения;
- нарушение порядка использования радио-, теле-, видео-, кинопрограмм, документальных и художественных фильмов, а также информационных компьютерных файлов и программ обработки информационных текстов, относящихся к специальным средствам массовой информации, связанного с применением скрытых вставок и иных технических приемов и способов распространения информации, воздействующих на подсознание людей и (или) оказывающих вредное влияние на их здоровье;
- нарушение возрастных ограничений при распространении продукции средств массовой информации;
- распространение в средствах массовой информации, а также в компьютерных сетях сведений, которые могут быть использованы для причинения вреда здоровью или нарушения общественной безопасности, в том числе о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ, их прекурсоров и аналогов, а также взрывчатых веществ и огнестрельного оружия.

Правонарушения, посягающие на информационные права и интересы государства:

- распространение в любой форме взглядов, идей или призывов с целью вызвать агрессию одной страны против другой;
- разглашение сведений, составляющих государственные секреты и служебной информации ограниченного распространения;
- нарушение авторских, смежных, изобретательских, патентных и иных прав государства на информацию;
- выдача иностранному государству, иностранной организации или их представителю государственных секретов;
- передача, похищение, собирание или хранение с целью передачи иностранному государству, иностранной организации или их представителю сведений, составляющих государственные секреты;
- призывы к действиям, направленным в ущерб внешней безопасности государства, его суверенитету, территориальной неприкосновенности, национальной безопасности и обороноспособности;
- унижение чести и достоинства представителя власти, выраженное в неприличной форме.

Обеспечение информационной безопасности. Обеспечение информационной безопасности — это деятельность выделенной социальной подсистемы безопасности по выявлению и нейтрализации угроз защищаемым правам и интересам. Обеспечение информационной безопасности представляет собой систему правовых, организационных и технических мер, реализуемых уполномоченными государственными органами и иными организациями.

Объектами обеспечения информационной безопасности выступают человек, общество и государство, их права и интересы, связанные с информационными ресурсами, информационными технологиями, информационной инфраструктурой, и реализуемые в информационной среде. Государство, общественные объединения и граждане участвуют в обеспечении международной информационной безопасности.

Публично-правовая сущность информационной безопасности выделяет в качестве регулятора складывающихся в связи с ее обеспечением отношений государство. Следовательно, в целях обеспечения информационной безопасности (как комплексного социально-правового явления) государство решает следующие задачи:

- обеспечивает реализацию конституционных прав и свобод граждан в информационной сфере;
- обеспечивает реализацию государственной информационной политики;
- обеспечивает безопасность процессов информатизации, построение национальной информационной инфраструктуры, формирование информационного общества;
- обеспечивает защиту информационных ресурсов, в том числе, содержащих информацию о личной жизни граждан, их персональные данные, государственные секреты и иные сведения, охраняемые в соответствии с законодательством;
- оказывает противодействие деструктивному информационному воздействию на сознание человека, информационную инфраструктуру и информационную среду;
- обеспечивает безопасность развития средств и систем информатизации, информационно-телекоммуникационных технологий;
- осуществляет борьбу с преступностью в информационной сфере, расследование правонарушений против информационной безопасности, примене-

ние мер ответственности за правонарушения в информационной сфере;
- обеспечивает защиту критически важных объектов информатизации;
- осуществляет защиту национального сегмента информационного пространства.

Характерная особенность, обуславливающая сложность правового обеспечения информационной безопасности заключается в том, что в информационной сфере формируются два вида отношений обеспечения информационной безопасности: обеспечение свободы поиска, сбора хранения, распространения информации и обеспечение прав и интересов субъектов отношений, связанных с упорядочением оборота информации (в том числе с установлением определённых запретов на доступ к ней).

Отношения, связанные с безопасностью информационной инфраструктуры, требуют регламентации и упорядочением оборота информации в ней. Изложенное (в условиях начального этапа формирования информационных правоотношений) требует определения основных правовых принципов обеспечения информационной безопасности, чтобы процессы информатизации не несли угрозу субъектам отношений, а обеспечение безопасности субъектов не сдерживало информационное развитие цивилизации.

Основными принципами обеспечения информационной безопасности являются:
- свобода поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией;
- ограничение распространения и (или) предоставления информации только законодательными актами;
- обеспечение безопасности личности, общества и государства при пользовании информацией и применении информационных технологий;
- правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса;
- баланс интересов личности, общества и государства в информационной сфере: баланс интересов распространителей и получателей информации, обладателей информационных ресурсов и лиц, осуществляющих доступ к ним;
- ответственность субъектов информационной безопасности за нарушения законодательства в информационной сфере;
- открытость деятельности по обеспечению информационной безопасности, предусматривающей информирование общества об обеспечении информационной безопасности с учетом ограничений, установленных законодательством;
- гармонизация и интеграция с международными системами информационной безопасности.

Специальным принципом правового регулирования обеспечения информационной безопасности является принцип «безопасность через развитие», определяющий в качестве основного условия обеспечения информационной безопасности стабильную динамику развития информационных средств реализации сбалансированных интересов личности, общества и государства.

Меры обеспечения информационной безопасности. Информационная безопасность обеспечивается применением системы организационных, правовых и технических мер. В их числе:
- меры предупреждения возникновения угроз информационной безопасности, включающие профилактическое воздействие на субъектов информационных отношений, мониторинг угроз информационной безопасности, устранение причин и условий их возникновения;
- меры по локализации угроз и пресечению правонарушений в информационной сфере;
- компенсационные и иные меры ликвидации последствий реализовавшихся угроз информационной безопасности.

К правовым мерам обеспечения информационной безопасности относятся:
- закрепление общеобязательных правил поведения в области обеспечения информационной безопасности, определение круга противоправных деяний, формирование перечня ограничений реализации информационных отношений в целях защиты прав и законных интересов субъектов взаимодействия. Определение условий введения данных ограничений;
- подготовка и издание нормативных правовых актов, в том числе, устанавливающих ответственность за преступления против информационной безопасности;
- разработка правовых механизмов регулирования отношений в информационной сфере;
- определение статуса субъектов обеспечения информационной безопасности, законодательное разграничение их полномочий;
- определение статуса информации, информационных ресурсов и систем, оснований и порядка доступа к ним;
- определение механизмов выявления и расследования правонарушений в информационной сфере, процедур привлечения к уголовной, административной и иным видам ответственности.

Организационные меры обеспечения информационной безопасности включают:
- совершенствование механизмов реализации прав граждан на получение, хранение, пользование и

распоряжение информацией, в том числе с использованием современных информационно-коммуникационных технологий, поступательное развитие информационного общества в целях достижения уровня ожидаемых результатов, определенных национальными документами стратегического планирования;

- формирование системы субъектов, осуществляющих правоприменительную деятельность по предупреждению, выявлению и пресечению правонарушений в информационной сфере и преступлений против информационной безопасности, организация их координации и взаимодействия;
- установление режимов информационной безопасности, в том числе режимов ограничения доступа к информации;
- организация и совершенствование деятельности по защите государственных секретов, а также по защите информации в государственных информационных системах, а также в информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено;
- создание системы обеспечения надежности и устойчивости функционирования критически важных объектов информатизации, разработка и внедрение современных методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которых могут причинить ущерб национальной безопасности;
- формирование системы мониторинга показателей и характеристик информационной безопасности в основных сферах жизнедеятельности государства;
- формирование системы информационного противоборства, противодействия информационной деятельности зарубежных государств, международных и иных организаций, отдельных лиц, наносящей ущерб интересам государства;
- разработка программ обеспечения информационной безопасности, совершенствование системы планирования и финансирования работ, связанных с реализацией правовых, организационных и технических методов обеспечения информационной безопасности;
- осуществление надзора и контроля за законностью деятельности граждан, организаций, государственных органов и должностных лиц в информационной сфере;
- лицензирование деятельности, регистрации и стандартизация работ и услуг, сертификации продукции и товаров в области обеспечения информационной безопасности;
- создание системы страхования информационных рисков физических и юридических лиц;
- определение механизмов выявления и расследования правонарушений в информационной сфере, совершенствование процедур привлечения к ответственности;
- развитие международного сотрудничества в сфере обеспечения защиты информации в международных телекоммуникационных системах и системах связи.

К техническим мерам обеспечения информационной безопасности относятся:

- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;
- использование криптографических средств защиты информации, а также систем контроля доступа и регистрации фактов доступа к информационной системе;
- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;
- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;
- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;
- формирование единой защищенной системы электронного документооборота и средств электронной цифровой подписи государственных органов.

Использование мер обеспечения информационной безопасности не должно нарушать права и законные интересы граждан, причинять вред или создавать угрозу причинения вреда их здоровью и имуществу.

Защита информационных ресурсов. Защита информационных ресурсов осуществляется посредством:

- определения общедоступной информации и закрепления запрета на ограничения ее распространения;

- определения категорий охраняемой информации и введения запрета на ее распространение;
- определение правил формирования информационных ресурсов, требований к обработке, хранению и использованию информации в них;
- закрепление прав на информационные ресурсы, выделение категорий субъектов отношений по поводу информационных ресурсов и определение их правового положения;
- определение противоправных деяний в отношении информации, закрепление ответственности за их совершение.

Обеспечение безопасности информационной инфраструктуры. Обеспечение безопасности информационной инфраструктуры осуществляется посредством:

- установления требований к надежности и безопасности используемых в ней аппаратных и программных средств (сертификации), проверки соответствия указанным требованиям;
- установления предписаний на обязательное использование отдельных средств и элементов информационной инфраструктуры;
- лицензирования отдельных видов деятельности по созданию и поддержке элементов и объектов информационной инфраструктуры;
- установления требований к необходимому уровню квалификации лиц, осуществляющих отдельные виды деятельности на объектах информационной инфраструктуры;
- выделения критически важных объектов информационной инфраструктуры, установления и нормативного закрепления дополнительных требований к обеспечению их безопасности;
- установления ограничения оборота отдельных видов аппаратных и программных средств, используемых на объектах информационной инфраструктуры.

Обеспечение безопасности информационной среды. Обеспечение безопасности информационной среды осуществляется посредством:

- обеспечения свободы средств массовой информации, определения правил распространения массовой информации;
- определения категорий информации, распространение которой оказывает деструктивное воздействие на сознание человека, национальную безопасность;
- определения категорий информации, распространение которой нарушает законные права и интересы граждан.

Способы правового регулирования обеспечения информационной безопасности. Правовое обеспечение информационной безопасности реализуется посредством введения необходимых ограничений и предписаний. Основной формой правового регулирования обеспечения информационной безопасности выступает правовой режим.

Ограничения (запреты) в сфере обеспечения информационной безопасности:

- *на распространение информации:*
  - экстремистского характера,
  - порнографического содержания, материалов, пропагандирующих культ насилия и жестокости,
  - информации, содержащей призывы к насильственному свержению конституционного строя,
  - информации, содержащей призывы к организации или проведению массовых беспорядков, к незаконным организации или проведению массовых мероприятий;
  - сведений, которые могут быть использованы для причинения вреда здоровью или нарушения общественной безопасности, в том числе о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ, их прекурсоров и аналогов, а также взрывчатых веществ и огнестрельного оружия;
  - информации, причиняющей вред здоровью и (или) развитию детей, оказывающей деструктивное информационное воздействие на личность,
  - информации содержащей пропаганду, войны, социальной, национальной, религиозной и расовой вражды или розни;
  - информации направленной на возбуждение расовой, национальной, религиозной вражды или розни, на унижение национальной чести и достоинства,
  - информации содержащей персональные данные гражданина;
  - информации, составляющей государственные секреты;
  - сведений, содержащих служебную информацию ограниченного распространения (служебную тайну);
  - сведений, составляющихй коммерческую тайну;
  - заведомо ложной, позорящей другое лицо информации;
  - информации, унижающей честь и достоинство лица, а также честь и достоинство представителя власти;
  - информации дискредитирующей деловую репутацию хозяйственного общества,

- информации содержащей ложные сведения о товарах и услугах,
- информации содержащей заведомо ложное сообщение, в том силе об опасности;
- информации содержащей угрозы причинения вреда правам и интересам лица, в том числе, угрозу убийства или причинения другого вреда здоровью, уничтожения имущества, угроза совершения акта терроризма;
- иной информации при отсутствии возможности отказаться от её получения;

- ***на сбор информации:***
  - содержащей тайну личной жизни лица;
  - содержащей персональные данные гражданина;
  - составляющей государственные секреты;
  - составляющей служебную информацию ограниченного распространения (служебную тайну);
  - составляющей коммерческую тайну;
  - составляющей профессиональную тайну;
  - для передачи ее иностранному государству, иностранной организации или их представителю в ущерб национальной безопасности государства;
- ***на использование информации:***
  - составляющей объекты авторского права и смежных прав, права промышленной собственности в нарушение прав их обладателей;
  - на использование вредоносных компьютерных программ;
- ***на наложение ограничений оборота информации:***
  - ограничение распространения общедоступной информации;
  - осуществление цензуры.

Предписания (*позитивное обязывание*) в сфере обеспечения информационной безопасности:

- ***на обязательное распространение информации:***
  - общедоступной по запросу граждан;
  - информации о правах, свободах и законных интересах физических лиц, правах и законных интересах юридических лиц и о порядке реализации прав, свобод и законных интересов;
  - о деятельности государственных органов;
  - о чрезвычайных ситуациях, экологической, санитарно-эпидемиологической обстановке, гидрометеорологической и иной информации, отражающей состояние общественной безопасности;
  - о состоянии преступности, а также о фактах нарушения законности;
  - информации, накапливаемой в открытых фондах библиотек и архивов, информационных системах государственных органов, физических и юридических лиц, созданных (предназначенных) для информационного обслуживания физических лиц;
- ***на соблюдение порядка:***
  - распространения продукции средств массовой информации, религиозной информации, информации о нацистской символике или атрибутике;
  - распространения рекламы;
  - документирования информации и её использования, в том числе, порядка получения и использования скрытой аудио- и видеозаписи, кино- и фотосъемок;
  - правил хранения документированной информации;
  - использования радио-, теле-, видео-, кинопрограмм, документальных и художественных фильмов, а также информационных компьютерных файлов и программ обработки информационных текстов, относящихся к специальным средствам массовой информации, связанного с применением скрытых вставок и иных технических приемов и способов распространения информации, воздействующих на подсознание людей и (или) оказывающих вредное влияние на их здоровье;
  - хранения информации в компьютерной системе, сети или на машинных носителях;
  - возрастных ограничений при распространении продукции средств массовой информации;
  - лицензирования отдельных видов деятельности;
  - сертификации отдельных элементов и комплексов информационно-коммуникационной инфраструктуры.

Система обеспечения информационной безопасности. Систему обеспечения информационной безопасности составляет совокупность взаимодействующих органов государственного управления, ответственных за осуществление государственной политики в области обеспечения информационной безопасности, других субъектов обеспечения национальной безопасности и реализуемых ими мер и методов по защите национальных интересов в информационной сфере. Система обеспечения информационной безопасности является составляющей системы обеспечения национальной безопасности.

В качестве конфигурации национальной системы субъектов обеспечения информационной безопасности предлагается рассматривать двухуровневую модель, состоящую из подсистем:

- государственного управления в области обеспечения информационной безопасности (субъектами такой подсистемы являются: Президент, Совет Министров, Совет Безопасности, органы государ-

ственного управления, ответственные за осуществление государственной политики в области обеспечения информационной безопасности);

- обеспечения информационной безопасности (такую подсистему образуют: государственный орган-координатор, органы-исполнители в области обеспечения информационной безопасности, другие субъекты обеспечения национальной безопасности). Подсистема обеспечения информационной безопасности является составной частью системы обеспечения национальной безопасности).

Основными функциями системы обеспечения информационной безопасности являются:

- реализация и совершенствование организационных, научно-технических, правовых, экономических и иных основ обеспечения информационной безопасности;
- организация и проведение мониторинга, анализа и оценки состояния информационной безопасности, выявление и прогнозирование внутренних и внешних рисков, вызовов и угроз информационной безопасности;
- реализация приоритетных направлений обеспечения информационной безопасности;
- разработка и практическая реализация комплекса мер по предупреждению, выявлению и нейтрализации информационных рисков, вызовов и угроз;
- разработка и своевременная корректировка индикаторов (показателей) состояния информационной безопасности, критериев эффективности деятельности субъектов ее обеспечения.

Президент, как субъект государственного управления в области обеспечения информационной безопасности:

- определяет государственную политику;
- определяет государственные органы, ответственные за обеспечение информационной безопасности и их компетенцию;
- осуществляет общее руководство системой обеспечения информационной безопасности в рамках управления системой обеспечения национальной безопасности;
- утверждает государственные программы в области обеспечения информационной безопасности.

Совет Министров, как субъект государственного управления в области обеспечения информационной безопасности в пределах своей компетенции:

- реализует через подчиненные ему органы государственного управления и организации государственную политику в области обеспечения информационной безопасности;
- разрабатывает документы стратегического характера в области обеспечения информационной безопасности и развития национальной информационной инфраструктуры;
- определяет правовой статус государственных органов и организаций в области информационной безопасности;
- принимает нормативные правовые акты в области обеспечения информационной безопасности;
- обеспечивает создание необходимых правовых, экономических, организационных и других условий, способствующих обеспечению защиты интересов личности, общества и государства от деятельности, направленной на причинение ущерба информационной безопасности;
- организует эффективное функционирование системы обеспечения информационной безопасности;
- обеспечивает удовлетворение потребностей органов государственного управления в необходимых финансовых и материальных ресурсах для реализации мер обеспечения информационной безопасности;
- утверждает государственные программы научно-исследовательских и опытно-конструкторских работ в интересах обеспечения информационной безопасности.

Совет Безопасности в пределах своей компетенции, как субъект в области обеспечения информационной безопасности:

- рассматривает вопросы информационной безопасности, затрагивающие интересы личности, общества и государства, принимает по ним решения;
- определяет приоритетные направления обеспечения информационной безопасности;
- вносит предложения Президенту по вопросам государственной политики в области обеспечения информационной безопасности.

Уполномоченный государственный орган-координатор обеспечения информационной безопасности:

- определяет пороговые значения индикаторов (показателей) состояния информационной безопасности;
- анализирует источники возникновения информационных конфликтов, разрабатывает меры по предотвращению развития информационных кризисов;
- разрабатывает и совершенствует комплекс стратегических мер по предупреждению, выявлению и нейтрализации информационных рисков, вызовов и угроз;
- готовит материалы по вопросам соблюдения информационных прав и свобод граждан для доклада Президенту. Обеспечивает Президента и по его поручениям соответствующие государственные органы и организации информационно-аналитическими материалами по вопросам обеспечения информационной безопасности;

- обеспечивает реализацию государственной информационной политики;
- координирует деятельность государственных органов и иных организаций по обеспечению информационной безопасности и осуществляет контроль за реализацией мер в данной области.

Органы-исполнители в области обеспечения информационной безопасности:

- организуют, координируют и контролируют деятельность государственных органов и иных организаций по вопросам технической защиты информации;
- предупреждают, выявляют и пресекают противоправную деятельность, направленную на причинение ущерба информационной безопасности;
- реализуют законные полномочия в области государственных секретов (тайны);
- принимают предусмотренные законодательством меры по недопущению незаконного ограничения свободы массовой информации, осуществления цензуры, распространения информации, размещение которой в средствах массовой информации запрещено, либо нарушения порядка распространения информации, доступ к которой ограничен;
- организуют проведение мониторингов интернет-ресурсов государственных органов и организаций;
- разрабатывают и утверждают правила безопасной эксплуатации и взаимодействия информационных ресурсов, систем и сетей;
- обеспечивают осуществление в соответствии с законодательством государственного надзора за деятельностью в области связи;
- осуществляют мероприятия информационного противоборства, организуют противодействие деструктивному информационному воздействию.

Обобщая вышеназванные подходы, можно определить общие критерии формирования модельной системы обеспечения информационной безопасности государства и ее институционально-субъектный состав.

Государство в лице его органов занимает ведущее место в системе обеспечения информационной безопасности, поскольку является не только выразителем национальных интересов, но и гарантом их реализации. Общество осуществляет контроль за деятельностью государства по обеспечению информационной безопасности. Гражданин обеспечивает собственную информационную безопасность посредством самозащиты прав, а также посредством участия в общественных институтах осуществляет контроль за деятельностью государства по обеспечению информационной безопасности.

По нашему мнению, современный период развития отношений в сфере обеспечения информационной безопасности позволяет перейти от уровня представлений об их правовом обеспечении к конкретным нормам, увязанным в систему. Сегодня в правовом обеспечении не стоит бояться «забежать вперед паровоза», так как общественные отношения в сфере обеспечения информационной безопасности в государствах – участниках СНГ если ещё и не в полной мере сложились, то уже приобрели определённо выраженные характерные очертания. Успешно формируются национальные и региональные системы обеспечения информационной безопасности, в стратегических концептуальных документах определены основные защищаемые интересы и приоритеты в информационной сфере, очерчен контур запретов и дозволений, получил общественное одобрение институт ответственности за нарушение информационной безопасности. Всё сказанноеё, по мнению авторов, создает достаточный базис для развития эффективного нормотворчества в сфере информационной безопасности.

Список литературы:

1. **Макаров О.С.** Правовое обеспечение информационной безопасности на примере защиты государственных секретов государств – участников Содружества Независимых Государств. Диссертация доктора юридических наук: 12.00.14. Москва, 2014.
2. **Бачило И.Л., Бондуровский В.В., Вус М.А., Кучерявый М.М., Макаров О.С.** О совершенствовании и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности // Информационное право. – М.,2013, № 1 (32). С.24-27.
3. **Бачило И.Л., Вус М.А., Кучерявый М.М., Макаров О.С.** К вопросу о концептуальных направлениях организационно-правового обеспечения информационной безопасности государств – участников СНГ // Информатизация и связь. – М., 2012, № 4. С. 4-11.
4. **Вус М.А., Макаров О.С.** К вопросу о разработке рекомендаций по совершенствованию и гармонизации национальных законодательств государств – участников СНГ в сфере обеспечения информационной безопасности» // Информатизация и связь – М., 2012, № 1. С. 5-8.
5. **Добряков С.А.** Административно-правовые меры защиты служебной информации, используемой подразделениями ГИБДД в правоохранительной деятельности: диссертация кандидата юридических наук : 12.00.14. Москва, 2008.
6. **Недосекова Е.С.** Административно-правовые аспекты обеспечения информационной безопасности таможенных органов Российской Федерации: автореферат диссертация кандидата юридических наук: 12.00.14. Люберцы, 2011.
7. **Сахно Э.Х.** Административно-правовая организация обеспечения информационной безопасности в Российской Федерации: Диссертация кандидата юридических наук : 12.00.14 Хабаровск, 2006.

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

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Цели и сфера действия закона

Настоящий модельный закон регулирует отношения в области создания и использования информационно-коммуникационных технологий в процессе информатизации жизнедеятельности общества, государства, человека, при осуществлении права на поиск, получение, распространение, передачу использование информации и обеспечении информационной безопасности.

Сферой действия настоящего модельного закона является деятельность по сближению национального законодательства и организации информационного взаимодействия субъектов в процессе формирования единого информационного пространства государств – участников Содружества Независимых Государств (СНГ).

Статья 2. Основные термины и понятия, используемые в настоящем законе

Для целей настоящего закона используются следующие понятия:

- **информация** — сведения или данные о фактах, событиях, явлениях, процессах доступные для использования независимо от способа их представления;
- **информационный объект** – информация, обладающая заданной совокупностью атрибутов (реквизитов), которые позволяют использовать её в информационных отношениях:
- **информационное пространство**—сфера деятельности и взаимодействия субъектов, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию;
- **информационное пространство** межгосударственного взаимодействия — информационное пространство каждой геополитической единицы – государства и образуемого единого информационного пространства обмена информационными ресурсами, создания и размещения комплексных интегрированных информационных ресурсов по целям сотрудничества;
- **информационная безопасность** – состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве;
- **обеспечение информационной безопасности**— деятельность по разработке и реализации системы мер правового, организационно-технического и организационно-экономического характера по выявлению угроз информационной безопасности, предотвращению их реализации, пресечению и ликвидации последствий реализации таких угроз в национальном и международном информационно-коммуникационном пространстве;
- **информационные и телекоммуникационные ресурсы**—объекты информационной инфраструктуры, а также собственно информация, выделяемая по определенному признаку и формирующаяся по целям и потребностям субъекта информационных отношений;
- **информация официальная**— информация, исходящая от органов государственной власти и органов местного самоуправления, других государственных и негосударственных органов и организаций, создаваемая, распространяемая и используемая в соответствии с правовым статусом ее источника;
- **защита информации**— деятельность, направленная на защиту прав субъектов на информацию, предотвращение несанкционированного доступа к ней и/или утечки защищаемой информации, несанкционированных и/или непреднамеренных воздействий на неё;
- **информатизация** — организационный, социально-экономический и научно-технический процесс создания благоприятных условий для удовлетворения информационных потребностей, реализации прав и свобод субъектов информационной сферы;

- **информационно-коммуникационные технологии (ИКТ)** —информационные процессы и методы работы с информацией, осуществляемые с применением средств компьютерной техники и телекоммуникаций;
- **сайт**— информационный объект в телекоммуникационной системе Интернета, предназначенный для размещения официальной или авторизованной информации для открытого доступа пользователей в телекоммуникационной сети по определенным сетевым адресам.

Иные термины и понятия, используемые в настоящем Законе, применяются в составе и значениях в соответствии с их использованием в национальном законодательстве.

Статья 3. Субъекты отношений в сфере действия настоящего закона

Субъектами отношений, реализующими права и полномочия в рамках данного закона, являются:

- органы государственной власти и местного самоуправления государств – участников СНГ;
- уполномоченные органы и организации в области формирования общих для СНГ информационных ресурсов, ИКТ; межгосударственных интегрированных информационных систем; удостоверяющих центров электронной подписи; ситуационных и консультативных центров, других структур, обеспечивающих безопасное использование ИКТ;
- граждане и организации при реализации их прав и обязанностей в информационном пространстве социально-экономического, культурного и других областей сотрудничества государств-участников СНГ;
- государственные и общественные экспертные и контрольные органы и организации в области обеспечения информационной безопасности.

Статья 4. Законодательство в области информации, информатизации и информационной безопасности

Законодательство государств – участников СНГ по регулированию отношений в области информации, информатизации и информационной безопасности включает:

- Модельный закон «Об информации, информатизации и обеспечении информационной безопасности»;
- национальное законодательство в области информации, информатизации и информационной безопасности государств Содружества Независимых Государств;
- нормативные правовые акты в области формирования и использования информации национального потенциала ИКТ в целях обеспечения прав и интересов граждан, деятельности органов государственной власти и местного самоуправления, учитывающие процессы формирования единого информационно-коммуникационного пространства СНГ при обеспечении безопасности государства, общества, человека и гражданина;
- другие законы и подзаконные акты, затрагивающие отношения в информационном пространстве.

Статья 5. Принципы правового регулирования отношений в рамках данного закона

Принципы правового регулирования отношений в рамках данного модельного закона предусматривают:

1. обеспечение свободы поиска, получения, передачи, обработки, распространения, использования и хранения информации, доступ к которой не ограничен законами государств;
2. свободный доступ к официальной информации органов государственной власти и органов местного самоуправления при обеспечении ее, достоверности, целостности, своевременности;
3. ограничение доступа к информации и обеспечение ее конфиденциальности устанавливается национальными законами государств – участников СНГ;
4. поддержание состояния безопасности информационных ресурсов, информационного обеспечения прав пользователей национальными и международными информационными системами;
5. обеспечение соблюдения государственного суверенитета государства и реализации норм международного права, норм национального законодательства в организации и реализации потенциала ИКТ в процессе информационного межгосударственного взаимодействия при регулировании отношений информационной безопасности государства, общества, человека и гражданина.

Статья 6. Основные принципы государственной политики в области информации, информатизации и обеспечения информационной безопасности

Основные принципы государственной политики в области информации, информатизации и информационной безопасности при соблюдении норм статьи 5 настоящего закона, предусматривают:

- обеспечение прав и законных интересов граждан, институтов общества и государства в информационной среде и пространстве информационного взаимодействия национальных и межгосударственных информационных систем;
- социальную направленность стратегических целей, основных задач и мероприятий, проводимых в сфере информатизации;

- ликвидацию информационного неравенства в обществе, реализацию условий для развития информационного общества;
- обеспечение доступа широких слоев граждан к информационно-телекоммуникационным сетям, информационным системам и технологиям, к системам открытого доступа к информации;
- открытость политики информатизации и активное привлечение к этой деятельности представителей науки, высшей школы и предпринимателей, работающих в информационной сфере;
- безопасность создаваемых и применяемых информационно-коммуникационных сетей, информационных технологий и систем;
- правовую, научную, техническую и экономическую обоснованность разрабатываемых и принимаемых решений;
- комплексность и системность подхода к разработке и применению информационно-телекоммуникационных сетей, информационных технологий и систем;
- системный подход к организационно-правовому обеспечению использования информационных технологий в государственном управлении, перевод реализации функций административных структур на цифровые технологии;
- развитие международного сотрудничества и использование зарубежного опыта в сфере информатизации в целях обеспечения конкурентоспособности создаваемых товаров и услуг на отечественном и мировом рынках;
- развитие законодательства в сфере информатизации, информации и обеспечения информационной безопасности.

ГЛАВА 2. ИНФОРМАЦИЯ, ИНФОРМАЦИОННЫЕ РЕСУРСЫ, ОСНОВЫ ПРАВОВОГО РЕЖИМА ИНФОРМАЦИОННЫХ РЕСУРСОВ

Статья 7. Информация и информационные ресурсы, виды и учёт информационных ресурсов

1. Информация как предмет общественных отношений является объектом прав всех видов субъектов в информационном пространстве межгосударственного взаимодействия; объектом прав и обязанностей человека и гражданина, органов государственной власти, любых видов организаций в соответствии с международным и национальным законодательством.

а). Субъект информационных отношений формирует свои информационные ресурсы и распоряжается ими в соответствии с его правовым статусом, с учетом видов, категорий информации по доступу; несет ответственность за ее безопасность и безопасное использование для общества и других субъектов информационных отношений.

б) Виды информационных ресурсов классифицируются в установленном государством порядке и могут формироваться как по субъектам, создающим и использующих информацию, так и по целям их использования, и по другим критериям. Основные массивы информационных ресурсов подлежат учёту в реестрах, регистрах и классификаторах, формируемых соответствующими органами исполнительной власти, архивами и библиотеками в электронной форме.

2. Формирование системы информационных ресурсов государства предусматривает создание систем информационных объектов, относимых к общенародному достоянию; ведомственных (отраслевых) ресурсов органов государственной власти и местного самоуправления в соответствии с их сферами ведения и полномочий; информационных систем производственных, научных и образовательных, социальных, торговых, финансовых и пр. организаций, а также общественных объединений, организаций и установление их правового режима.

Статья 8. Основы правового режима информационных ресурсов

1. Правовой режим информационных ресурсов устанавливается государствоми должен соблюдаться всеми субъектами информационной деятельности и информационных отношений.

2. Правовой режим информационных ресурсов и информационно-коммуникационных технологий включает:

- соблюдение порядка документирования информации;
- установление права собственности на определенный информационный ресурс;
- установление режима доступа и правил обеспечения безопасности этого информационного ресурса (объекта).

3. Документирование информации предусматривает:

- упорядочение номенклатуры информационных объектов, их представления в соответствующей информационной системе в письменном, или электронном виде;
- установление порядка учета и легализации факта наличия информации;
- порядок контроля соблюдения правил работы с объектами оцифрованной, электронной, бумажной официальной и другой документированной информации в государственных, корпоративных, межгосударственных информационных системах, в структуре систем международного обмена информацией, включая информационное пространство межгосударственного взаимодействия;

- установление формы собственности и (или) исключительных прав на объекты интеллектуальной собственности, включаемые в структуру информационного ресурса (базы и банки данных, объекты авторских прав). Право собственности на информационный объект реализуется через полномочия владения, распоряжения и пользования. Исключительные права авторов и других законных правообладателей на контент документа, данные или записи, содержащиеся в базах данных и других носителях текста, включаемых в информационную среду и информационное пространство межгосударственного взаимодействия, регулируются в соответствии с законодательством об интеллектуальной собственности. Если закон использует термин «обладатель», то его следует сопровождать указанием на законность такого обладания: «законный обладатель»;
- установление категории информационного объекта по доступу предполагает порядок создания и использования общедоступной информации и порядок регулирования работы с информацией конфиденциального характера;
- определение методов и форм обеспечения безопасности информационного ресурса и ответственности за нарушение правил работы с информационным ресурсом, а также установление видов и форм ответственности за нарушение правового режима информационных ресурсов или использования информационных объектов во вред правам и законным интересам государства, граждан.

Статья 9. Правовой режим открытой (общедоступной) информации

Правовой режим общедоступной информации предусматривает:

1. обеспечение обнародования и свободного распространения сведений официального характера, включающих: нормативно-правовую информацию, которая создается органами государственной власти в процессе их деятельности по управлению делами общества и государства, статистическую, экологическую, метеорологическую, миграционную, информацию о состоянии социально-экономической и культурной жизни страны; о выборах и референдумах, о состоянии законности и правопорядка, уровне преступности и других видов информации, которая предоставляется соответствующими органами через системы общественного доступа к Интернет – среде и СМИ для информирования населения государства и международной общественности и использования этой информации;
2. соблюдение права каждого субъекта свободно знакомиться с информацией, составляющей общедоступные сведения. Право на ознакомление с общедоступными сведениями и их использование не может быть ограничено. Общедоступная информация в форме открытых данных распространяется в Интернет–среде и не требует оформления процедур передачи трансграничного объекта;
3. публичное предоставление информации национальными юридическими лицами, а также иностранными юридическими лицами, осуществляющими деятельность на территории государства, осуществляется в случаях и порядке, установленных национальными законами;
4. порядок поиска и получения открытой и общедоступной информации устанавливается национальным законодательством государства путем разработки Единого Реестра общедоступной информации;
5. Получение общедоступной информации «по «обращению» не может быть связано с оформлением доступа как платной услуги.

Статья 10. Информация ограниченного доступа

1. Информация, которая относится законом к государственным секретам, к конфиденциальной информации в форме коммерческой тайны, к служебной информации ограниченного распространения, к персональным данным, к профессиональной тайне, а также тайне личной жизни, требует соответствующей идентификации и установления порядка санкционированного доступа к ней.

2. Правила использования ограничительных грифов на соответствующих носителяхинформации ограниченного доступа регулируются национальными законами.

ГЛАВА 3. ИНФОРМАТИЗАЦИЯ, ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Статья 11. Государственная политика в сфере информатизации

1. Государственная политика в сфере информатизации направлена на создание условий для эффективного удовлетворения информационных потребностей личности, общества и государства на основе обеспечения доступа к информации и использования информационных систем и технологий.

2. Основными направлениями государственной политики информатизации являются:

- обеспечение эффективности и безопасности формирования и использования информационного пространства государства, формирование единого информационного пространства взаимодействия государств-участников СНГ;

- формирование, развитие и защита ИКТ, обеспечение их совместимости и взаимодействия в едином информационном пространстве;
- развитие и использование потенциала ИКТ, создание отечественного программного продукта;
- обеспечение национальной безопасности государства, безопасности граждан и организаций в сфере использования информационно-коммуникационных систем и информационных технологий;
- создание и совершенствование системы привлечения инвестиций и механизма стимулирования разработки и реализации проектов информатизации, участия государства в международном сотрудничестве;
- обеспечение потребностей и вызовов системы государственного и межгосударственного управления современными программными и коммуникационными средствами и технологиями.

3. В целях осуществления государственной политики в сфере создания и эксплуатации информационных систем и применения ИКТ органы государственной власти и органы местного самоуправления:

- участвуют в разработке и реализации государственных целевых программ в области развития информационного общества;
- формируют и реализуют перспективные и оперативные планы и программы в области совершенствования управления на основе освоения информационных технологий, упорядочения информационных ресурсов в области предоставления услуг населению, выполнения в электронном формате всех доступных информатизации функций и операций в системе их ведения и компетенции;
- участвуют в разработке решений о межгосударственном и межотраслевом информационном взаимодействии в рамках реализации программ сотрудничества государств–участников СНГ и с другими зарубежными партнерами;
- создают специализированные органы по оценке эффективности использования информационных технологий для инноваций в управленческих процессах.

Статья 12. Организационно-правовое обеспечение реализации государственной политики в сфере информатизации

1. Механизмы организационного и правового обеспечения в области информатизации определяются в соответствии с государственной политикой как в области развития потенциала ИКТ, так и в области использования этого потенциала в системе государственного управления и обеспечения развития информационного общества, с учетом укрепления межгосударственного информационного взаимодействия.

2. Организационное обеспечение информационно-коммуникационной инфраструктуры и развития национальной базы ИКТ реализуются в режиме научно-технического производства, как самостоятельной отрасли государственной и мировой экономики.

3. Основными индикаторами успешной деятельности государственных и негосударственных структур в области информатизации являются:

- показатели освоения мирового и национального рынка, оценка работы по количественным показателям и получаемой прибыли;
- безопасность ИКТ и их применения для реализации потребностей общества и человека.

Статья 13. Формирование и структуризация информационного пространства

1. Информационное пространство рассматривается как область информационного взаимодействия государств – участников СНГ, коммуникационные связи которых реализуются преимущественно через Интернет и государственные системы СМИ, телекоммуникационные системы, мобильные формы связи, локальные информационные системы межгосударственного и внутригосударственного общения.
2. Закон определяет порядок правового регулирования отношений в области двух взаимодействующих систем: информационной инфраструктуры ИКТ – отрасли и информационной инфраструктуры электронного управления, реализуемого всей совокупностью органов государственной власти и местного самоуправления в национальном информационном пространстве, а также в пространстве информационного взаимодействия государств – участников СНГ.
3. Национальное законодательство государств – участников СНГ предусматривает:

- регулирование порядка распространения информации в Интернет с указанием лиц, осуществляющих деятельность по обеспечению функционирования информационных систем, обеспечивающих прием, передачу, доставку или обработку электронных сообщений пользователей сети Интернет;
- определяет права и обязанности организатора распространения информации, владельца сайта (и/или страницы сайта).

4. Национальные законы предусматривают порядок ведения реестра сайтов. В соответствии с настоящим модельным законом могут быть организованы информационные системы согласования структуры реестровсайтов.
5. Государственная политика информатизации Содружества Независимых Государств направлена на повышение качества жизни граждан на основе

применения информационных и телекоммуникационных технологий при реализации важнейших направлений жизни общества и выполнении управленческих функций, реализуемых всей системой органов государственной власти и местного самоуправления посредством использования продукции, создаваемой отраслью ИКТ.

Статья 14. Организационно- правовое обеспечение развития информационной инфраструктуры отрасли ИКТ

1. Организационно-правовое регулирование в области производства и эксплуатации потенциала ИКТ формируется как комплексная и объединяющая государственные, корпоративные и частные производства и средства их обеспечения система, нацеленная на обеспечение конкурентоспособности отрасли информационных технологий, на повышение качества жизни граждан, на развитие экономической, социально-политической, научно-образовательной и культурных сфер жизни общества.
2. Правительства государств – участников Содружества Независимых Государств разрабатывают и принимают перспективные программы и планы развития отрасти ИКТ и контролируют их исполнение.
3. В части правового регулирования инфраструктуры отрасли ИКТ органами исполнительной власти решаются следующие задачи:
   а) упорядочение производственных, научно-производственных структур; структур сервисного характера (ситуационные, консультативные, сопровождающие, аналитические); органов, выполняющих контрольные функции (сертификация, лицензирование); юридических служб (договоры, конфликты, угрозы, споры по производству, качеству продукции и рынку) и др.;
   б) обеспечение правил подготовки и повышения квалификации специалистов для сферы ИКТ и всех видов специалистов, задействованных а Интернет – среде (программисты, операторы, администраторы информационных систем, разного уровня провайдеры в информационном пространстве и др.) и субъектов, ответственных за безопасность среды и специализированных и локальных информационных систем;
   в) разработка и внедрение правовых документов, определяющих статус органов, подразделений, должностные обязанности и ответственность специалистовв отраслевыхи региональных системах управления;
   г) установление правил и режима работы сервисных, консультативных и сопровождающих структур по договорам с заказчиками, потребителями продукции ИКТ – сектора экономики;
   д) разработка и внедрение классификаторов и реестров продукции и сервисов, оказываемых на договорной основе сектором экономики и производства ИКТ пользователям и потребителям;
   е) анализ состояния рынка продукции ИКТ в национальном и международном обороте.

Статья 15. Организационно-правовое регулирование информационной инфраструктуры системы государственного управления

1. Организационно-правовое регулирование информационной инфраструктуры системы государственного управления решает задачи перевода функциональной деятельности аппарата государственного управления на использование ИКТ в целях электронизации процесса управления. Эта работа осуществляется в следующих направлениях:
   - обеспечение перехода на электронный документ в процессе реализации функциональных обязанностей подразделений в системе конкретного органа;
   - установление порядка использования электронной подписи;
   - обеспечение режима и правил работы с информационными ресурсами, включая служебную и деловую информацию;
   - создание информационных систем (баз и банков данных) документированной информации в соответствии со сферой ведения органа исполнительной власти (органа местного самоуправления).
   - создание автоматизированных (электронных) систем управления (АСУ, ЭСУ), на базе интеграции которых в отраслевых и региональных системах могут создаваться комплексные электронные системы государственного управления;
   - установление согласованных по технологии и целевой ориентации информационно-коммуникационных взаимодействий органов и межведомственного обмена информацией с другими субъектами в управлении делами страны;
   - создание информационных, справочных, консультационных информационных систем с учетом правового режима информационных ресурсов для обеспечения информатизации функций государственного и муниципального управления (систем открытого доступа к информации, «сервисов одного окна» по предоставлению информационных услуг гражданам и организациям);

- создание систем сбора информации и конкретных общественных инициатив населения по совершенствованию работы органов государственной власти и местного самоуправления;
- осуществление иных функций по информатизации систем законотворческих, исполнительных органов власти, судебной, нотариальной и других профилей работы по управлению делами государства и общества.

2. Оказание информационных услуг — предоставление открытой информации о деятельности органов государственной власти и органов местного самоуправления, официальной информации (данных) обеспечивается в порядке функциональной деятельности государственных и муниципальных органов, и должно осуществляться на безвозмездной основе.
3. В целях реализации программ по переводу структур государственного аппарата на расширение применения системы электронного управления создаются механизмы координации и согласования работы всех функциональных структур каждого органа и его контактов в электронной форме с другими органами системы управления, а также создаются подразделения, обеспечивающие экспертную оценку качества работы и получаемых результатов.

Статья 16. Взаимодействие органов государственного управления и местного самоуправления со структурами, создающими базу ИКТ

1. Правовое регулирование отношений органов государственного и местного самоуправления, как заказчиков продукции отрасли ИКТ с органами, компаниями, фирмами и другими организациями — исполнителями проектов информатизации государственного и местного управления — нацелено на установление ответственности каждого из участников за определенный компонент информатизации и на определение прав в распоряжении информационными ресурсами, которые находятся в обработке собственника информационной системы.
2. Отношения заказчика создания информационной системы, сайта и (или) заказчика услуг на обработку информации регулируются гражданско-правовым договором с элементами публичной ответственности с учетом масштаба и среды распространения информации.
3. С учетом определяемых приоритетов планируемых и осуществляемых мероприятий по программам и планам информатизации соответствующими структурами управления формируются показатели (индикаторы) государственных программ с указанием целевых параметров по количеству и качеству достигаемых результатов.

Статья 17. Юридическое оформление отношений субъектов в процессе информатизации: договоры, соглашения, регламенты

1. Органы государственной власти и местного самоуправления в процессе информатизации используют следующие механизмы их взаимодействия между собой и с другими субъектами:
   а) взаимодействие органов и их подразделений в структуре одной отрасли управления реализуется на основе положений о них, принимаемых руководством отраслью (ведомством) локальных нормативных актов и регламентов по вопросам информационного взаимодействия в процессе реализации функций этих структур;
   б) оформление порядка информационного взаимодействия в структуре национальной системы органов государственной власти и местного самоуправления осуществляется на основе: национальных законов; правоприменительных актов вышестоящих в системе управления органов; соглашений (публичных договоров) органов исполнительной власти между собой о порядке и условиях обмена необходимой и достаточной информацией при исполнении функций и операций, связанных с технологиями информатизации;
   в) отношения органов исполнительной власти с другими, не государственными организациями по вопросам информатизации оформляются договорами с учетом их предмета как гражданско-правовые (договора подряда, услуг, купли-продажи, выполнения НИР или НИОКР), а также как публично-правовые (в случаях использования форм аутсорсинга и отношений с субъектами облачной обработки информации). Выбор формы договора определяется номенклатурой работ в области разработки, монтажа, пуско-наладки и сопровождения объектов, предусмотренных как предмет договорных отношений.

Договор на работы, связанные с обработкой информационных ресурсов по заказу их собственника или распорядителя в соответствии с гражданско-правовым законодательством государства не может предусматривать перехода или распространения прав собственника на информационный ресурс, получаемый от заказчика и предоставляемый ему или соответствующим доверенным лицам в результате выполнения работ по его обработке.

Отношения, связанные с выполнением информационных функций органов государственной власти или органов местного самоуправления, их части или комплекса операций, затрагивающих интересы и права третьих лиц

(физических или юридических лиц), должны оформляться публичным договором в одной из двух возможных форм:

1) форма делегирования функции и соответствующих полномочий; (в случае предоставления публичных услуг не самим органом, а другой государственной организацией, реализующей, например, функции «одного окна» или государственного МФЦ не в структуре органа исполнительной власти);
2) форма смешанного — публично-гражданского договора на выполнение информационных работ, предусмотренных статусом органа исполнительной власти, исполнителем, не входящим по своему правовому статусу в систему органов государственной власти или местного самоуправления. (Форма такого договора должна быть разработана и учитывать, во-первых, условия работы с публично-значимой информацией; во-вторых, формы ответственности не только исполнителя, но и самого заказчика; в-третьих, устанавливать гарантии безопасности.)

С учетом п.п. 2-4 данной статьи осуществляется регулирование отношений в процессе формирования межгосударственных информационных систем в национальных структурах управления, а также в процессе формирования и использования интегрированных регионально распределенных информационных систем в информационном пространстве СНГ.

ГЛАВА 4. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ОТВЕТСТВЕННОСТИ ЗА ПРАВОНАРУШЕНИЯ В ПРОЦЕССАХ ИНФОРМАТИЗАЦИИ

Статья 18. Государственная политика в области обеспечения информационной безопасности

1. Государственная политика государств – участников СНГ реализуется в Стратегиях, Концепциях развития информационного общества при обеспечении информационной безопасности национального потенциала ИКТ и конкретных форм международного сотрудничества, взаимодействии при освоении и использовании информационного пространства; поддержании состояние безопасности общественных отношений в области создания и использования ИКТ и информационных ресурсов; при защите интересов личности, общества и государства и максимальном учете воздействия на их развитие факторов проявления внутренних и внешних угроз.

2. Обеспечение информационной безопасности рассматривается как деятельность государственных органов и организаций по поддержанию состояния безопасности, стабильного безопасного информационного обеспечения функционирования и развития всех социальных и государственных институтов и механизмов при использовании технических, программных, технологических, организационных и правовых средств информатизации в едином информационном пространстве и сферах международного сотрудничества государств.

3. Организационно-правовое регулирование обеспечения информационной безопасности рассматривается как важнейший институт информационного права и законодательства, в первую очередь, путём принятия модельных законов МПА СНГ, гармонизации национальных законов государств – участников СНГ, ОДКБ, ЕврАзЭС и других форм регионального международного информационного взаимодействия.

Статья 19. Направления, цели и задачи обеспечения информационной безопасности

1.Направления обеспечения информационной безопасности охватывают все программные решения в области развития информационного общества и все направления национальной безопасности каждого государства, реализуются через перспективные программы и планы развития информационного общества и интегрируют проблемы безопасности информационного пространства.

2. Обеспечение государственной политики, координацию деятельности системы обеспечения информационной безопасности и оценку состояния обеспечения безопасности по всем направлениям развития информационного общества, включая направления международного сотрудничества и взаимодействия в информационном пространстве межгосударственного взаимодействия, осуществляет уполномоченный государственный орган по обеспечению информационной безопасности.

3. Цели обеспечения информационной безопасности включают:

- создание условий безопасного поступательного развития средств и методов применения потенциала ИКТ, используемых в процессах информатизации страны;
- безопасное информационное обеспечение всех направлений национальной безопасности и поддержание суверенитета государства;
- безопасность формирования и использования систем международного информационного пространства при региональном сотрудничестве государств (в рамках СНГ, ОДКБ, ЕврАзЭС и других форм международного информационного сотрудничества);
- противодействие распространению вредной для общества и человека информации;

4. При обеспечении целей информационной безопасности государство решает следующие задачи:

- создание отрасли производства средств информатизации;
- обеспечение безопасности программного обеспечения всех форм информатизации и связи;

- обеспечение контроля качества национального и используемого импортного информационного продукта.

5. Государство формирует государственные и корпоративные структуры, ответственные за состояние информационно-коммуникационной инфраструктуры страны и создает инфраструктуру управления процессами информатизации с учетом их отраслевого, регионального и местного значения.

Статья 20. Методы организационно-правового регулирования обеспечения информационной безопасности

Методы организационно-правового регулирования обеспечения информационной безопасности включают:

а) методы и средства охраны и защиты информационных ресурсов с учетом их категорий по доступу и видам информации;

б) методы и средства охраны и защиты информационных систем с учетом их статуса и режима использования;

в) методы предотвращения несанкционированного доступа к информационным ресурсам, а также специальные меры (и порядок их реализации) по ликвидации возможных деструктивных последствий осуществления противоправных деяний, предусмотренных национальным законодательством;

г) специальные методы обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

д) защита прав и законных информационных интересов граждан, организаций и органов государственной власти в информационном пространстве государства с учетом соблюдения установленных государством гарантий доступа к информации и всех форм ее использования;

е) защита от распространения по каналам массовых коммуникаций (включая социальные сети Интернета, СМИ, рекламу) информации, способной причинить вред обществу и человеку.

Статья 21. Обеспечение информационной безопасности критически важных объектов информационно-коммуникационной инфраструктуры

Важнейшим объектом информационной безопасности при всех условиях является сознание и психофизиологическое здоровье человека и населения каждого государства.

В соответствии со стратегиями, программами, планами развития информационного общества и стратегией национальной безопасности государства соответствующие органы государственной власти устанавливают перечни критически важных объектов информационно-коммуникационной инфраструктуры, требующих адекватных методов обеспечения безопасности, технологических, материальных, финансовых и кадровых ресурсов, необходимых для обеспечения заданного состояния указанных объектов.

Критически важные объекты информационно-коммуникационной инфраструктуры находятся в ответственных зонах ведения органов государственного управления.

В целях обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктурыгосударство устанавливает порядок их формирования, функционирования и контроля за их состоянием и целевым использованием.

Статья 22. Обеспечение безопасности информационно-коммуникационной инфраструктуры и ИКТ

Обеспечение безопасности информационно-коммуникационной инфраструктуры осуществляется посредством осуществления комплекса мер:

- применение методов, средств и мер организационной, правовой и технической охраны и защиты;
- установление требований к надежности и безопасности аппаратных и программных средств (сертификация), проверки соответствия указанным требованиям;
- установление предписаний на обязательное использование отдельных средств и элементов информационно-коммуникационной инфраструктуры;
- лицензирование отдельных видов деятельности по созданию и поддержке элементов и объектов информационно-коммуникационной инфраструктуры;
- установление специальных требований к необходимому уровню квалификации лиц, осуществляющих отдельные виды деятельности на объектах информационно-коммуникационной инфраструктуры;
- выделение критически важных объектов информационно-коммуникационной инфраструктуры, установление и нормативное закрепление дополнительных требований к обеспечению их безопасности;
- установление ограничения оборота отдельных видов аппаратных и программных средств, используемых на объектах информационно-коммуникационной инфраструктуры.
- установление государственного контроля за качеством мер обеспечения безопасности информационно-коммуникационной инфраструктуры;
- создание, нормативное обеспечение и координация деятельности соответствующих национальных и межгосударственных органов и организаций в области информационного взаимодействия и

реализации политики в области информационной и коммуникативной безопасности.

Статья 23. Защита прав граждан, организаций и органов государственной власти на реализацию законных прав, исполнение обязанностей и функций этих категорий субъектов в информационном пространстве

1. Право на информацию — право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом гарантируется конституционным и информационным национальным законодательством и международными нормами. Ограничения на реализацию этих прав и порядок доступа и работы с информацией ограниченного использования устанавливается законом.

2. К организационно-правовым мерам ограничения доступа к информационно-коммуникационным системам и последующей передачи информации из них относятся установление специального режима допуска на объекты (территорию и в помещения), где может реализовываться доступ к информации, разграничение уровней доступа к информационным ресурсам по кругу лиц и характеру информации.

3. К организационно-техническим мерам ограничения доступа к информационно-коммуникационным системам и возможности последующей передачи информации из них относятся меры физической, аппаратной и программной защиты информационно-коммуникационным систем, использование криптографических средств защиты информации, а также систем контроля доступа и протоколирования фактов доступа к информационно-коммуникационной системе.

4. Использование технических мер ограничения доступа к информационно-коммуникационным системам не должно причинять вред или создавать угрозу причинения вреда здоровью и имуществу граждан.

Статья 24. Обеспечение безопасности информационной среды: открытой и общедоступной информации, информации ограниченного доступа

1. Официальная и иная открытая информация, исходящая от идентифицируемых субъектов, требует условий распространения и использования, которые исключают опасность нарушения её доступности и целостности, способных повлечь угрозу нанесения вреда пользователям этой информацией.

2. Правила классификации, определение видов и категорий информационных ресурсов, используемых в процессе функционирования информационных систем национального и межгосударственного значения, правила обеспечения безопасности их использования должны предусматривать:

а) закрепление прав на информационные ресурсы и определение правового статуса субъектов относительно форм работы с информационными ресурсам;
б) защиту информационных ресурсов в соответствии со статьями 8 и 9 настоящего модельного закона инормами национального законодательства государств-участников СНГ по вопросам определения правового режима, категорий и видов информационных ресурсов, правил работы со сведениями и данными;
в) соблюдение установленного порядка доступа и работы с открытой и общедоступной информацией;
г) определение категорий информации ограниченного доступа, соблюдение законодательства о защите государственной тайны, служебной тайны, коммерческой тайны и других категорий информации ограниченного доступа;
д) установление правил работы с персональными данными в органах государственной власти, управления и в организациях независимо от их формы собственности и правового статуса;
е) ведение учета форм противоправных деяний в отношении информации и прав субъектов на информацию; анализ эффективности применения мер ответственности к правонарушителям установленного порядка и правил работы с информацией.

Статья 25. Защита от распространения вредной и использования деструктивной информации

1.Официальная и иная открытая информация, исходящая от идентифицируемых субъектов в информационном пространстве, требует условий распространения и использования, исключающих опасность ее искажения и нанесения вреда субъектам — пользователямтакой информации;

2. Запрещается несанкционированное обладателем распространение информации, которая может нарушатьего законные права и интересы.Требует совершенствования законодательство об инсайдерской информации и правовой режим служебной информации ограниченного доступа.

3. Запрещается распространение информации, оказывающей деструктивное воздействие на сознание, подрывающей национальную безопасность;

3.1 Информацией, распространение которой нарушает законные права и интересы граждан и организаций, является заведомо ложная, позорящая, унижающая честь и достоинство личности информация; сведения, дискредитирующие деловую репутацию хозяйствующего субъекта; ложные сведения о товарах и услугах; заведомо ложное сообщение, в том силе об опасности; информация, содержащая угрозы причинения вреда правам и интересам лица, в том числе, угрозу убийства или причинения другого вреда здоровью, уничтожения имущества; иная информация при отсутствии возможности отказаться от её получения.

3.2 К информации, оказывающей деструктивное воздействие на сознание человека и подрывающей нацио-

нальную безопасность, следует относить информацию экстремистского, порнографического характера; информацию, пропагандирующую культ насилия и жестокости, содержащую призывы к насильственному свержению конституционного строя, организации или проведению массовых беспорядков; информацию; пропагандирующую войны, социальную, национальную, религиозную и расовую вражду или рознь; информацию включающую угрозу совершения акта терроризма; сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ, их прекурсоров и аналогов, а также взрывчатых веществ и огнестрельного оружия.

4. Порядок функционирования источников информирования населения, определяемый национальным законодательством и органами саморегулирования средств массовой информации и коммуникаций, должен предусматривать соблюдение требования аутентификации публикуемой и распространяемой информации.

Статья 26. Виды и формы юридической ответственности за правонарушения в области информационных отношений

Юридическая ответственность в области информационных отношений реализуется в соответствии с нормами уголовного, гражданско-правового, административного национального законодательства с соблюдением норм соответствующего процессуального законодательства.

Для рассмотрения конфликтов и нарушения договорных отношений в области информационного взаимодействия и информационной безопасности государства – участники СНГ могут создавать третейский или арбитражный суды. Прецеденты, связанные с нарушением международного права в области защиты прав человека, могут рассматриваться соответствующими международными судами.

Защита прав создателей объектов интеллектуальной собственности при их использовании в информационно-коммуникационном пространстве сети Интернет и взаимодействии субъектов государств – участников СНГ по этим вопросам осуществляется в соответствии с модельными и национальными законами об интеллектуальной собственности.

Статья 27. О введении в действие настоящего модельного закона

1. Настоящий Закон вступает в силу со дня его официального опубликования.

2. В целях гармонизации национальных законодательных актов государства – участники СНГ осуществляют их приведение в соответствие с настоящим законом.

Правительствам государств – участников СНГ рекомендуется подготовить и внести в установленном порядке в национальные парламенты соответствующие предложения.

Разработчики проекта:

д.ю.н. Бачило И.Л. – Институт государства и права РАН;

д.ю.н. Макаров О.С. – Институт национальной безопасности Республики Беларусь

к.ю.н. Перевалов Д.В. – Институт погранслужбы Республики Беларусь

к.т.н. Вус М.А. – Санкт-Петербургский институт информатики и автоматизации РАН

сентябрь, 2014 г.

АННОТАЦИИ

В.В. Бондуровский, И.Л.Бачило, М.А. Вус,
М.М. Кучерявый, О.С. Макаров

Парламентское измерение информационной безопасности в рамках СНГ и ОДКБ на современном этапе

Ключевые слова: информационная политика, международная информационная безопасность, СНГ, ОДКБ, развитие и гармонизация законодательства.

Освещаются вопросы международного сотрудничества по формированию системы информационной безопасности, развитию и гармонизации национального законодательства в этой области в рамках СНГ и ОДКБ.

И.Л. Бачило, М.А. Вус, О.С. Макаров

Об изменениях Модельного закона СНГ «Об информатизации, информации и защите информации » (2005 г.) в его новой редакции с изменённым названием «Об информации, информатизации и обеспечении информационной безопасности»

Ключевые слова: модельный закон МПА СНГ, информация, информатизация, информационная безопасность

Освещается подход к разработке изменений в базовый закон МПА СНГ об информатизации, сравнительный анализ структур и характеристика отличий существующего и проекта нового Модельного закона.

Д.В. Перевалов

Правовые и организационные аспекты формирования системы безопасности критически важных объектов информационно-коммуникационной инфраструктуры

Ключевые слова: критически важные объекты, информационно-коммуникационная инфраструктура, безопасное функционирование, обеспечение безопасности.

В статье рассматривается проблема создания действенной системы безопасности критически важных объектов информационно-коммуникационной инфраструктуры. В качестве одного из решений данной проблемы видится формирование и обеспечение безопасного функционирования системы критически важных объектов информационно-коммуникационной инфраструктуры, а также поддержание необходимого уровня функционирования системы обеспечения безопасности таких объектов. Реализация такого подхода создаст необходимые условия для должной и надёжной деятельности всех общественных и государственных институтов.

А.А. Лепёхин

О некоторых аспектах разработки и реализации административных регламентов в сфере информационной безопасности

Ключевые слова: административный регламент, критически важные объекты, информационно-коммуникационная инфраструктура безопасное функционирование, обеспечение безопасности.

Рассматриваются основные подходы к разработке и реализации административных регламентов в сфере информационной безопасности на примере организации защиты критически важных объектов информатизации. Определены цели, задачи и основные направления в данной сфере и предполагаемый практический результат деятельности государственных органов сфере регулирования информационно-комуникационной среды.

М.М. Кучерявый, И.И. Лифшиц

Подходы к оценке уязвимостей и угроз информационной безопасности для объектов критическкой инфраструктуры Российской Федерации на примере национальной платежной системы

Ключевые слова: национальная платежная система (НПС); информационная безопасность (ИБ), система менеджмента информационной безопасности (СМИБ); анализ рисков; уязвимости, угрозы; аудит; показатели (метрики) ИБ; оценка результативности.

Актуальность рассмотрения вопросов анализа уязвимостей и угроз критичных систем Российской Федерации в полной мере применима к национальной платежной системы (НПС), особенно с учетом известных инцидентов по блокированию работы систем Visa и MasterCard в марте 2014 г. При анализе уязвимостей и угроз, как правило, применятся достаточно хорошо известная методическая база – международные стандарты ISO серии 27000 и, в ряде случаев, например, для финансовых информационных систем – стандарты Банка России СТО БР ИББС. Однако применение для анализа НПС только национальных стандартов Банка России объективно ограничено – т.к. комплекс БР ИББС рассматривает только отраслевые риски нарушения информационной безопасности (ИБ), а субъектный состав НПС значительно шире. В данном исследовании была рассмотрена современная нормативная база комплекса БР ИББС (версии 2014 г.) и показано практическое применение современных стандартов ISO серии 27000, существенно расширяющие возможности оценки уязвимостей и угроз ИБ по отношению к объектам критичной инфраструктуры, а также даны рекомендации по смягчению (парированию) аналогичных угроз НПС в будущем.

М.В. Буйневич, О.А. Тиамийу

Программная архитектура системы управления доверенной маршрутизацией в глобальных телекоммуникационных сетях

Ключевые слова: глобальные телекоммуникационные сети, доверенная маршрутизация, система управления, программная архитектура.

Введено понятие механизма доверенной маршрутизации в глобальных телекоммуникационных сетях и рассмотрено его алгоритмическое содержание. Показана необходимость организации системы управления доверенной маршрутизацией и предложена ее двухуровневая распределенная программная архитектура, базирующаяся на агентном подходе.

К.Е. Израилов

Методика оценки эффективности средств алгоритмизации, используемых для поиска уязвимостей

Ключевые слова: методика оценки, эффективность, алгоритмизация, машинный код, поиск уязвимостей, метод анализа иерархий.

Рассмотрена проблема оценки эффективности средств алгоритмизации и предложено ее решение методом анализа иерархий. Разработана методика оценки, специализированная под задачу поиска уязвимостей в машинном коде, для чего классифицированы альтернативные средства алгоритмизации и сформирована система из 10 критериев. Приведен пример ее практической реализации для разработанной автором утилиты и ближайшего аналога.

М.В. Харинов, В.П. Заболотский

Критическая технология квазиоптимального машинного зрения

Ключевые слова: цифровое изображение, оптимальная аппроксимация, иерархия приближений, метод Оцу, метод Уорда, модель Мамфорда-Шаха, среднеквадратичное отклонение.

В статье рассматривается проблема автоматического выделения объектов на цифровых изображениях и обсуждается вариант ее решения на основе квазиоптимальных приближений, которые аппроксимируют изображение с близкой к минимальной суммарной квадратичной ошибкой. Проблема сегментации формулируется как проблема разделения изображения на вложенные изображения объектов. Задача оптимизации ставится и решается как задача аппроксимации оптимальных приближений изображения иерархическими приближениями. Дается аналитическое обоснование алгоритмов и проводится их сравнительный анализ.

Д.С. Черешкин

Проблемы обеспечения информационной безопасности в новых условиях

Ключевые слова: информационная безопасность, критическая информационная инфраструктура, кибербезопасность, кибер-атаки, директивные документы, мониторинг, риски нарушения.

Рассматриваются изменения подходов к обеспечению информационной безопасности критической информационной инфраструктуры страны, связанные с появлением новых видов угроз – кибернетических. Эти угрозы, ориентированные на разрушение и/или нарушение нормальных режимов функционирования информационных систем и коммуникационных сетей, ставят новые задачи и определяют новые направления в обеспечении информационной безопасности. Анализируются эти направления и способы их реализации в США и Российской Федерации. Основой анализа являются принятые в странах директивные документы и конкретные решения. Определяются пути возможного решения поставленных задач.

О.С. Макаров, М.А. Вус, Д.В. Перевалов

К вопросу разработки правового обеспечения информационной безопасности

Ключевые слова: информация, информационная безопасность, национальная безопасность, информационное право.

Рассматривается авторский подход к формированию, структуризации и систематизации правовых норм обеспечения информационной безопасности.

SUMMARY

V.V. Bondurovsky, I.L. Bachilo, M.A. Vus, M.M. Kucheryavy, O.S. Makarov

The parliamentary dimension of information security within the CIS and the CSTO at the present stage

Keywords: information policy, international security, CIS, CSTO, development and harmonization of legislation.

Covers the issues of international cooperation in the formation of an information security system, the CIS and CSTO.

I.L. Bachilo, M.A. Vus, O.S. Makarov

About changes to the Model law of the CIS "On Informatization, and information protection (2005) in his new edition with a modified title, «On information, information and ensuring information security»

Keywords: the model law of the IPA CIS, information, Informatization, information security

Illuminated approach to the development of amendments to the basic law of the IPA CIS on Informatization, comparative analysis of structures and characteristic differences between the existing and new draft Model law.

D.V. Perevalov

Legal and organizational aspects of formation of safety system jf critical objects of information and communication infrastructure

Keywords: critical objects, information and communication infrastructure, safe functioning, safety.

The article examines the problem of formation of safe functioning system of critical objects of information and communication infrastructure. One way to solve the problem is to form and to provide safe functioning of the system of critical objects of information and communication infrastructure as well as to maintain the necessary level of functioning the system of safety of such objects. The implementing of this approach will create the conditions necessary for proper and reliable activities of all public and state institutions.

A.A. Lepekhin

Several aspects of the development and implementation of administrative regulations in information security

Keywords: administrative rules, critical objects, information and communication infrastructure, safe functioning, safety.

Discusses approaches to the development and implementation of administrative regulations in the field of information security at the example of the organization protect critical information technology. Defined goals, objectives and guidelines in this area and the estimated practical result of public authorities the regulation of information and communication environment.

M.M. Kucheryavyi, I.I. Lifshitz

Approach to the assessment of vulnerabilities and security threats to critical infrastructure facilities of the Russian Federation on the example of the national payment system

Keywords: national payment system (NPS); Information security of the banking system (IBBS); information security (IS); Information Security Management System (ISMS); risk analysis; vulnerabilities; threats; audit; measure; performance evaluation.

The urgency of addressing issues of vulnerability assessment and threats to critical systems of the Russian Federation is fully applicable to the national payment system (NPS), especially in view of the known incidents of blocking the work of Visa and MasterCard in March 2014. In the analysis of vulnerabilities and threats are usually applied sufficiently well-known methodological framework - international ISO 27000 standards and, in some cases, for example, financial information systems - BR IBBS complex (development Bank of Russia). This issue shows that the requirements only BR IBBS complex not cover the full requirements of the present level of information security for the objects of critical financial infrastructure NPC. Several reasons for this situation: - subject composition of the NPC is much wider field of application of the BR IBBS complex not fully supports PDCA cycle applied to ISMS functionally limited risk assessment breach of information security. Insufficient attention to the problem of information security with full coverage of life cycle stages can lead to the emergence of further incidents (like Visa and MasterCard), as the most important questions of continuity and maintain availability of the processing core were outside any control of users, organizations and authority in the Russian Federation. Accordingly, for the purpose of fair, accurate, reproducible and objective analysis of threats and vulnerabilities, the NPC must also apply the requirements of the ISO 27000 series of numerical methods for assessing the effectiveness of the ISMS, based on the requirements of the ISO 27000 series, will ensure a reliable and operational control over the current level of information security in with respect to the NPC (as set of assets), as well as to propose measures to avoid a recurrence in the future or substantial "easing" the negative consequences in the event that external risk factors will be shown again.

M.V. Buinevich, O.A. Tiamiyu

Software architecture of trusted routing control system in the global telecommunications networks

Keywords: global telecommunication networks, trusted routing, control system, software architecture.

In this article the concept of trusted routing mechanism in global telecommunications networks is introduced and its algorithmic content is considered. The necessity of organizing trusted routing control system is shown and its two-level distributed software architecture that is of agent-based approach is proposed.

K.E. Israilov

Methods of assessing the effectiveness of medium of algorithmization used to find vulnerabilities

Keywords: assessment methodology, efficiency, algorithmization, machine code, vulnerabilities search, analytic hierarchy process.

The problem of evaluating the effectiveness of tool of algorithmization is considered and its solution is proposed by analytic hierarchy process. Specialized estimation methodology for the task of finding vulnerabilities in machine code, for which are classified alternative means of algorithmization and established a system of 10 criteria, is developed. An example of its implementation for utilities developed by author and the closest analogue are given.

M.V. Kharinov, V.P. Zabolotski

Crucial technology of quasi-optimal machine vision

Keywords: digital image, optimal approximating, hierarchy of approximations, Otsu method, Ward's method, Mumford-Shah segmentation model, problem, standard deviation.

The paper focuses on the problem of automatic object detection in digital images and discusses the option of its decisions on the basis of quasi-optimal approximations that approach the image with close to the minimum value of total square error. Segmentation problem is formulated as the problem of separating an image into sub-images referred to as objects. Optimization problem is treated and solved as the problem of majorizing of the optimal approximations of the image by the hierarchical approximations. Analytical substantiation of algorithms is provided and their comparative analysis is proposed.

D.S. Chereshkin

The problem of information security in the new conditions

Keywords: information security, critical information infrastructure, cyber security, cyber attacks, policy documents, monitoring, risks.

Discusses changes in approaches to information security critical information infrastructure of the country associated with the emergence of new types of cyber-threats. These threats aimed at the destruction and/or violation of the normal modes of functioning of information systems and communication networks, present new challenges and new directions to ensure information security. These areas are analysed and the ways of their realization in the United States and the Russian Federation. Basis of analysis are taken in the policy documents and concrete solutions. Identifies ways of possible solutions.

O.S. Makarov, M.A Vus., D.V. Perevalov

To the question of development of the legal information security

Keywords: information, information security, national security, and information law.

Discusses the author's approach to the formation, structuring and systematization of legal standards of information security.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Бачило Иллария Лаврентьевна – доктор юридических наук, профессор, заведующая сектором информационного права Института государства и права РАН.

Bachilo I.L. – Doctor of Juridical Sciences, professor, Head of the Information Law Department at the Institute for State and Law of RAS.

e-mail: illariya@ rambler.ru

Бондуровский Владимир Владимирович – кандидат юридических наук, доцент, начальник информационно-аналитического управления ОДКБ — заместитель Ответственного секретаря Парламентской Ассамблеи ОДКБ.

Bondyrovsky V.V - candidate of Juridical Sciences, Professor, head of information-analytical Departament of the CSTO Deputy Sesretary-General of the CSTO parliamentary Assembly.

e-mail: bondvvodkb@mail.ru

Буйневич Михаил Викторович – доктор технических наук, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени проф. М. А. Бонч-Бруевича.

Buinevich M.V. – Doctor of Technical Sciences, professor of «Secure Communications System» Department of the St. Petersburg State University of Telecommunications.

e-mail: bmv1958@yandex.ru

Вус Михаил Александрович – кандидат технических наук, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН, дважды лауреат Премии Правительства России в области образования.

Vys M.A., Candidate of Technical Sciences, senior researcher of the Applied Informatics Laboratory of St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS).

e-mail: mixail-vys@yandex.ru

Заболотский Вадим Петрович – доктор технических наук, профессор, главный научный сотрудник лаборатории прикладной информатики Санкт-Петербургского института информатики и автоматизации РАН (СПИИРАН).

Zabolotsky V.P., Doctor of Technical Sciences, professor, chief researcher, Laboratory of Applied Informatics, State Organization of St. Petersburg Institute for Informatics and Automation of RAS (SPIIRAS).

e-mail: 240lai@iias.spb.su

Израилов Константин Евгеньевич – аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени проф. М. А. Бонч-Бруевича.

Izrailov K. E. – post-graduate student of «Secure Communications System» Department of the St. Petersburg State University of Telecommunications.

e-mail: конstantin.izrailov@mail.ru

Кучерявый Михаил Михайлович – кандидат политических наук, доцент, Федеральная служба технического и экспортного контроля.

Kucheryavyi M.M. – Candidate of Political Sciences, Associate Professor, Russian Federal Service for Technical and Export Control (FSTEC).

e-mail: szfo@fstec.ru

Лепёхин Александр Николаевич – кандидат юридических наук, доцент, начальник кафедры правовой информатики Академии МВД Республики Беларусь.

Lepiokhin A.N. – Candidate of Juridical Sciences, Professor, head of Department of legal informatics of the Ministry of internal Affairs of the Republic of Belarus.

e-mail: prav_informatika@mail.ru

Лившиц Илья Иосифович – кандидат технических наук, ООО «Газинформсервис».

Livshitz I.I. - Candidate of Technical Sciences, LLC «Gazinformservis»

e-mail: livshitz_il@hoybox.ru

Макаров Олег Сергеевич – доктор юридических наук, доцент, заместитель начальника Института национальной безопасности Республики Беларусь.

Makarov O.S. - Doctor of Juridical Sciences, Professor, Deputy head of the Institute of national bezopasnosti of the Republic of Belarus

e-mail: makarovos@list.ru

Перевалов Дмитрий Васильевич – кандидат юридических наук, доцент Института погранслужбы Республики Беларусь.

Perevalov D.V. – Candidate of Juridical Sciences, Professor of the Institute of border service of the Republic of Belarus.

e-mail: perevalov@tut.by

Тиамийу Осуолале Абдулрахамон – аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени проф. М. А. Бонч-Бруевича.

Tiamiyu A. Osuolale, post-graduate student of «Secure Communications System» Department of the St. Petersburg State University of Telecommunications

e-mail: ozutiams@yahoo.com

Харинов Михаил Вячеславович — кандидат технических наук, доцент; старший научный сотрудник лаборато-

рии прикладной информатики Учреждения Российской академии наук Санкт-Петербургского института информатики и автоматизации РАН (СПИИРАН).

Kharinov M.V. — Candidate of Technical Sciences, associated professor; senior researcher, Laboratory of Applied Informatics, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS).

e-mail: khar@iias.spb.su

Черешкин Дмитрий Семёнович – доктор технических наук, профессор, заведующий лабораторией Института системного анализа РАН.

Chereshkin D.S. – Doctor of Technical Sciences, Professor, head of laboratories Institute of system analysis Russian Academy of Sciences

e-mail: cheresh@isa.ru

КНИЖНАЯ ПОЛКА

СЛОВАРЬ – СПРАВОЧНИК ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ПАРЛАМЕНТСКОЙ АССАМБЛЕИ ОДКБ / Под общ. ред. М.А. Вуса и М.М. Кучерявого. – СПб.: СПИИРАН. Изд-во «Анатолия». «Полиграф-Экспресс», 2014. – 96 с. **ISBN 978-5-7452-0050-2**

Государства – члены ОДКБ в качестве одного из основных направлений создания системы коллективной безопасности рассматривают сближение основных положений законодательных актов в области обороны и безопасности. Понятийный аппарат, складывающийся в разных отраслях законодательства, обусловлен характером регулируемых отношений. Согласованная политика требует определенности и однозначности понятийного аппарата.

Информационная безопасность становится сегодня важнейшим компонентом национальной и международной безопасности. Само понятие информационная безопасность превратилось из узкотехнического в широкоупотребительное, а юридические определения многочисленных специальных терминов зачастую играют решающую роль при толковании норм законов в правоприменительной практике.

За два десятилетия существования Независимых Государств в них разработано и принято большое число нормативно-правовых актов, однако для большинства этих актов сегодня характерны терминологическое многообразие и слабая определенность используемого понятийного аппарата. В этой связи необходима унификация в нормативно-правовой базе государств – членов ОДКБ, прежде всего, базовых терминов и понятий, используемых в процессе нормативного правового регулирования и сотрудничества, их единообразная трактовка.

Предлагаемый справочник содержит 163 группы терминов и различных трактовок понятий из международных и национальных правовых актов, относящиеся к сфере информационной безопасности. Словарный материал представлен в табличной форме. Он включает набор категорий, которые можно рассматривать как базовые для сферы информационной безопасности, а также относящиеся к сфере информационной безопасности лексические единицы, получившие юридическое толкование в международных и национальных правовых документах государств – членов ОДКБ, с указанием их первоисточника. Представленная выборка понятийного аппарата не претендует на полноту, но может послужить ориентиром в правотворческой деятельности.

Издание адресовано 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. Материал может быть использован в правотворческой и правоприменительной деятельности, в научных исследованиях и в учебном процессе.

М.А. Вус
М.М. Кучерявый

Перечень требований и условий предоставляемых для публикаций

Рукописи, предоставляемые в редакцию должны соответствовать следующим требованиям:

- тема статьи должна быть актуальной, иметь научное или практическое значение и публиковаться авторами впервые;
- рукопись должна быть оформлена в соответствии с "Правилами оформления текстов для публикации";
- автором указываются: фамилия, имя, отчество (полностью), должность, ученая степень, ученое звание, место работы, контактный телефон и адрес электронной почты - на русском и английском языках;
- к статье должна быть аннотация не более 4-х предложений на русском и английском языках;
- в начале статьи должны быть указаны ключевые слова на русском и английском языках;
- статья представляется в одном экземпляре на бумажном и электронном носителях (кроме дискет);
- общий объем статьи не должен превышать 7 страниц, включая таблицы, иллюстрации и список литературы (как правило, не более 7 наименований);
- статья должна быть подписана автором, который несет ответственность за содержание публикуемого материала.

Условия опубликования статьи

- статьи, не соответствующие установленным требованиям представления и оформления, не рассматриваются и не публикуются;
- в одном номере журнала публикуется, как правило, только одна статья автора, в том числе с соавторами;
- решение о публикации рукописи принимается Редакционным советом на основании результата рецензирования и экспертной оценке;
- в случае приема рукописи к публикации автор должен оперативно давать ответы на вопросы редакции, связанные с замечаниями по статье;
- в случае отказа в публикации Редакционный совет должен предоставить автору рецензию с обоснование отказа публикации.

Правила оформления статей

1. Статьи необходимо подавать в электронном виде (*.doc или *.rtf) с распечаткой (или файлом в формате *.pdf) - во избежание неточностей прочтения формул.
2. Картинки, графики, фотографии и другие виды иллюстраций, по возможности, представляйте не только включенными в текст, но и отдельными файлами в исходном формате (не интегрированными в документ Word).
3. Сокращения и аббревиатуры необходимо раскрывать (в скобках или в сноске).
4. Для удобства каталогизации статьи должны быть снабжены краткими аннотациями (3-4 предложения).
5. Давая в тексте статьи ссылки на формулы, выражения или ограничения, пожалуйста, убедитесь в том, что соответствующие объекты в статье есть и пронумерованы.
6. Ссылки на литературу следует давать в тексте в квадратных скобках, в случае цитирования - с указанием страниц.
7. При оформлении списка литературы желательно обращать внимание на наличие выходных данных работ и избегать повторных указаний одной и той же работы под разными номерами.
8. Ссылки на законы, нормативные акты, конвенции и пр. желательно указывать по установленной форме: Закон РФ "___" от х месяца хххх г. № ___. Ст. ___.
9. Иноязычные слова, термины и фамилии, написание которых допускает варианты, просьба писать в пределах одной статьи одинаково.

XIV САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ

«РЕГИОНАЛЬНАЯ ИНФОРМАТИКА (РИ-2014)»

Санкт-Петербург, 29-31 октября 2014 г.

Информационное письмо
Исх. № К-1/2014

Уважаемые господа!

Приглашаем Вас принять участие в работе XIV Санкт-Петербургской международной конференции **«Региональная информатика (РИ-2014)»,** которая традиционно будет проходить в Санкт-Петербурге под эгидой ЮНЕСКО при поддержке Правительства Санкт-Петербурга **с «29» по «31» октября 2014 года.**

УЧРЕДИТЕЛИ КОНФЕРЕНЦИИ

- Правительство Санкт-Петербурга
- Законодательное Собрание Санкт-Петербурга
- Правительство Ленинградской области
- Министерство образования и науки РФ
- Министерство связи и массовых коммуникаций РФ
- Российская академия образования
- Отделение нанотехнологий и информационных технологий РАН
- Санкт-Петербургский Научный центр РАН и др.

ПРОГРАММА КОНФЕРЕНЦИИ ВКЛЮЧАЕТ СЛЕДУЮЩИЕ ТЕМАТИЧЕСКИЕ НАПРАВЛЕНИЯ

- Региональная политика информатизации. Электронное правительство
- Теоретические проблемы информатики и информатизации
- Телекоммуникационные сети и технологии
- Информационная безопасность
- Правовые проблемы информатизации
- Информационно-аналитическое обеспечение органов государственной власти
- Информационное обеспечение финансово-кредитной сферы и бизнеса
- Средства массовой информации
- Информационные технологии в критических инфраструктурах
- Информационные технологии в производстве
- Информационные технологии на транспорте
- Информационные технологии в научных исследованиях
- Информационные технологии в образовании
- Информационные технологии в здравоохранении
- Информационные технологии в сервисе
- Информационные технологии в экологии
- Информационные технологии в гидрометеорологии
- Информационные технологии в дизайне
- Информационные технологии в издательской деятельности и полиграфии
- Геоинформационные системы
- Распределенные информационно-вычислительные системы, грид-технологии
- Научная школа молодых ученых «Информационные технологии математического моделирования»
- Молодежная научная школа «Региональная информатика и проблемы устойчивого развития»
- Молодежная научная школа «Безопасные информационные технологии»
- Научная школа для старшеклассников «Информатика будущего»

УСЛОВИЯ УЧАСТИЯ В КОНФЕРЕНЦИИ

Для того, чтобы зарегистрироваться в качестве участника Конференции необходимо заполнить анкету и отправить ее по электронной почте: **ri@spoisu.ru** либо заполнить анкету на сайте: **http://spoisu.ru/conf/ri2014,** указав сведения о перечислении организационного целевого взноса предприятия: номер и дату платежного поручения.

Авторам докладов необходимо также приложить материалы (тезисы) доклада, подготовленные в соответствии с требованиями к оформлению.

Анкета участника, требования и примеры оформления документов размещены на сайте: **http://spoisu.ru/conf/ri2014**

Заявки на участие в Конференции принимаются до **24 октября 2014 г.** включительно.

Тезисы докладов, поступившие в Оргкомитет не позднее **27 сентября 2014 г.** будут опубликованы в сборнике материалов до начала Конференции.

По окончании Конференции будет издан сборник трудов, куда войдут материалы докладов, рекомендованных к опубликованию Программным комитетом.

ФИНАНСИРОВАНИЕ ПОДГОТОВКИ И ПРОВЕДЕНИЯ КОНФЕРЕНЦИИ

Подготовка и проведение Конференции «РИ-2014» осуществляется при поддержке Правительства

Санкт-Петербурга с привлечением организационных целевых взносов (добровольных пожертвований) предприятий-соустроителей Конференции.

Минимальный размер организационного целевого взноса участника Конференции составляет 3000 рублей.

В соответствии со сметой указанные средства расходуются на подготовку и проведение Конференции, в т.ч аренду помещений, издание трудов Конференции, других информационных материалов. Проживание в гостинице, забронированной по предварительной заявке, и питание участники оплачивают самостоятельно.

В платежном поручении следует указать:

Получатель: СПОИСУ. Р/с 40703810627000003078 в Дополнительном офисе «Приморский» ОАО «Банк «Санкт-Петербург» к/с 30101810900000000790

БИК 044030790 ИНН 7813148260 КПП 781301001

Назначение платежа: Организационный целевой взнос (добровольное пожертвование) на подготовку и проведение Конференции «РИ-2014» согласно информационного письма № К-1/2014, (представитель - ФИО). НДС не облагается.

МЕСТО ПРОВЕДЕНИЯ КОНФЕРЕНЦИИ И КОНТАКТНЫЕ ТЕЛЕФОНЫ

Торжественное открытие Конференции «РИ-2014» состоится **29 октября 2014 года** в 10:00 часов в Белом зале Дома ученых им. М. Горького РАН по адресу: Санкт-Петербург, Дворцовая наб., д. 26.

Начало регистрации гостей и участников с 9:00 часов.

Контакты для оперативной связи:

моб. тел.: (931) 211-36-90. http://spoisu.ru/conf/ri2014

Почтовый адрес Оргкомитета Конференции:

199178, Санкт-Петербург, В.О., 14-я линия, д.39, Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН).

СПИИРАН: тел.: (812) 328-19-19,
(812) 328-33-11, факс: (812) 328-44-50,
e-mail: lai@iias.spb.su, spiiran@iias.spb.su
СПОИСУ: тел./факс: (812) 317-83-16,
e-mail: spoisu@mail.ru