Санкт-Петербургский институт информатики и автоматизации РАН
Институт государства и права РАН
ГУО «Институт национальной безопасности Республики Беларусь»
ГУО «Академия МВД Республики Беларусь»
УО «Центр специальной подготовки (Республика Беларусь)»

СТРАТЕГИЧЕСКИЙ ВЕКТОР ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Санкт-Петербург - Минск - Москва

Санкт-Петербургский институт информатики и автоматизации РАН
Институт государства и права РАН
ГУО «Институт национальной безопасности Республики Беларусь»
ГУО «Академия МВД Республики Беларусь»
УО «Центр специальной подготовки (Республика Беларусь)»

25-летию МПА СНГ
и
10-летию ПА ОДКБ
посвящается

СТРАТЕГИЧЕСКИЙ ВЕКТОР ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Санкт-Петербург
2016

ББК 67.412.1

Авторы:

Р.М. Юсупов – предисловие;
И.Л. Бачило – гл. 4, 8; В.В. Бондуровский – гл. 1-3;
М.А. Вус, О.С. Макаров – гл. 1-3, 7, 8;
А.Н. Лепёхин, Д.В. Перевалов – гл. 5, 6.

Рецензент — доктор политических наук *М.М. Кучерявый*.

С32 СТРАТЕГИЧЕСКИЙ ВЕКТОР ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Сборник / [сост. М.А. Вус, О.С. Макаров] / Предисловие: чл.-кор. РАН Р.М. Юсупов – СПб.: СПИИРАН, 2016. – 122 с. ил.

ISBN 978-5-7452-0036-6

В материалах сборника раскрываются основные положения правового регулирования обеспечения международной информационной безопасности на пространстве СНГ и ОДКБ. Издание подготовлено по материалам работ инициативного коллектива российских и белорусских ученых. Для парламентарией и учёных, специалистов в области международных отношений и информационной безопасности, аспирантов и студентов.

ISBN 978-5-7452-0036-6

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ....5

ЧАСТЬ 1. ПРОБЛЕМА ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ....8

ГЛАВА 1. СТАНОВЛЕНИЕ И РАЗВИТИЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРАХ ДЕЯТЕЛЬНОСТИ СНГ и ОДКБ....8

1.1. Правовые формы сотрудничества государств – участников СНГ и государств – членов ОДКБ по обеспечению международной информационной безопасности....8

1.2. Развитие правового регулирования обеспечения международной информационной безопасности государств – участников СНГ....10

1.3. Развитие правового регулирования обеспечения международной информационной безопасности в сфере отношений государств – членов ОДКБ....13

1.4. Проблемы правового регулирования обеспечения международной информационной безопасности....15

ГЛАВА 2. ПОНЯТИЙНО-КАТЕГОРИАЛЬНЫЙ АППАРАТ В СФЕРЕ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СНГ и ОДКБ....20

2.1. Вектор формирования понятийно-категориального аппарата в сфере обеспечения международной информационной безопасности....20

2.2. Феномен информационной безопасности....21

2.3. Понятие и сущность обеспечения информационной безопасности....27

2.4. Базовые правовые категории в сфере обеспечения международной информационной безопасности на пространстве СНГ и ОДКБ....32

ГЛАВА 3. КОМПЛЕКСНЫЙ ПОДХОД К ПРАВОВОМУ ОБЕСПЕЧЕНИЮ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ....35

3.1. Вектор правового регулирования обеспечения международной информационной безопасности на пространстве СНГ и ОДКБ в современный период....35

3.2. Обоснование системы обеспечения международной информационной безопасности....38

3.3. Формы правового обеспечения информационной безопасности....47

ЧАСТЬ II. ВЕХИ РАЗВИТИЯ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРОСТРАНСТВЕ СНГ и ОДКБ....55

ГЛАВА 4. МОДЕЛЬНОЕ РЕГУЛИРОВАНИЕ В ОБЛАСТИ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ....55

4.1. История развития модельного регулирования в области информации, информатизации и обеспечения информационной безопасности на пространстве СНГ....55

4.2. Структура и содержание Модельного закона СНГ «Об информации, информатизации и обеспечении информационной безопасности»....62

ГЛАВА 5. МОДЕЛЬНОЕ РЕГУЛИРОВАНИЕ НА ПРОСТРАНСТВЕ СНГ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАЦИОННО - КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ 66

5.1. Обоснование и структурно-сущностная характеристика модельного регулирования в области обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры....66

5.2. Понятие и содержание критически важных объектов информационно-коммуникационной инфраструктуры....69

5.3. Формирование системы критически важных объектов информационно-коммуникационной инфраструктуры....70

5.4. Обеспечение безопасности критически важных объектов информационно-коммуникационной инфраструктуры....74

5.5. Модельное регулирование административных процедур, осуществляемых уполномоченными органами в сфере обеспечения информационной безопасности 79

ГЛАВА 6. СОВЕРШЕНСТВОВАНИЕ И ГАРМОНИЗАЦИЯ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ЭКСПЛУАТАЦИИ ОТКРЫТЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ ДЛЯ ПРЕДУПРЕЖДЕНИЯ ИХ ИСПОЛЬЗОВАНИЯ В ТЕРРОРИСТИЧЕСКИХ И ИНЫХ ПРОТИВОПРАВНЫХ ЦЕЛЯХ....82

6.1. Необходимость совершенствования и гармонизации национального законодательства в сфере эксплуатации открытых телекоммуникационных сетей для предупреждения их использования в террористических и иных противоправных целях....82

6.2. Структура Рекомендаций по правовому регулированию эксплуатации ОТКС для предупреждения их использования в террористических и иных противоправных целях....83

6.3. Приоритетные направления и основные меры правового регулирования эксплуатации ОТКС для предупреждения их использования в террористических и иных противоправных целях 85

ГЛАВА 7. СОВЕРШЕНСТВОВАНИЕ И ГАРМОНИЗАЦИЯ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ЗАЩИТЫ ГОСУДАРСТВЕННОЙ ТАЙНЫ НА ПРОСТРАНСТВЕ ОДКБ....89

7.1 Основания для гармонизации правового регулирования защиты государственной тайны 89

7.2. Становление и развитие правового регулирования защиты государственной тайны 91

7.3. Основные направления совершенствования и гармонизации законодательства в сфере защиты государственной тайны на пространстве ОДКБ....93

ЧАСТЬ III. СТРАТЕГИЧЕСКИЙ ВЕКТОР ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРОСТРАНСТВЕ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ....96

ГЛАВА 8. О СТРАТЕГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ГОСУДАРСТВ – УЧАСТНИКОВ СНГ....96

8.1. Предпосылки для разработки Стратегии информационной безопасности....96

8.2. Концептуальный подход к разработке Стратегии информационной безопасности 99

8.3. О перспективах реализации Стратегии…… 102

ПРИЛОЖЕНИЕ 104

ПРЕДИСЛОВИЕ

Содружество Независимых Государств (СНГ) — признанная международным сообществом региональная межгосударственная организация. На протяжении четверти века своего существования СНГ ведёт поиск оптимальных форм сотрудничества и адаптации его институтов и механизмов к потребностям многостороннего взаимодействия. Большое внимание уделяется обеспечению безопасности и противодействию организованной преступности и терроризму в их различных формах и проявлениях. Важнейшее направление сотрудничества — противодействие новым вызовам и угрозам. Межгосударственное сотрудничество в этой сфере является наиболее востребованным.

Углублению взаимодействия в рамках Содружества способствуют формирование общего информационного пространства, расширение межгосударственного информационного обмена, создание и развитие совместных информационно-телекоммуникационных систем. Информационная сфера — весьма чувствительный фактор жизнедеятельности общества. Бурное развитие информационно-коммуникационных технологий (ИКТ) все больше становится причиной перемен в политической, экономической и социально-культурной сферах.

Важнейшим результатом формирования информационного общества на рубеже веков стало возникновение глобального информационного пространства, в котором развернулась острая борьба за достижение информационного превосходства. Защищённость информации и информационной среды является фактором, активно влияющим на состояние национальной безопасности государств. Вместе с тем становятся все более изощрёнными атаки на критически важные объекты инфраструктуры государств. Во всём мире растет число случаев использования ИКТ для распространения идей экстремизма и терроризма, совершения трансграничных преступлений, связанных с нарушением прав и свобод человека.

Информационное пространство и киберпространство постепенно превращаются практически в «зону боевых действий». Проблема информационной безопасности стала глобальной проблемой в связи с реальной возможностью применения потенциала новейших ИТК в целях обеспечения военно-политического превосходства, силового противоборства и шантажа.

Вследствие сказанного взаимодействие в сфере обеспечения международной информационной безопасности является одним из приоритетных направлений сотрудничества государств – участников СНГ.

Информационная безопасность является сегодня важнейшим компонентом национальной, региональной и международной безопасности. Государства, являющиеся участниками СНГ, выступили инициаторами подготовки ежегодно принимаемой Генеральной Ассамблеей ООН резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», отвечающей интересам всего мирового сообщества.

Проблема информационной безопасности связана с категорией суверенитета и юрисдикции государств, что 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.

Советом глав государств СНГ ещё в 2008 г. была принята Концепция сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности. Комплексным планом мероприятий по реализации Концепции была предусмотрена разработка Рекомендаций по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности. Проект таких Рекомендаций, разработанный коллективом российских и белорусских учёных, публиковался для широкого обсуждения на страницах ряда периодических печатных изданий, представлялся на международных научных конференциях. Этот документ, носящий концептуальный характер, прошел экспертное обсуждение в парламентах государств-участников и был принят на 38-м пленарном заседании Межпарламентской Ассамблеи СНГ (МПА СНГ) в 2012 г.

В принятых МПА СНГ Рекомендациях были обоснованы предложения: об изменении существовавшего с 2005 г. базового Модельного закона МПА СНГ «Об информатизации, информации и защите информации» и о разработке нового Модельного закона «О критически важных объектах информационно-коммуникационной инфраструктуры», а также о подготовке Стратегии обеспечения информационной безопасности государств – участников СНГ. Эти предложения были поддержаны Советом Федерации Федерального Собрания Российской Федерации; комплекс законодательных инициатив получил своё закрепление в межгосударственных программах сотрудничества государств – участников СНГ в сфере безопасности на 2014–2018 гг., которые утвердил Совет глав государств СНГ.

Сложившееся неформальным образом творческое сотрудничество российских и белорусских учёных в области информационной безопасности явилось весьма продуктивным. Разработанный интернациональным авторским коллективом проект Стратегии обеспечения информационной безопасности государств – участников СНГ, после прохождения процедур парламентской экспертизы и межпарламентского согласования, был одобрен на 41-м пленарном заседании МПА СНГ в 2014 г. Этот документ создает методологическую основу согласования деятельности государств в области совершенствования организационного и правового обеспечения информационной безопасности Содружества и может быть использован при планировании деятельности по обеспечению информационной безопасности государств – участников СНГ.

Принятие проекта Стратегии информационной безопасности государств – участников СНГ придало новый импульс усилиям в направлении создания совместного потенциала по противодействию информационным угрозам правам и свободам граждан и интересам государства и общества, обозначило вектор их приложения, сформировало цели реализации. Однако на сегодня актуальным остаётся вопрос практического внедрения данной разработки в практику международного взаимодействия государств – участников СНГ.

В 2014 – 2016 гг. рассмотрение Стратегии проходило в рабочих органах Экономического совета и Исполнительного комитета СНГ. Комиссия по экономическим вопросам Экономического совета СНГ, рассмотревшая принятый Межпарламентской Ассамблеей документ, направила его на согласование в правительства государств – участников (2014). Экспертная группа Исполкома СНГ согласовала документ, доработанный с учётом поступивших от ряда государств Содружества замечаний (2015).

В 2016 г. документ был направлен в Совет постоянных полномочных представителей государств – участников СНГ при уставных и других органах Содружества для включения вопроса о его рассмотрении в повестку дня очередного заседания Совета министров иностранных дел государств – участников СНГ.

Практика показывает, что разработанные российскими и белорусскими учёными ещё в 2013 г. теоретические конструкции Стратегии информационной безопасности государств – участников СНГ, заложенные в ней подходы остаются актуальными и востребованными и сегодня. Вместе с тем представляется, что в условиях возрастающей динамики информационных отношений, при настойчивом социальном заказе на концептуальные и правовые основы информационной безопасности затягивание процесса принятия Стратегии является сдерживающим фактором развития сотрудничества в области совершенствования международной информационной безопасности на пространстве Содружества Независимых Государств.

Будем надеяться, что Содружество Независимых Государств, являющееся одной из авторитетных международных организаций, продолжит активную деятельность в области создания эффективной системы обеспечения международной информационной безопасности.

Директор СПИИРАН,
член-корреспондент РАН
Р.М. Юсупов

ЧАСТЬ 1. ПРОБЛЕМА ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

==========

ГЛАВА 1. СТАНОВЛЕНИЕ И РАЗВИТИЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРАХ ДЕЯТЕЛЬНОСТИ СНГ И ОДКБ

1.1. Правовые формы сотрудничества государств – участников СНГ и государств – членов ОДКБ по обеспечению международной информационной безопасности

Сегодня, когда мир еще не определился в отношении «сетевой паутины» информационно-коммуникационных технологий (ИКТ), только через пробы и ошибки прокладывает путь к гармонизации международных информационных отношений, проявляется особый интерес к истории и поиску корней, лежащих в основе эффективных форм взаимодействия (государств, народов, религий), выбору пути наименьших потерь уже имеющихся ресурсов исторического развития планеты.

После образования на пространстве бывшего СССР ряда независимых государств их, в том числе, информационное взаимодействие формируется и развивается в рамках региональных международных организаций, первыми из которых стали Содружество Независимых Государств (СНГ) и Организация Договора о коллективной безопасности (ОДКБ)[1]. 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. Учредительные документы СНГ и ОДКБ зарегистрированы в Секретариате ООН в соответствии со статьёй 102 Устава ООН. В 2004 г. ООН предоставила ОДКБ статус наблюдателя.

В современных геополитических, технологических и экономических условиях отношения постсоветских независимых государств, реализующиеся в региональных формах международного сотрудничества, требуют общих или согласованных подходов (в том числе, по проблемам информационного взаимодействия и информационной безопасности). Одним из способов решения на международном уровне встающих на этом пути задач является сближение законодательства.

Известный исследователь проблем становления современного права профессор Ю.А. Тихомиров подчеркнул: «*Важно знать, что большая работа по сближению национальных законодательств проводится в рамках МПА СНГ. Ее основой служат согласование концепций развития национального законодательства, выработка общих подходов и решений, рассмотрение вариантов, возможных коллизий и их последствий. Аналитическое сопоставление научных концепций и объективная оценка информации*

---

[1] Целями СНГ в соответствии с Уставом этой международной организации является развитие равноправного и взаимовыгодного сотрудничества народов и государств, содействие широкому информационному обмену.
ОДКБ – организация военно-политического сотрудничества. Она ориентируется на защиту суверенитета государств – членов от внешних воздействий и на обеспечение их безопасности по всем направлениям. ОДКБ сегодня превратилась в полноформатную многофункциональную региональную структуру противодействия традиционным и новым вызовам и угрозам миру, безопасности и стабильности. Диапазон таких вызовов в последнее время неуклонно расширяется, распространяясь и на информационную сферу.

позволяют избегать ошибок и односторонних действий и находить приемлемые для государств-участников варианты решений»[2].

Ведущую роль в этом процессе занимает совместное законодательное моделирование. Его результатом являются модельные законодательные акты и иные формы правовых конструкций, предлагаемых для регулирования однотипных и комплексных общественных отношений. «*Модельный закон есть законодательный акт рекомендательного характера, содержащий типовые нормы и дающий нормативную ориентацию для законодателя. Он не является обязательным для законодательных органов и служит для них нормативно-ориентирующим стандартом. И первое, что бросается в глаза, — свойство модельных актов быть своеобразным «мостом» между нормами международного и национального права, способность «вплетаться» в ткань национальных нормативных систем. Модельные законы непосредственно «впитывают» в себя принципы и нормы международного права, «переводя» их в нормативно-концентрированном виде в национальные законодательные акты*»[3].

Вместе с тем, как отмечают исследователи, сегодня очевиден недостаточный прогресс в имплементации конструкций модельного законодательства СНГ и ОДКБ в нормы законодательства национального[4]. Повышению эффективности этого процесса может способствовать, например, заимствование опыта Южно-Американского союза государств и авторитет модельного законотворчества Южной Америки, где национальные законы подтверждаются резолюцией парламента Ассамблеи[5].

Динамика сближения законодательства в форматах СНГ и ОДКБ приобретает сегодня особую значимость в вопросах правового обеспечения региональной безопасности, в том числе, в информационной сфере. В рамках этих международных организаций проводится системная работа по формированию единой понятийной базы, сопряжению научных подходов и направлений практического обеспечения информационной безопасности, гармонизации правовых механизмов и унификации законодательства. В условиях глобализации экономического, социального и культурного развития, ускоряющейся информатизации общества особую значимость приобретают такие политические мобилизующие документы как стратегии национальной безопасности и стратегии развития информационного общества, с учётом нашедших отражение в них аспектов обеспечения информационной безопасности.

---

[2] Тихомиров, Ю.А. Курс сравнительного правоведения. / Ю.А. Тихомиров.— М.: Издательство НОРМА, 1996. — 432 с.

[3] Там же.

[4] «Объективно оценивая результаты модельного законотворчества в интересах СНГ и ОДКБ необходимо констатировать, что национальный законодательный процесс демонстрирует порой отрешенность и невосприимчивость к результатам законодательного моделирования. В то же время, не следует забывать, что «политический аспект воздействия рекомендательных норм имеет не меньшее значение, чем правовой. Являясь согласованными моделями желательных для международного сообщества норм поведения государств, эти нормы дают определенный толчок практике государств, консолидируют ее» (Шестакова Е.В. Модельное законодательство (Теоретико-правовые аспекты и практика применения): Дис. канд. юрид. наук: 12.00.01 Москва, 2006 203 с. РГБ ОД, 61:06-12/1481)

[5] Союз южноамериканских Стран (USAN) является межправи-тельственным союзом, объединяющим два существующих таможенных союза: МЕРКОСУР и Андское Сообщество Стран, как часть продолжающегося процесса южноамериканской интеграции (авт.).

1.2. Развитие правового регулирования обеспечения международной информационной безопасности государств – участников СНГ

Межпарламентская Ассамблея СНГ, состоящая из парламентских делегаций государств – участников, взаимодействует со всеми странами Содружества в сфере безопасности. С момента подписания Алма-Атинского Соглашения о Межпарламентской Ассамблее государств – участников СНГ (1992 г.) одним из приоритетов в деятельности МПА СНГ явилось содействие в реализации международных договоров и межгосударственных программ сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности. Адаптируя международный опыт борьбы с угрозами информационной безопасности применительно к условиям государств Содружества, МПА СНГ разрабатывает для них типовые модельные законодательные акты и рекомендации. Эти документы, как отмечалось выше, не обладают обязательной юридической силой, однако наличие типовых моделей правового регулирования определённых отношений составляет потенциал для развития национальных систем информационного законодательства в общем ключе. Благодаря их наличию создаётся механизм имплементации положений международно–правовых документов в национальные правовые системы государств – участников СНГ.

Профильным органом в обсуждаемой сфере на первом этапе явилась Постоянная комиссия МПА СНГ по вопросам обороны и безопасности, которая с первых шагов своей деятельности основные усилия сконцентрировала на формировании общих правовых стандартов безопасности для стран Содружества. Эта деятельность осуществлялась в соответствии с решениями и другими руководящими документами, принимавшимися высшими уставными органами СНГ[6].

На первых этапах интеграционного сотрудничества Независимых Государств наибольшее влияние на формирование национальных законодательств в сфере обеспечения информационной безопасности оказали разработанные в рамках деятельности Постоянной комиссии Модельные законы: «О персональных данных» (1999), «Об электронной цифровой подписи» (2000), «О государственных секретах» (2003), «Об оперативно-розыскной деятельности» (2006), а также многие рекомендации и иные документы, принятые МПА СНГ по инициативе данной комиссии.

В 2004 г. на базе Постоянной комиссии МПА СНГ по вопросам обороны и безопасности была учреждена Объединенная комиссия по гармонизации законодательства в сфере борьбы с терроризмом, преступностью и наркобизнесом в СНГ. В 2013 г. она получила свое второе название — Объединенная комиссия при МПА СНГ по гармонизации законодательства в сфере безопасности и противодействия новым вызовам и угрозам. Особенность этого органа состоит в том, что в его состав, наряду с парламентариями, вошли представители специализированных органов СНГ и компетентных органов государств – участников Содружества.

Первыми актами СНГ, относящимися к информационной сфере, явились Соглашение «О сотрудничестве в области информации» и Рекомендательный законодательный Акт «О принципах регулирования информационных отношений в государствах – участниках Межпарламентской Ассамблеи» (1993). В 1996 г. была

[6] В результате работы этой профильной комиссии МПА СНГ к 2004 г. разработала и приняла 42 документа, основную часть которых составили специальные модельные законодательные акты в различных областях обеспечения обороны и безопасности, что было четвертой частью основного наработанного МПА СНГ массива документов за время ее деятельности к тому времени.

принята Концепция формирования информационного пространства Содружества Независимых Государств. Десятилетием позже Советом глав государств СНГ была принята Стратегия сотрудничества в сфере информатизации; следом, а в 2008 г. была принята Концепция сотрудничества государств – участников СНГ в сфере 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. Этот вопрос с некоторым запозданием нашел своё отражение в Перспективном плане модельного законотворчества в СНГ на 2011–2015 гг.[7].

В 2012 г. Советом глав государств СНГ была принята Стратегия сотрудничества государств в построении и развитии информационного общества, а в ноябре 2013 г. было подписано Соглашение «О сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности».

Бурное и стремительное развитие информационной сферы в начале XXI в. обусловило отставание в выработке правовых механизмов адекватного реагирования на новые вызовы и угрозы. Несмотря на то, что в СНГ и ОДКБ и до этого принимались межгосударственные документы, имеющие важное значение для обеспечения информационной безопасности, следует признать, что они объективно они не смогли исключить негативные проявления в данной сфере. Современный уровень вызовов и угроз информационной безопасности детерминировал необходимость поиска новых подходов к комплексному, в том числе, правовому противодействию им.

В соответствии с планами работы МПА СНГ интернациональный коллектив российских и белорусских учёных в 2010–2012 гг. 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 обсуждался на научных конференциях и публиковался для широкого обсуждения на страницах ряда периодических научных изданий, что способствовало продвижению и, в конечном итоге, предопределило успешное завершение работы над ним.[8] Проект выдержал комплексную экспертизу в парламентах государств – участников СНГ. Рекомендации по совершенствованию и гармонизации национального законодательства в сфере информационной безопасности были приняты на 38-м пленарном заседании МПА СНГ (постановление от 23.11.2012 № 38-20)[9].

В названных Рекомендациях был обоснован комплекс предложений: об изменении действовавшего в то время базового Модельного закона «Об информатизации, информации и защите информации»; о разработке нового Модельного закона «Об объектах критически важной информационно-коммуникационной инфраструктуры»; о подготовке Модельного регламента административных процедур, осуществляемых

---

[7] Вус, М.А. К вопросу о разработке рекомендаций по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности. / М.А. Вус, О.С. Макаров // Информатизация и связь. – 2012. – № 1. – С. 5-8.

[8] О совершенствовании и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности / И.Л. Бачило, В.В. Бондуровский, М.А. Вус, М.М. Кучерявый, О.С. Макаров // Информационное право. – 2013. – № 1(32). – С. 24-27.

[9] Информационный бюллетень МПА СНГ. – 2013. – № 57. – Часть 2. – С. 161-179.

уполномоченными органами в сфере обеспечения информационной безопасности государств – участников СНГ, а также о необходимости разработки для Содружества проекта Стратегии обеспечения информационной безопасности. Все эти предложения были поддержаны Советом Федерации Федерального Собрания Российской Федерации и нашли своё отражение в обновлённом Перспективном плане модельного законотворчества МПА СНГ на 2012–2015 гг.[10] В дальнейшем комплекс законодательных инициатив получил своё закрепление в межгосударственных программах сотрудничества в сфере безопасности на период 2014–2018 гг., утверждённых Советом глав государств СНГ[11].

Все проекты межгосударственных документов, разработанные интернациональным коллективом российских и белорусских учёных, прошли комплексную экспертизу в государствах Содружества и были приняты на 41-м пленарном заседании МПА СНГ (постановление от 28.11.2014 №№ 41-13 – 41-17), а одобренный МПА СНГ проект Стратегии обеспечения информационной безопасности государств – участников Содружества Независимых Государств направлен в Исполнительный комитет СНГ для рассмотрения в установленном порядке с перспективой его принятия высшими уставными органами СНГ и подготовки новых межгосударственных программ сотрудничества в сфере безопасности[12].

В рамках мероприятий Программы сотрудничества государств – участников СНГ по борьбе с терроризмом и иными насильственными проявлениями экстремизма тем же инициативным российско-белорусским научным коллективом в 2013 г. была проведена работа по разработке Рекомендаций по правовому регулированию эксплуатации открытых телекоммуникационных сетей (ОТКС) для предупреждения их использования в террористических и иных противоправных целях. Документ, успешно прошедший экспертизу в парламентах государств – участников СНГ, также был принят Межпарламентской Ассамблеей (постановление от 20.11.2013 № 39-25)[13].

В 2015 году российскими и белорусскими учёными осуществлена разработка Комментария к принятому ещё в 2003 г. Модельному закону СНГ «О государственных секретах». Комментарий был принят Постановлением МПА СНГ от 27.11.2015 № 43-19, направлен в парламенты государств – участников Межпарламентской Ассамблеи СНГ и рекомендован для использования в законотворческой деятельности.[14]

Материалы и наработки всех вышеназванных проектов обсуждались на научно-практических конференциях: «Теоретические и прикладные проблемы информационной безопасности» (Республика Беларусь, г. Минск, 2012 и 2014 г.), «Информационная безопасность как составляющая национальной безопасности государства» (Республика Беларусь, г. Минск, 2013 г.); «Информационная безопасность Регионов России (ИБРР-2013)» и «Региональная информатика (Российская Федерация, г. Санкт-Петербург, 2012 и 2014 г.)» и др. Об итогах работ и полученных результатах докладывалось на секциях

[10] Информационный бюллетень МПА СНГ. – 2015. – № 62. – Часть 1. – С. 75.
[11] Бачило, И.Л. К вопросу о развитии информационного законодательства СНГ / И.Л. Бачило, М.А. Вус, О.С. Макаров // Информатизация и связь. – 2014. – № 1. – С. 13-16.
[12] Информационный бюллетень МПА СНГ. – 2015, № 62. Часть 2. – С.27-57.
[13] Информационный бюллетень МПА СНГ. – 2014, № 60. Часть 2. – С. 458-477.
[14] Информационный бюллетень МПА СНГ. – 2016, № 64. Часть 2. – С. 255-402.

национального ИНФОФОРУМА по информационной безопасности (2012–2015 гг.), материалы исследований и разработок публиковались в научных изданиях[15].

В период 2010–2016 гг. были российскими и белорусскими учёными реализованы важные шаги на пути становления правового обеспечения информационной безопасности на пространстве СНГ. Были разработаны стратегические направления обеспечения информационной безопасности; сформирован и научно обоснован определенный понятийный аппарат; обоснованы и предложены новые модельные конструкции обеспечения защиты критически важных объектов информатизации и открытых телекоммуникационных сетей, а также информационных ресурсов ограниченного доступа.

1.3. Развитие правового регулирования обеспечения международной информационной безопасности в сфере отношений государств – членов ОДКБ

Договор о коллективной безопасности на постсоветском пространстве был подписан в 1992 г., однако ОДКБ, как организация военно-политического 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 опасности в Концепции коллективной безопасности ОДКБ указаны попытки вмешательства извне во внутренние дела государств, попытки дестабилизации их внутриполитической обстановки, международный терроризм, политика шантажа.

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 гармонизация положений национальных законодательных актов в области обороны и безопасности. В целях реализации данного направления в 2006 г. была создана Парламентская Ассамблея ОДКБ – орган межпарламентского сотрудничества государств – членов ОДКБ.

Программа совместных действий государств – членов ОДКБ по формированию системы информационной безопасности была принята в 2008 г. В 2010 г. обеспечение информационной безопасности, как важное направление сотрудничества, было

---

[15] Бачило И.Л. Об изменениях модельного закона СНГ «Об информатизации, информации и защите информации» (2005) в его новой редакции с изменённым названием «Об информации, информатизации и обеспечении информационной безопасности» / И.Л. Бачило, М.А. Вус, О.С. Макаров // Информатизация и связь. – 2014. – № 3. – С.9-13.

закреплено в Уставе ОДКБ.[16] 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 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 вызовам и угрозам в информационной сфере.

Заявленная постановка научной проблематики послужила основой для разработки российско-белорусским авторским коллективом Рекомендаций по сближению и гармонизации законодательства государств – членов ОДКБ в сфере информационно-коммуникационной безопасности, принятых ПА ОДКБ в 2014 г. (постановление от 27.11.2014 № 7-6).[17] Разработчиками этого документа было акцентировано внимание на особой актуальности формирования активной согласованной информационной политики государств – членов ОДКБ, развитии общего информационного пространства и создании совместного потенциала по противодействию информационным угрозам. В принятых ПА ОДКБ Рекомендациях сформулированы общие подходы к сближению законодательства государств – членов ОДКБ в сфере информационно-коммуникационной безопасности, а также предложен алгоритм его реализации[18]. В качестве приложения к Рекомендациям разработан примерный перечень наиболее опасных правонарушений в области информационной безопасности, затрагивающих

---

[16] В формате ОДКБ принят подход, согласно которому под информационной безопасностью понимается «состояние защищенности личности, общества, государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве».

[17] Для совершенствования системы информационной безопасности в ОДКБ / М.А. Вус, М.М. Кучерявый, О.С. Макаров, Г.И. Перекопский // Власть – 2014. – № 8. – С.37-40.

[18] Документы седьмого пленарного заседания Парламентской Ассамблеи Организации Договора о коллективной безопасности. Санкт-Петербург, 27 ноября 2014 г. – МПА СНГ. Приложение к «Информационному бюллетеню». – 2015. – № 62. – С. 124.

национальные интересы государств и посягающих на законные права и интересы граждан государств – членов Организации Договора о коллективной безопасности[19].

Ещё ранее постановлением ПА ОДКБ в 2010 г. были приняты разработанные в ФГБУН «Санкт-Петербургский институт информатики и автоматизации Российской академии наук» Рекомендации по сближению законодательства государств – членов ОДКБ по вопросам государственной тайны. Эта работа выполнялась в сотрудничестве с сектором информационного права ФГБУН «Институт государства и права Российской академии наук» (г. Москва) и ГУО «Институт национальной безопасности Республики Беларусь» (г. Минск). Принятый ПА ОДКБ документ был направлен в парламенты государств – членов ОДКБ «для использования в работе по приведению национального законодательства в соответствие с принятыми рекомендациями»[20].

Одновременно с названными Рекомендациями их разработчиками был подготовлен и выпущен в свет «Глоссарий основных понятий в законодательстве о государственной тайне государств – членов ОДКБ»[21]. В 2014 г. Санкт-Петербургский институт информатики и автоматизации Российской академии наук подготовил и выпустил в свет «Словарь – справочник по информационной безопасности для Парламентской Ассамблеи ОДКБ»[22]. В перспективных планах ПА ОДКБ — разработка проекта Модельного закона «О государственной тайне»[23].

Всё вышеизложенное позволяет констатировать, что Организацией Договора о коллективной безопасности ведется активная работа по формированию правовых основ обеспечения информационной безопасности в рамках уставных задач этой организации. На сегодняшний день пройден этап сопряжения национальных правовых представлений об информационной безопасности и становится очевидной необходимость подготовки и принятия соглашения государств – членов ОДКБ по её обеспечению.

1.4. Проблемы правового регулирования обеспечения международной информационной безопасности

В связи с тем, что современное общество всё более трансформирует свои социальные отношения перемещая их в информационную среду, где традиционные, выработанные тысячелетиями регуляторы безопасности не действуют или действуют недостаточно эффективно, а адекватных систем их защиты в информационной сфере пока не разработано, социум претерпевает негативные последствия реализации информационных угроз: растет информационная преступность, на личность оказывается деструктивное информационное воздействие, углубляется кризис институтов тайн и т.д. В современных условиях рельефно проявляется дилемма: обозримый путь общественного развития пролегает через процессы информатизации, однако

---

[19] Там же. – С. 145-146.

[20] Документы седьмого пленарного заседания Парламентской Ассамблеи Организации Договора о коллективной безопасности. Санкт-Петербург, 27 октября 2010 г. – МПА СНГ. Приложение к «Информационному бюллетеню». – 2011. – № 48. – С. 78-126.

[21] Глоссарий основных понятий в законодательстве о государственной тайне государств – членов ОДКБ / Сост.: И.Л .Бачило, М.А. Вус, В.С. Гусев, О.С. Макаров. – СПб.: СПИИРАН, 2011. – 79 с.

[22] 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.

[23] Макаров, О.С. О защите государственных секретов в ОДКБ / О.С. Макаров, М.А. Вус, М.М. Кучерявый // Информатизация и связь. – 2013. – № 6. – С. 31-33.

информатизация общества порождает геометрическое возрастание угроз национальной безопасности.[24]

Результаты наблюдений и научных обобщений позволяют отметить, что основным угрозообразующим для информационной безопасности фактором во втором десятилетии XXI века стал нарастающий дисбаланс между прорывным насыщением потребностей социума технологиями информатизации и ощутимым отставанием в организации использования всё возрастающего информационного ресурса общества. Цифровая эпоха сделала первые шаги в технологическом направлении, но испытывает сложности в синхронизации интересов акторов и обеспечении их безопасности. Однако именно от этой стороны процесса зависит переход к цифре в области управления, реализации программ социального развития, обеспечение прав человека и гражданина, совершенствование демократических процессов и т.д. В этой части еще предстоит преодолеть пороги, оставляемые обществом при переходе к новому этапу цивилизационного развития. Таким образом, процессы обеспечения информационной безопасности оказываются напрямую связанными с условиями нового этапа информатизации: переходом от насыщения общества средствами ИКТ к использованию информационных ресурсов в решении задач социального, политического, культурного развития.[25]

В современном мире всё диалектично, вследствие чего побочным эффектом технологического прогресса становятся негативные факторы социального, культурного, экономического плана (киберпреступность, кибертерроризм, информационные войны и др.), питательной средой которых среди прочих выступают информационное, цифровое неравенство, правовая неопределенность и безнаказанность. Для продолжения прогрессивного развития информационного общества необходимо обеспечить эффективное противодействие угрозам использования современных информационных технологий для нарушения мира и безопасности, совершения преступлений, подготовки и осуществления террористических актов, распространения террористической идеологии в практике разрешения противоречий общественного развития. Такая работа в силу трансграничности угроз информационной безопасности должна проводиться как на национальном уровне, так и с позиций международного (регионального) взаимодействия.

Формирование системы обеспечения международной информационной безопасности определяется степенью политического доверия между правительствами государств с учётом принципов взаимопонимания, равноправия и согласованности интересов. Вследствие этого очевидна необходимость ведения диалога по всему спектру этих вопросов, разработка и совершенствование международных договоров и национального законодательства в области информационной безопасности. Непременным условием решения вопросов по правовому и организационному обеспечению информационной безопасности является понимание того, что государство находится в неразрывной связи и взаимодействии с другими аналогичными структурами и субъектами, реализуя функции стратегического и тактического партнерства, сотрудничества и добрососедства.

---

[24] Информационное общество: Информационное управление. Информационные войны. Информационная безопасность / С.М. Виноградова [и др.]; под общ. ред. М.А. Вуса.– СПб.: Изд-во СПбУ. ФЦП «Интеграция», 1999. – 212 с.

[25] Юсупов, Р.М. Научно-методологические основы информатизации. / Р.М. Юсупов, В.П Заболотский В.П. – СПб.: Наука, 2000. - 455 с.

Представляется, что решение обозначенных выше проблем находится не в технической, а в социальной плоскости, и предполагает осознание обществом новых, обусловленных процессами информатизации условий социальной жизни и выработку определенных правил безопасной межличностной, общественной, государственной и межгосударственной коммуникации с последующим их юридическим закреплением и формированием соответствующего механизма обеспечения безопасности складывающихся отношений.

В современных условиях особую роль в обеспечении информационной безопасности призвано выполнить право, взаимодействие правовых систем разных государств и отраслей национального законодательства в рамках каждой правовой системы. Во всех областях жизни социума для поддержания стратегической стабильности и партнерства, и одновременно для создания условий формирования безопасного информационного общества, настоятельно необходима адекватная нормативно-правовая основа.

Сегодня приходится констатировать, что в области современного правового регулирования всей сферы информационного взаимодействия складывается ситуация напряжения и это предопределяет поиск поворота к оздоровлению информационной среды (особенно Интернет-среды), поиск путей обеспечения информационной безопасности. В таких условиях на первый план выходят вопросы урегулирования новых формирующихся отношений, а также вопросы оценки адекватности и продуктивности, с позиций информационной безопасности, уже принятых законов, как национальных, так и международных правовых актов.

Идущий процесс поиска адекватных форм организации и правового регулирования как внутригосударственных, так и международных отношений тормозится рядом обстоятельств. К их числу следует отнести разрыв в подготовке специалистов (разные языки во взаимодействии специалистов по информатике и информационной безопасности), неоправданную ориентацию преимущественно на защиту информационных ресурсов ограниченного доступа при ослабленном внимании к безопасности «открытых данных» и «свободного программного обеспечения» как к источникам опасности в социальных сетях и во всей системе взаимодействующих социального и экономического информационных пространств. Это далеко не все факторы, которые нуждаются в большем внимании в связи с наведением порядка в обеспечении информационной безопасности[26]. Но и их достаточно для иллюстрации первостепенности комплекса задач правового регулирования в этой сфере.

Учет динамики процессов использования информационных технологий и информационных ресурсов (как во внутригосударственном управлении, так и в практике межгосударственного взаимодействия), а также необходимость своевременной реакции на изменения в трендах соответствующих сфер социального и информационного

---

[26] В структуре исследования проблем информационной безопасности также выделяются следующие темы:
1) причины, мотивы и формы возникновения конфликтов в информационной сфере;
2) правовые проблемы обеспечения информационной безопасности на национальном и межгосударственном уровне: государств – участников СНГ, ОДКБ;
3) вопросы уголовной, административной ответственности за правонарушения и преступления в информационной сфере;
4) правового режима тайн, конфиденциальной и персональной информации (См.: Бачило, И.Л. Факторы развития гражданского общества в условиях информатизации / И.Л. Бачило. Государство и право XXI век. Реальное и виртуальное. – М., 2012. – С. 99-129.)

развития[27] определяют направления, масштабы и формы правового и организационного обеспечения информационной безопасности. Это одинаково актуально как на национальном уровне, так и в рамках международного сотрудничества государств – участников СНГ (также и государств – членов ОДКБ).

Задачи охраны и защиты информационных ресурсов и информационно-коммуникационных технологий, как информационно-технологической системы, не исчерпывают проблем обеспечения информационной безопасности в СНГ, ОДКБ и в объединяющих ими государствах. В настоящий момент особенно важно обеспечение информационной безопасности в таких сферах общественной жизни как трудовая занятость населения, экономика, социальная среда. Требуют внимания процессы миграции, толерантности и законности в областях национальной, этнической, религиозной напряженности в связи со свободным передвижением населения. Не перестают быть актуальными проблемы в области борьбы с наркоманией; проблемы, связанные с детской преступностью и уязвимостью детей от воздействия пропаганды информации, вредной для их развития.[28]

Названные проблемы информационной безопасности актуальны не только во внутренней жизни каждого государства, но и во всей системе стратегического взаимодействия государств в рамках СНГ (ОДКБ). Вопросы обеспечения информационной безопасности сопровождают, а часто и предопределяют, безопасность во всех направлениях жизни каждого государства и их взаимодействия в процессе сотрудничества и партнерства. Здесь организационные и правовые механизмы призваны обеспечить как внутригосударственный порядок безопасности, так и синхронизировать его в разных формах взаимодействия и деловых контактов.

Схожесть подходов государств двух указанных региональных международных организаций в преодолении проблем обеспечения информационной безопасности может послужить основой для создания межгосударственной системы её обеспечения в рамках СНГ, ОДКБ, а также других региональных союзов, формирования единого экономического пространства с учетом специфики среды сетевых инфокоммуникаций.

Формирование институтов правового регулирования обеспечения информационной безопасности осуществляется не только в региональном, но и в глобальном международном масштабе. Китай, Россия, Таджикистан и Узбекистан еще в 2011 г. совместно выработали предложения для резолюции Генеральной Ассамблеи «Правила поведения в области обеспечения международной информационной безопасности» и направили этот документ в адрес Генерального секретаря ООН. Одновременно была предпринята попытка подготовки концепции «юридически обязывающей» Конвенции обеспечения международной информационной безопасности. Этот документ был обсужден на ряде международных встреч, но пока не получил юридического оформления на уровне ООН[29].

Группа правительственных экспертов ООН по международной информационной безопасности (МИБ), завершившая свою работу в июне 2013 г., консенсусом приняла проект доклада для вынесения на Генеральную Ассамблею ООН, в котором закреплен

---

[27] См., например, Новости@Mail.ru.Новости Политики: В США ужесточили меры сохранения данных после утечек Сноудена [Электронный ресурс]. – Режим доступа: https://news.mail.ru/politics/13970162. - Дата доступа: 22.09.2015.

[28] Бачило, И.Л. О причинах и мотивах правонарушений в области расовых, этнических, национальных и религиозных отношений / И.Л. Бачило. – Государство и право. – № 3. – 2013. – С. 33-43.

[29] Смирнов, А.И. Глобальная безопасность и «мягкая сила 2.0.»: вызовы и возможности для России / А.И. Смирнов, И.Н. Кохтюлина. - М., 2012. – С. 98-103.

тезис о заинтересованности всех стран именно в мирном использовании ИКТ. По инициативе России в 2014 г. была созвана новая Группа экспертов по МИБ, которая могла бы детально проработать совокупность политико-правовых вопросов обеспечения информационной безопасности.

Концепцию данной инициативы можно охарактеризовать, как намерение криминализировать угрозы информационной безопасности и перевести информационное противоборство в правоохранительную плоскость, что наглядно иллюстрирует тезис, озвученный Послом по особым поручениям МИД России А.В. Крутских: «*Главное понять: мы все — за предотвращение кибервойн или за их регулирование и, следовательно, легитимизацию. Россия однозначно — за первый вариант*»[30].

Краткий обзор современных подходов и инициатив в сфере правового регулирования МИБ свидетельствует о важных шагах на пути формировании системы правового обеспечения региональной и глобальной информационной безопасности. Необходимыми условиями успешности данного процесса представляются синхронность темпов развития информационных отношений, интенсивности разработки и внедрения всеобъемлющих юридически обязывающих мер по неукоснительному соблюдению принципа неприкосновенности национального суверенитета государств.

* * *

[30] Информационная безопасность как составляющая национальной безопасности государства: материалы междунар. науч.-практ. конф. Минск, 11–13 июля 2013: в 3 т. / Ин-т. нац. безопасности Респ. Беларусь: редкол. С.Н. Князев [и др.]. – Минск, 2013. – Т.1. – 174 с.

ГЛАВА 2. ПОНЯТИЙНО-КАТЕГОРИАЛЬНЫЙ АППАРАТ В СФЕРЕ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СНГ и ОДКБ

2.1. Вектор формирования понятийно-категориального аппарата в сфере обеспечения международной информационной безопасности

Решение задач обеспечения информационной безопасности требует сотрудничества и партнерства на всех уровнях: индивидуальном, корпоративном, государственном и международном. Для эффективного взаимодействия необходимы выработка понятийного аппарата и согласованное использование базовых терминов и дефиниций в научной и практической деятельности, процессах международного взаимодействия, нормативных актах.

Терминологическое многообразие и слабая определенность используемых в различных документах понятий становятся сегодня актуальной проблемой. И, как следствие, в свете решения задач правового регулирования отношений в сфере обеспечения международной информационной безопасности исключительную важность приобретает вопрос проработки и однозначного толкования правовых дефиниций. Практика межгосударственного сотрудничества настоятельно требует унификации и единообразия трактовок в нормативно-правовой базе государств – участников основных терминов и понятий, используемых в процессе взаимодействия государств, их органов и организаций. Необходимо достигнуть создания цепочки генетической связи между пониманием и наполнением определенным смыслом таких понятий, как «опасность», «безопасность», «информационная безопасность», «обеспечение информационной безопасности», «правовое обеспечение информационной безопасности», «угрозы безопасности», «кибербезопасность», «преступления с применением средств ИКТ» и др. Без понимания связи названных концептов невозможно наполнить необходимым содержанием правовое обеспечение информационной безопасности, а также адекватно оценить существующее состояние законодательства в этой области.

Унификацию понятийно-категориального аппарата предлагается рассматривать как одно из приоритетных направлений совершенствования законодательства и эффективного правоприменения. При этом унификацию терминов следует осуществлять в отношении всех нормативных правовых актов, предметом правового регулирования которых являются информационные отношения и обеспечение информационной безопасности. При толковании понятий, которые еще не включены в национальное законодательство, но уже содержатся в модельных законодательных актах МПА СНГ или ПА ОДКБ, представляется рациональным рекомендовать государствам – участникам использовать положение последних.

При проработке и уточнении содержательного наполнения встречающихся в международной практике терминов, согласовании, одобрении и их переводах на национальные языки, а также дополнении терминами, используемыми в национальных законодательствах, может быть сформирован многоязычный терминологический словарь в сфере обеспечения международной информационной безопасности на пространствах СНГ и ОДКБ. Создание такого терминологического словаря в сфере обеспечения международной информационной безопасности должно стать практически полезным, прежде всего, для законотворческой деятельности и правоприменительной

практики. Первый опыт подобной работы оказался весьма успешным. Коллектив составителей Словаря-справочника терминов и определений понятий модельного законодательства государств – участников СНГ, вышедшего в свет в 2012 г., был отмечен дипломом Национального форума информационной безопасности «ИНФОФОРУМ–2013».[31]

Сегодня создание словаря-тезауруса терминов, используемых в области правового регулирования отношений по обеспечению информационной безопасности, представляется исключительно полезным для практики регулирования правовых отношений и взаимодействия в таких международных образованиях, как Евразийский экономический Союз, БРИКС и др.

2.2. Феномен информационной безопасности

Прогресс информационно-коммуникационных технологий, повлекший многообразие информационных процессов и развитие информационных отношений современного общества обусловил потребность введения в юридический оборот понятия «информационная безопасность». Результаты использования законодателем данного понятия[32] наглядно иллюстрируют проблемы и трудности юридической техники, выразившиеся в формировании антагонистических подходов к его толкованию, а также отсутствии единой исчерпывающей трактовки, отражающей феноменологическую сущность явления информационная безопасность.

Само понятие «информационная безопасность» является достаточно широким и в разных контекстах отличается своим содержательным наполнением. Это обстоятельство отражается, прежде всего, на лексике сферы информационной безопасности. Впервые в законодательстве СНГ понятие «информационная безопасность» было использовано в Рекомендательном акте «О принципах регулирования информационных отношений в государствах МПА СНГ» (1993), однако его конкретное содержание при этом не раскрывалось. В международно-правовых актах СНГ рассматриваемое понятие 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». Трактовка этого термина в законе, принятом МПА СНГ, совпала с его определением, использованном в Федеральном законе «Об участии в международном информационном обмене» (1996), который в настоящее время утратил силу.

В Законе Республики Казахстан «О национальной безопасности» (1998) термин информационная безопасность определен как «состояние защищенности государственных информационных ресурсов, а также прав личности и интересов общества в информационной сфере». Акцент сделан, в первую очередь, на защищенности государственных информационных ресурсов.

Доктрина информационной безопасности Российской Федерации (2000) и Концепция национальной безопасности Республики Таджикистан (2003) используют

---

[31] Словарь-справочник терминов и определений понятий модельного законодательства государств – участников СНГ / Под ред. М.А. Вуса и В.В. Бондуровского. – СПб.: Издательство «Юридический Центр-Пресс», 2012. – 360 с.

[32] Например, Модельный закон СНГ «О международном информационном обмене»; Соглашение между правительствами государств – членов Шанхайской организации сотрудничества от 16 июня 2009 г.; Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года.

такую трактовку понятия: «информационная безопасность — состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства». Акцент сделан здесь на национальных интересах в информационной сфере, которые определяются через интересы субъектов национальной безопасности. В проекте новой Доктрины информационной безопасности Российской Федерации (2016)[33] информационная безопасность рассматривается как состояние защищенности личности, общества и государства от внутренних и внешних угроз в информационной сфере, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации, достойные качество и уровень их жизни, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

В типовом проекте законодательного акта об информационной безопасности МПА ЕврАзЭС (2004), принятом в пакете с законопроектом об основных принципах электронной торговли, понятие информационная безопасность определялось как «состояние защищенности прав, свобод, охраняемых законом интересов физических, юридических лиц и государства в информационной сфере от внутренних и внешних угроз». Такой подход (выделение охраняемых законом интересов), может быть, и адекватен для сферы электронной коммерции, однако представляется, что это частное определение может иметь ограниченную сферу применения.

Стратегия сотрудничества государств – участников СНГ в сфере информатизации, утвержденная в 2006 г. Решением Совета глав государств – участников СНГ, включала определение понятия «информационная безопасность» в трактовке, буквально совпадающей с содержащейся в Доктрине информационной безопасности России и Концепции национальной безопасности Республики Таджикистан. Принятая двумя годами позже Концепция сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности (на период с 2008–2010 гг.), также утвержденная Решением Совета глав государств – участников СНГ[34] использовала уже иное определение этого термина: «информационная безопасность — состояние защищенности от внешних и внутренних угроз информационной сферы, формируемой, развиваемой и используемой с учетом жизненно важных интересов личности, общества и государства». При этом во вводной части документа было отмечено, что, «…проникая во все области человеческой деятельности, ИКТ формируют глобальную информационную сферу, представляющую собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений». Акцент при таком подходе, как видим, в известной мере «традиционно – технократический»: в первую очередь внимание акцентируется на объект (информационную сферу), а только затем уже — на субъекты информационной безопасности (и только «с учетом жизненно важных

[33] http://www.scrf.gov.ru/documents/6/135.html

[34] Указанный документ подписали только Республика Армения, Республика Беларусь, Республика Казахстан, Кыргызская Республика, Российская Федерация и Республика Таджикистан. Все эти шесть государств являются членами ОДКБ.

интересов»?!)[35]. При таком подходе сама проблема информационной безопасности на практике нередко искусственно сужается до задач защиты информации.

Стратегия обеспечения информационной безопасности государств – участников Содружества Независимых Государств[36] использует содержательное наполнение понятия информационная безопасность, впервые приведенное в тексте Соглашения о сотрудничестве в области обеспечения международной информационной безопасности, заключенного в 2009 г. между правительствами государств – членов Шанхайской организации сотрудничества: «Информационная безопасность — состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве»[37]. При такой формулировке это базовое понятие охватывает становящиеся все более актуальными и опасными сегодня угрозы социально-гуманитарного плана, в частности, угрозы распространения информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде государства. Источниками подобных угроз могут являться как государства, так и негосударственные структуры, а также частные лица[38].

Использование вышеназванного толкования рассматриваемого понятия представляется наиболее оправданным и с позиций задач, стоящих перед ОДКБ[39]. Как отмечалось выше, сегодня понятие «информационная безопасность» в данной формулировке нашло свое отражение в Положении о сотрудничестве государств – членов ОДКБ, утвержденном Решением Совета коллективной безопасности ОДКБ от 2010 года.

Ни сколько не умаляя значимости обобщений, представляется, что формальная ориентация на самое ёмкое определение понятия «информационная безопасность» из наиболее ранних нормативных правовых актов лишает нас возможности оценить сущностные характеристики данного термина. Для понимания семантики информационной безопасности представляется необходимым обратиться к нюансам доктринального толкования этого понятия. Существует множество научных трактовок информационной безопасности[40], обобщение которых позволяет определить

---

[35] В этом контексте нельзя не упомянуть прозвучавшие призывы ЮНЕСКО (Париж, 2009 г.) обращать внимание не только на позитивные возможности, которые создают ИКТ, но и на необходимость анализа и учета негативных социальных последствий их бурного распространения и некритического использования.

[36] Постановление Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств от 28.11.2014 г. № 41-13

[37] В числе подписантов этого Соглашения ШОС Республика Казахстан, Кыргызская Республика, Российская Федерация, Республика Таджикистан и Республика Узбекистан, которые являются членами ОДКБ. Республика Беларусь имеет статус наблюдателя в ШОС.

[38] Признаками таких угроз являются появление и тиражирование в средствах массовой информации (включая электронные), в сетях информационного обмена (сети Интернет и др.) информации, которая искажает представление о политической системе, общественном строе, внешней и внутренней политике, важных политических и общественных процессах в государстве, духовных, нравственных и культурных ценностях его населения; информации, которая пропагандирует идеи терроризма, сепаратизма и экстремизма; разжигает межнациональную, межрасовую и межконфессиональную вражду.

[39] Руководствуясь интересами гармонизации законодательства и закрепления правовых понятий в социальном обороте видится полезным избегать излишнего «терминотворчества» в рамках «родственных» интеграционных объединений, ориентируясь на уже имеющиеся дефиниции и заимствуя их (авт.).

[40] «… состояние всех компонентов ИКТ – информационных ресурсов, технологий и коммуникаций, – позволяющее осуществить их формирование и использование в интересах общества, государства и человека при минимизации отрицательных последствий для создателей, держателей и пользователей этих ресурсов, возникающих под влиянием внутренних и внешних угроз» (Бачило, И.Л. Информационное право: учебник / И.Л. Бачило. – М.: Издательство Юрайт; 2011. – 2-е изд., перераб. и доп. – С. 452).

теоретический тренд, согласно которому информационная безопасность — это состояние защищенности информационных интересов от воздействия угроз. Придерживаясь в целом существующего доминирующего подхода, считаем необходимым акцентировать несколько концептуальных позиций в определении исследуемого понятия.

Уяснению содержания понятия «информационная безопасность» способствует его декомпозиция по составляющим: предмету и цели, что позволяет рассмотреть каждый из элементов. Элемент «информационная» характеризует исследуемый феномен как относящийся к информационной сфере. Элемент «безопасность» обеспечивает качественную характеристику состояния общественных отношений, определяющую, что отсутствует (или не оказывает влияния) недекларированное внешнее деструктивное воздействие на их развитие. Возможны разные пути достижения данного состояния:

- ✓ **«угрозоустойчивость» отношений** – т.е. их свойство не подвергаться изменениям при воздействии на них угроз (иммунитет);
- ✓ **«угрозозащищенность»** (достигается посредством создания отдельной подсистемы, предупреждающей, выявляющей и пресекающей деструктивное воздействие угроз на «базовые» социальные отношения);
- ✓ **«неуязвимость»** – развитие в условиях априорной несопрягаемости со средой реализации угроз.

В целях определения содержания понятия «информационная безопасность» целесообразно также обратиться к результатам феноменологического исследования данного явления. Феномен «информационная безопасность» представляет собой качественную характеристику отношений в информационной сфере, заключающих в себе парадигму развития и содержащих свойство устойчивости к воздействию угроз[41]. Сущность феномена формируют характеризующие признаки:

- информационная безопасность является характеристикой защищенности определенной совокупности прав и интересов субъектов отношений;
- субъектами отношений выступают личность, общество и государство;
- объектами защиты являются права и интересы субъектов;
- указанные права и интересы возникают по поводу информации;
- рассматриваемые права и интересы объективно подвергаются деструктивному воздействию со стороны определенных факторов (угроз), среди которых доминирующими являются информационный терроризм, информационная преступность, применение информационного оружия, посягательства на безопасность информации;

«…сложное явление, включающее объект безопасности, образуемый совокупностью информационных потребностей государства и его деятельности по удовлетворению этих потребностей, угроз объекту безопасности, деятельности государства по противодействию угрозам, а также субъектов этого противодействия» (Стрельцов, А.А. Содержание понятия «обеспечение информационной безопасности» / А.А. Стрельцов // Информационное общество. – 2001. – Вып. 4. – С. 46–52).

«…состояние защищенности национальных интересов Российской Федерации в информационной сфере, состоящих из совокупности сбалансированных интересов личности, общества и государства, от внутренних и внешних угроз» (Полякова, Т.А. Правовое обеспечение информационной безопасности при построении информационного общества в России: дис. … д-ра юрид. наук: 12.00.14 / Т.А. Полякова. – М., 2008. – С. 117).

[41] Парадигма развития проявляется в гарантированной реализации субъектами информационных отношений своих интересов, что позволяет рассматривать информационную безопасность как безопасность динамической системы. По мнению Р.А. Юсупова основной характеристикой безопасности динамической системы является устойчивость ее развития (Юсупов Р.М. Наука и национальная безопасность / Р.М. Юсупов. – СПб.: Наука, 2011. – 2-е издание, переработанное и дополненное. – С. 278–279).

- 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 ни какие внешние и внутренние факторы.

Исходя из подхода к информационной безопасности как к интегрированной категории, объединяющей несколько измерений безопасности, в целях реализации совокупности интересов субъектов отношений,акцент делается на такую особенность рассматриваемого феномена, что в случае, если хотя бы один или несколько из совокупности информационных интересов субъекта не обеспечены защитой и не могут быть реализованы, то даже при условии достаточной защищенности остальных прав и интересов, «информационная безопасность субъекта» как явление не возникает.

В связи с тем, что феноменологическая сущность информационной безопасности представлена как свобода реализации информационных интересов в условиях активности угроз, содержание информационной безопасности можно определить как сбалансированное состояние симметричной защищенности информационных интересов акторов информационного взаимодействия от деструктивного воздействия внешних и внутренних информационных угроз, гарантирующее устойчивое развитие информационных отношений.

Изложенная теоретическая основа авторского подхода к дефиниции и содержанию информационной безопасности позволяет подойти к пониманию правовой сущности данного феномена. Так, например, в учебнике по информационному праву профессора И.Л. Бачило информационная безопасность определяется как «состояние всех компонентов ИКТ – информационных ресурсов, технологий и коммуникаций – позволяющее осуществлять их формирование и использование в интересах общества, государства и человека при минимизации отрицательных последствий для создателей, держателей и пользователей этих ресурсов, возникающих под влиянием внутренних и внешних угроз»[42].

Информационная безопасность представляется состоянием социума, позволяющим достигать консенсуса субъектов правоотношений (человека, общества и государства) в естественном многообразии их прав и интересов на определенном этапе общественного развития. Это многообразие и существующая пока степень неопределенности интересов субъектов (даже в рамках одного государства, а тем более в рамках ассоциаций государств) определяет сложность правового регулирования статуса и взаимодействия конкретных субъектов между собой в разных областях жизнедеятельности общества.

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. Информационная безопасность отношений субъектов возникает и существует при условии, что совокупность реализуемых ими прав находится в определенной степени регулирования

---

[42] Бачило, И.Л. Информационное право. Учебник 3-е издание./ И.Л. Бачило. - М.: Издательство Юрайт. 2013. – С 485.

в национальном законодательстве. Таким образом, синтез разных вариантов определения и анализ сущности этого феномена позволяет рассматривать информационную безопасность как отвечающее сбалансированным интересам личности, общества и государства состояние информационных технологий, информационных ресурсов, информационной среды в целом, позволяющее сохранять гарантированную устойчивость заданных параметров инфокоммуникационной системы и отношений информационного взаимодействия ее пользователей.

Информационная безопасность может быть определена как состояние информационных ресурсов, технологий и коммуникаций, позволяющее формировать их создание, комплексирование и использование в процессе функционального (целенаправленного) применения в интересах государства, общества и человека в информационном пространстве каждого государства, межгосударственных образований, а также в пространстве инфокоммуникаций сети Интернет.

Содержание, обычно вкладываемое в понятие «информационная безопасность» на практике, зачастую сужает его понимание до технических аспектов защиты информации, при этом опускаются, прежде всего, её социально-гуманитарные аспекты межличностной коммуникации. Нормативное регулирование в таком случае становится, по сути, техническим и направленно преимущественно на стандартизацию технологических процессов, удаляясь от нормативного обеспечения общественных отношений. В силу изложенного в последнее время стала заметна практика использования более ёмкого понятия *«информационно-коммуникационная безопасность»,* что акцентирует контекстную составляющую защищаемых интересов.

К формулировке «информационно-коммуникационная безопасность» апеллирует Программа деятельности Парламентской Ассамблеи Организации Договора о коллективной безопасности на 2011–2015 гг., включившая в свои планы разработку Рекомендаций по сближению и гармонизации национального законодательства государств – членов ОДКБ в сфере обеспечения информационно-коммуникационной безопасности. В процессе подготовки названных Рекомендаций одним из ключевых вопросов стало определение предметного поля сближения и гармонизации законодательства и, соответственно, уточнение содержательного наполнения понятия «информационно-коммуникационная безопасность».

Легитимного понятия «информационно-коммуникационная безопасность» в правовом поле СНГ и ОДКБ до настоящего времени выработано не было. В русскоязычном международно-правовом поле встречается понятие «информационная и коммуникационная безопасность», использующееся в трактовке: «состояние защищенности личности, общества, государства и их интересов от существующих и потенциальных угроз в сфере информационных и коммуникационных средств и технологий, включая меры, направленные на обеспечение доступности, целостности, конфиденциальности и подлинности информации». Это понятие использовано в тексте Соглашения между Правительствами Российской Федерации и Федеративной Республики Бразилии о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности (2010).

Следует отметить, что приведённое выше понятие «информационная и коммуникационная безопасность» трактуется шире предложенного Комиссией Евросоюза (2001) англоязычного понятия «сетевая и информационная безопасность» (Network and Information Security), которое было определено как «*способность сети или информационной системы противостоять при заданном уровне надежности случайным угрозам или умышленным вредоносным действиям, которые подвергают*

риску доступность, подлинность, целостность и конфиденциальность хранимых или передаваемых данных и связанных с ними служб, доступ к которым осуществляется с помощью таких сетей или систем»[43].

В качестве основных угроз в области обеспечения международной информационной и коммуникационной безопасности в российско-бразильском Соглашении перечислены следующие:

1) использование информационных и коммуникационных средств и технологий в международных конфликтах во враждебных целях, как в гражданской, так и в военной сферах, включая выведение из строя критически важных инфраструктур;

2) использование информационных и коммуникационных средств и технологий для осуществления террористической деятельности и в террористических целях;

3) использование информационных и коммуникационных средств и технологий для осуществления преступной деятельности и в преступных целях;

4) использование доминирующего положения в сфере информационных и коммуникационных средств и технологий в ущерб интересам и безопасности других государств;

5) стихийные бедствия и технологические аварии, влияющие на безопасное и стабильное функционирование глобальных и национальных информационных и коммуникационных инфраструктур.

При всех достоинствах, как видно из приведенных выше в трактовке российско-бразильского Соглашения определений понятия и перечня угроз информационной и коммуникационной безопасности, они не охватывают становящиеся все более актуальными сегодня угрозы, затрагивающие различные чувствительные сферы жизнедеятельности общества, в частности, связанные с возможным деструктивным использованием Интернет технологий в целях осуществления негативных форм социального взаимодействия, представляющие общественную опасность[44].

На основании проведённого анализа современных угроз в информационной сфере, исходя из компетенции и уставных задач ОДКБ и акцентируясь на контекстной составляющей обеспечения информационной безопасности, предлагается рассматривать *«информационно-коммуникационную безопасность государств – членов ОДКБ» как состояние информационного пространства ОДКБ, при котором исключены возможности нарушения прав личности, общества и интересов государств – членов Организации Договора о коллективной безопасности в информационной сфере, а также деструктивного и противоправного воздействия на элементы совместной информационной инфраструктуры ОДКБ и национальных критических информационных инфраструктур государств – членов ОДКБ.*

2.3. Понятие и сущность обеспечения информационной безопасности

В целях определения содержательной трактовки понятия «обеспечение информационной безопасности» необходимо обратиться к родовому понятию

---

[43] Communication from the Commission to the Council, the European parliament, the European Economic and Social Committee and the Committee of the Regions «Network and Information Security: Proposal for A European Policy Approach». Brussels, 6.6.2001. COM (2001)298 final.

[44] Смирнов, А.А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза: монография / А.А. Смирнов. – М.: ЮНИТИ-ДАНА: Закон и право, 2012. – 159 с.

«обеспечение национальной безопасности», толкование которого представлено в научной литературе[45].

Исследование теоретических основ обеспечения национальной безопасности позволяет выделить характеризующие признаки данной деятельности: это деятельность адаптивной системы[46], сущность которой заключается в том, чтобы, с одной стороны, идентифицировать основные интересы объектов защиты и не препятствовать их развитию, с другой стороны, определить угрозы защищаемой системе, спрогнозировать их возможное деструктивное воздействие и, в конечном итоге, упреждающе выстроить систему мер несопряжения интересов и угроз с учетом векторов их развития.

Названная характеристика вполне применима для определения понятия «обеспечение информационной безопасности».

Ведущими исследователями информационного права определены подходы к изучению сущности обеспечения информационной безопасности[47].

---

[45] «Под обеспечением безопасности нужно понимать комплексную деятельность Российского государства по достижению урегулированного правом состояния защищенности конституционных и иных законных интересов личности, общества, государства и нации, которая охватывает такие направления воздействия, как предупреждение, выявление и нейтрализация угроз безопасности, или иначе предупреждение, выявление и нейтрализация вредоносных природных и техногенных факторов окружающей среды, связанных с санкционированным и контролируемым государством правомерным использованием субъектами права предметов, явлений и процессов — природных и техногенных источников опасности конституционным и иным законным интересам личности, общества, государства, нации, а также предупреждение выявление и нейтрализация правонарушений и юридических казусов, способствующих возникновению и развитию данных факторов» (Стахов, А.И. Административно-публичное обеспечение безопасности Российской Федерации: монография / А.И. Стахов. – М.: ЮНИТИ-Дана. Закон и право, 2006. – С. 63).

«Под обеспечением национальной безопасности Российской Федерации понимается целенаправленная деятельность государственных и общественных институтов, а также граждан по выявлению, предупреждению угроз безопасности личности, общества и государства и противодействию им в качестве обязательного и непременного условия защиты национальных интересов России» (Общая теория национальной безопасности: учебник / А.А. Прохожев [и др.]; под общ. ред. А.А. Прохожева. – М.: Изд-во РАГС, 2005. – Изд. 2. – С. 110).

[46] «Адаптивная система – система, которая в процессе эволюции и функционирования демонстрирует способность к целенаправленному приспосабливающемуся поведению в сложных средах. Адаптивная система может приспосабливаться к изменениям как внутренних, так и внешних условий» (Деревицкий, Д.П. Прикладная теория дискретных адаптивных систем управления./ Д.П., Деревицкий, А.Л. Фрадков.– М.: Наука, 1981. – 216 с).

[47] Для рассмотрения понятия «обеспечение информационной безопасности» Стрельцов А.А. проводит фразеологический анализ его составляющих, в результате чего «обеспечение» понимается им как совокупность материальных и духовных объектов, финансовых, правовых и организационных средств, которые повышают эффективность деятельности по достижению целей; «информационной» рассматривается как предметная сфера обеспечения как вида деятельности; «безопасность» — как невозможность нанесения вреда кому-нибудь или чему-нибудь вследствие проявления угроз, т.е. их защищенность от угроз. Исходя из изложенного, содержание понятия «обеспечение информационной безопасности» заключается: «…в создании условий, при которых нанесение вреда зависящим от информации свойствам или составляющим объекта безопасности невозможно. Создание этих условий осуществляется субъектами обеспечения информационной безопасности посредством целенаправленной деятельности по противодействию угрозам нанесения вреда зависящим от информации свойствам или составляющим объекта безопасности, выполняемой с использованием средств обеспечения информационной безопасности» (Стрельцов, А.А. Теоретические и методологические основы правового обеспечения информационной безопасности: дис. … д-ра юрид. наук: 05.13.19 / А.А. Стрельцов. – М., 2004. – С. 67). «Обеспечение информационной безопасности есть совокупность деятельности по недопущению вреда свойствам объекта безопасности, обусловливаемым информацией и информационной инфраструктурой, а также средств и субъектов этой деятельности» (Там же. – С. 32).

Исследуя понятие «обеспечение безопасности», Н.Н. Куняев также дает толкование каждой составляющей данного словосочетания. В структуре понятия «обеспечение» он выделяет характеризующие элементы: «деятельность по обеспечению (оказание помощи субъектам в достижении поставленных ими целей); средства обеспечения (совокупность материальных, духовных, финансовых, правовых, организационных и технических средств осуществления деятельности по обеспечению); субъекты обеспечения (индивиды, организации, органы государства, осуществляющие деятельность по обеспечению)» (Куняев, Н.Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере: дис. … д-ра юрид. наук: 12.00.14 / Н.Н. Куняев. – М., 2010. – С. 134).

В доктринальных документах СНГ обеспечение информационной безопасности государств – участников СНГтрактуется как «*система мер правового, организационно-технического и организационно-экономического характера по выявлению угроз информационной безопасности, предотвращению их реализации, пресечению и ликвидации последствий реализации таких угроз*»[48].

Обобщение определяющих сущность обеспечения информационной безопасности подходов сквозь призму избранной методологии позволяет осуществить их систематизацию[49].

Первый подход исходит из объективного понимания информационной безопасности как проявления сущностной природы информации сохранять устойчивость своих свойств при различных отрицательных воздействиях (функция саморегулирования). В этом контексте под обеспечением информационной безопасности понимается обеспечение устойчивого развития базовых институтов. Данный подход можно назвать «иммунным», предполагающим в качестве основного метода реализации моделирование адаптивности субъекта к изменениям окружающей среды. В этом смысле обеспечение информационной безопасности — это «*постоянно действующий комплекс правовых, организационных, технологических и технических служб и условий, создающих безопасное функционирование всех средств информационной инфраструктуры и взаимодействия информационных систем органов государственной власти, местного самоуправления, структур гражданского общества, экономики, а реализацию прав граждан в информационном пространстве государства и в глобальных информационных системах, включая Интернет*»[50].

Второй подход основывается на признании субъектного характера обеспечения информационной безопасности. В данном случае обеспечение информационной безопасности направлено на создание барьера между интересами и угрозами интересам конкретных субъектов отношений. Субъектное понимание информационной безопасности составляет основу деятельностных, ценностных (аксиологических) и других ее определений, как производной от национальных интересов. Названный подход можно назвать «оборонительным». Основным методом обеспечения информационной безопасности в указанном случае представляется режимный метод[51], обеспечивающий построение системы регламентов поведения субъектов отношений.

Третий подход основывается на определении обеспечения информационной безопасности как деятельности по устранению возникающих угроз на разных стадиях их

---

[48] Концепция сотрудничества государств – участников Содружества Независимых Государств в сфере обеспечения информационной безопасности: решение Совета глав государств Содружества Независимых Государств, 10 октября 2008 // Содружество. Информационный вестник Совета глав государств и Совета глав правительств СНГ. – 2008. – № 2(32). – С. 106–113.

[49] Авторскую градацию стратегических подходов обеспечения информационной безопасности предлагает Фатьянов А.А.: «современная теория защиты информации выделяет три уровня стратегии защиты информации в зависимости от угроз: оборонительная — от наиболее опасных угроз, наступательная — от всех известных угроз, упреждающая — от всех потенциально возможных угроз. Система защиты государственной тайны как по уровню оснащенности, так и по структурному построению должна обеспечивать уровень безопасности информации, адекватный упреждающему уровню. Конечно, это достаточно дорого и весьма сложно, но необходимо» (Фатьянов, А.А. Правовое обеспечение безопасности информации в Российской Федерации: учебное пособие / А.А. Фатьянов. – М., Издательская группа «Юрист», 2001. – С. 364).

[50] Бачило, И.Л. Информационное право. Учебник для магистров 3-е изд. / И.Л. Бачило. - М.: ЮРАЙТ, 2912. С. 485-488.

[51] Кузнецов П.У. предлагает «…двухуровневый (конъюнктивно-интегративный и высокотехнологичный) режимный метод правового обеспечения информационной безопасности» (Кузнецов, П.У. Теоретические основания информационного права: дис. … д-ра юрид. наук: 12.00.14 / П.У. Кузнецов. – Екатеринбург, 2006. – С. 14).

зарождения и развития. Здесь обеспечение информационной безопасности направлено на выявление и нейтрализацию угроз и их источников и может рассматриваться как «наступательная» деятельность. Стержневыми методами обеспечения информационной безопасности рассматриваются аналитико-прогностические и пресекательно-профилактические. В рамках данного подхода информационная безопасность обеспечивается выделенной целевой подсистемой.

Четвертым подходом можно считать определение обеспечения информационной безопасности как создания таких условий, при которых угрозы вовсе не воздействуют на защищаемые интересы. Такое сомнительное в плане выполнимости для социальных отношений условие, тем не менее, позволяет рассматривать в аспекте информационной безопасности и это определение наравне с другими, ввиду технической и технологической обусловленности данной сферы общественных отношений. Действительно, в настоящее время не вызывает сомнения возможность переноса отношений в искусственную, технологически обусловленную среду. Следовательно, данная среда может быть проектирована как опережающе недоступная для воздействия угроз.

Как видим, три из четырех названных подходов предполагают обеспечение информационной безопасности как результат взаимодействия двух систем: «защищаемой» и «защищающей»[52].

По нашему мнению, в случае формирования системы информационной безопасности в условиях активно неблагоприятной среды, воздействия угроз и вызовов информационной безопасности система обеспечения информационной безопасности может строиться исключительно как выделенная, обеспечивающая, с обособленными от «базовых процессов» функциями безопасности.

Изложенное позволяет сделать вывод, что обеспечение международной информационной безопасности государств – участников СНГ и государств – членов ОДКБ на современном этапе базируется на концептуальном подходе рассмотрения сущности данного явления как активной деятельности выделенной социальной подсистемы безопасности по выявлению и нейтрализации угроз.

Таким образом, *обеспечение международной информационной безопасности на пространстве СНГ (и ОДКБ) можно рассматривать, как деятельность государственных органов и организаций по поддержанию состояния безопасности личности, общества и государства в информационном пространстве при создании и использовании информационных, коммуникационных технологий (и средств их применения) и информационных ресурсов в целях стабильного безопасного*

---

[52] Точку зрения о существовании двух систем в сфере обеспечения информационной безопасности (базовой – иммунной и надстроечной — обеспечивающей) развивает Юсупов Р.М., обосновывающий вывод, что «…безопасность не всегда обеспечивается только защитой. Она также может быть достигнута соответствующими правилами поведения и взаимодействия субъектов, высокой профессиональной подготовкой персонала, безукоризненной работой техники…» (Юсупов, Р.М. Наука и национальная безопасность / Р.М. Юсупов. – СПб.: Наука, 2011. – 2-е издание, переработанное и дополненное. – С. 117).

Кузнецов П.У. также заостряет проблему «сосуществования» двух систем информационных отношений, называя их «естественная (система самоорганизации)» и «искусственная» (система безопасности)», призывает к их синергетичности. Для определения и понимания пути решения проблем обеспечения безопасного состояния информационной сферы П.У. Кузнецов предлагает обратиться к «… методологии систем, комплексной науке, изучающей влияние различных факторов на ее состояние, прежде всего, таких, как сложность, устойчивость, целостность и стабильность» (Кузнецов, П.У. Теоретические основания информационного права: дис. … д-ра юрид. наук: 12.00.14 / П.У. Кузнецов. – Екатеринбург, 2006. – С. 308–309). При этом Кузнецов П.У. в качестве важнейшей характеристики системы с точки зрения безопасности выделяет «…устойчивость и определяет ее как способность отражать действие угроз» (Там же. – С. 309).

функционирования и развития всех социальных и государственных институтов и механизмов.

Результатом обеспечения международной информационной безопасности является непрерывно действующие комплексы правовых, организационных, технологических и технических мер и служб, создающих условия безопасного функционирования всей информационной инфраструктуры, государственного управления, а также средств ИКТ, которыми пользуются граждане и другие субъекты гражданского общества и структуры, обеспечивающие информационное взаимодействие этих государств между собой.

Из названных подсистем обеспечения информационной безопасности особое место занимает категория «правовое обеспечение информационной безопасности», уяснение сущности которой возможно посредством выделения уникального набора ее идентификационных признаков, каковыми являются:

- учет состояния защищенности определенной совокупности прав и интересов субъектов отношений (в соответствии с международными нормами и национальным законодательством) от деструктивного воздействия определенных факторов (угроз);
- задача одновременного обеспечения заданного уровня безопасности всех взаимодействующих субъектов при соблюдении их прав и интересов. На этой основе создание динамично развивающейся системы правового регулирования процессов информатизации, что требует правовых решений в области использования информационных ресурсов, информационных технологий, информационной инфраструктуры и информационной среды в целом (в том числе, в условиях воздействия на них внутренних и внешних угроз);
- создание таких условий, при которых на заданный вектор и темп развития информационных отношений не оказывают существенного деструктивного влияния внешние и внутренние факторы. Именно в этом состоит основная задача обеспечения информационной безопасности.

В науке сформирована доминирующая концепция системно-структурного построения обеспечения информационной безопасности, позволяющая определить ее категориальное содержание: права и интересы субъектов отношений — угрозы реализации выделенных интересов — меры противодействия угрозам — обеспечения безопасности интересов. Правовое обеспечение информационной безопасности, реализуемое в системе правовых актов (включающих и модельное законодательство), призвано переводить систему отношений из теоретической в практическую плоскость.

Важнейшей в системе правового обеспечения информационной безопасности является подсистема выявления угроз, выступающих в качестве противовеса состоянию безопасности. В этой связи в системе правового обеспечения необходимо установить механизмы отслеживания процессов нарастания конфликтов и угроз, обеспечивая систему мониторинга динамики состояния безопасности общества, государства, человека. При этом следует принимать во внимание, что реализация угроз информационного характера проявляется в самых разных сферах жизнедеятельности (экономика, социальная сфера, производство, рынок и т.д.) и опосредованно влияет на национальную безопасность в политической, экономической и иных сферах.

Правовое регулирование обеспечения информационной безопасности опосредует архитектуру системы задач информационной безопасности: интересы субъектов — виды угроз — индикаторы оценки угроз — способы противодействия и сдерживания их реализации — отслеживание форм реализуемых угроз — виды и меры ответственности

субъектов, действующих в зоне правонарушений и преступлений в системе информационной безопасности. Институт угроз является теоретической социально-политической конструкцией. В правовом поле реальные угрозы представлены в форме составов правонарушений и преступлений.

Публично-правовая сущность информационной безопасности[53] выделяет в качестве регулятора складывающихся в связи с ее обеспечением отношений государство. Следовательно, в целях обеспечения информационной безопасности (как комплексного социально-правового явления) государство выстраивает политику развития информационного общества, стратегию информационной безопасности и формирует соответствующую правовую основу обеспечения информационной безопасности.

Таким образом, *правовое обеспечение информационной безопасности представляется как разработка и применение правовых средств и механизмов правовой системы государства в области организации охраны и защиты инфокоммуникационных и информационных ресурсов в целях поддержания их свойств в состоянии гарантированной устойчивости и соблюдения законности информационного взаимодействия субъектов в процессе решения задач безопасности развития государства, общества, создания условий реализации прав и интересов личности, защиты интересов государства в рамках международного сотрудничества.*

2.4. Базовые правовые категории в сфере обеспечения международной информационной безопасности на пространстве СНГ и ОДКБ

В процессе многолетней работы над проблемами научно-правового обеспечения информационной безопасности российско-белорусским коллективом учёных была выработана определенная совокупность терминов и трактовок их определений, отражающая авторский взгляд на разрабатываемые проблемы. Не все из названных терминов в дальнейшем были предложены для нормативного толкования, однако они, как видится, представляют исследовательский интерес и помогают сориентироваться в научных истоках изложенных на страницах данной работы подходов к решению проблем обеспечения информационной безопасности:

- ***информационное пространство межгосударственного взаимодействия*** (в данном случае, СНГ и ОДКБ) — информационное пространство каждой геополитической единицы — государства и образуемого единого информационного пространства обмена информационными ресурсами, создания и размещения комплексных интегрированных информационных ресурсов по целям сотрудничества;

---

[53] В оценке состояния правового обеспечения информационной безопасности выявляется проблема соотношений механизмов публичного и гражданского права. Часто, и особенно это заметно на области санкций за административные правонарушения, где мера наказания касается возмещения вреда, нанесенного пострадавшему субъекту. В то время как значимость нарушений прав человека или иного субъекта в публично-правовом аспекте уходит в тень. С другой стороны, наблюдаем и некоторую узурпацию гражданского права и законодательства относительно публично значимых и используемых объектов. Например, регулирование статуса и природы информационных систем, баз и банков данных, причисление провайдеров системы Интернет к посредникам в чисто имущественных гражданско-правовых отношениях. Нарушение авторских прав в Интернет-среде при их квалификации сужается до защиты права интеллектуальной собственности по ГК, но не учитывает значимости этих правонарушений в системе публичного интереса и собственно прав автора на свое произведение в условиях глобального информационного пространства. Все это существенно отражается на решении проблемы идентификации субъектов, выступающих в роли нарушителей информационной безопасности (авт.).

- ***информационная инфраструктура*** — сложная система, позволяющая структурировать используемый и создаваемый ресурс в области информационных, коммуникационных технологий и других средств информатизации, имеющая определенное научное, экономическое, организационное, материальное, кадровое, правовое обеспечение, необходимое для реализации целей информатизации;
- ***информационные ресурсы*** — выделяемая и используемая совокупность знаний, сведений и иных форм представления доступной информации субъектом в соответствии с его интересами и структурируемая им по определенным критериям (хронологии, видам, формам обработки, коммуникаций и др.), включая создаваемую, приобретаемую и используемую информацию по сфере его деятельности в соответствии с действующим законодательством;
- ***защита информации*** — деятельность, направленная на предотвращение утечки, неправомерного доступа и использования информации (сведений, данных), предотвращающая несанкционированные и непреднамеренные вредные воздействий на конкретные информационные объекты;
- ***информатизация*** — процесс создания и использования ИКТ, информационных ресурсов и информационных систем, организуемый в целях формирования информационного общества и удовлетворения потребностей общества, государства, человека;
- ***информационная система*** — имущественный комплекс, используемый для сбора, накопления, хранения, поиска и получения, обработки, передачи и распространения информации, который включает как программное обеспечение, необходимое технически-технологическое оборудование, так и информационный ресурс определенного субъекта;
- ***государственные информационные ресурсы*** — совокупность знаний, сведений и иных форм доступной информации, находящейся в ведении и распоряжении органов государственной власти и органов местного самоуправления, а также других органов и организаций и граждан, взаимодействующих с государственными органами и между собой по проблемам реализации их прав и обязанностей, при соблюдении правового режима этих ресурсов, устанавливаемого в соответствии с национальным и международным законодательством;
- ***государственная политика обеспечения информационной безопасности*** — деятельность государства по определению содержания (форм, средств, задач, субъектов, функций и др.) обеспечения информационной безопасности;
- ***деструктивное информационное воздействие*** — осуществление информационного влияния на политические и социально-экономические процессы происходящие в государстве, на государственные органы этих государств, а также на физических и юридических лиц в целях ослабления обороноспособности государства, нарушения общественной безопасности, принятия заведомо невыгодных решений, заключения заведомо невыгодных международных договоров, ухудшения отношений с другими государствами, создания социально-политической напряженности внутри государства, формирования угрозы возникновения чрезвычайных ситуаций, разрушения традиционных духовных и нравственных ценностей, создания препятствий для нормальной деятельности государственных органов, а также причинения иного ущерба национальной безопасности;

- ***информационный источник угрозы национальной безопасности*** — фактор или совокупность факторов, способных при определенных условиях привести к возникновению угрозы национальной безопасности;
- ***информационный суверенитет*** — правовой статус, обеспечивающий способность государства самостоятельно осуществлять функции государства в информационной сфере с целью соблюдения прав и свобод граждан, обеспечения национальной безопасности;
- ***национальные интересы в информационной сфере*** — совокупность потребностей государства по реализации сбалансированных интересов личности, общества и государства в информационной сфере;
- ***информационная угроза национальной безопасности*** — потенциальная или реально существующая возможность нанесения ущерба национальным интересам;
- ***критически важный объект информатизации*** — объект информатизации, который обеспечивает функционирование экологически опасных и (или) социально значимых производств и (или) технологических процессов, нарушение штатного режима которых может привести к чрезвычайной ситуации техногенного характера; осуществляет функции информационной системы, нарушение (прекращение) функционирования которой может привести к значительным негативным последствиям для национальной безопасности в политической, экономической, социальной, информационной, экологической, иных сферах; обеспечивает 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;
- ***правовой статус субъекта правоотношений в области информационной безопасности*** — интегрированная совокупность нормативно закрепленных прав и обязанностей субъекта во всех видах информационных отношений;
- ***информационный инцидент*** — событие, нарушающее основные права и интересы субъектов информационных отношений.

* * *

ГЛАВА 3. КОМПЛЕКСНЫЙ ПОДХОД К ПРАВОВОМУ ОБЕСПЕЧЕНИЮ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Вектор правового регулирования обеспечения международной информационной безопасности на пространстве СНГ и ОДКБ в современный период

В науке информационного права правовое обеспечение информационной безопасности понимается широко, с учетом всего диапазона общественных отношений, формирующихся и реализуемых в процессе развития информационного общества. Регулирование отношений в области обеспечения информационной безопасности охватывает формирование и использование информационных технологий, коммуникаций и все формы работы с информацией, затрагивающие права и интересы человека, общества и государства. Комплексный институт правового регулирования обеспечения информационной безопасности образуется совокупностью норм информационного, конституционного, гражданского, административного и уголовного права, регулирующих отношения в области противодействия угрозам безопасности объектов национальных интересов в информационной сфере. В результате сегодня имеет место большой массив различных законодательных и иных правовых актов, относящихся к сфере информационной безопасности и разброс отдельных правовых норм по отраслям законодательства[54].

В государствах – участниках СНГ и государствах – членах ОДКБ за последние 20 лет сформирована законодательная основа регулирования информационных отношений, предназначенная для опосредования отношений в области как внутреннего развития информационных ресурсов и технологий, так и их использования во всех сферах жизнедеятельности общества. Однако нарастающий разрыв в темпах энергоемкости технологической структуры информатизации и усвоении потенциала ИКТ в управлении делами общества и государства, в реализации прав человека и его включенности в этот процесс преодолевается национальными правовыми системами с большим трудом и издержками. Многогранность отношений информатизации и обеспечения безопасности информационной сферы ведут к наращиванию числа законов и других нормативных правовых актов. При этом их взаимодействие плохо обеспечивается, ибо каждый новый закон требует поправок и изменений в уже действующие. Создается цепочка работы правовой системы и законодательства фактически самой на себя с очень малым коэффициентом полезного влияния на реальные отношения социальных акторов.

Схожим является состояние современного модельного информационного законодательства. Существует слабая согласованность в вопросах регулирования

---

[54] В ходе работы по систематизации законодательства при подготовке концепции Информационного кодекса специалисты ИГП РАН предложили новый подход к структуризации институтов информационного права. Вопросы информационной безопасности в этой концепции определены как суперинститут информационной безопасности, который имеет свою внутреннюю структуру в форме институтов и субинститутов. Работа по применению такого подхода к деятельности органов государственной власти может быть представлена в структуре базовых групп функций органов исполнительной власти, развертывающихся в систему функций, подфункций и операций. (Концепция Информационного кодекса Российской Федерации / Под ред. И.Л. Бачило – М.: ИГП РАН – Изд-во «Канон+» РООИ «Реабилитация», 2014. – 192 с.)

обеспечения информационной безопасности между отдельными модельными законами об информации, о доступе к информации, о публичных услугах, о персональных данных и иных категориях информации ограниченного доступа, об использовании электронной подписи и т.д. Здесь возможен и нужен консолидирующий акт на основе согласования общей терминологии, методов регулирования отношений и удержания процесса в безопасном состоянии.

Проблема правового регулирования обеспечения международной информационной безопасности является одной из самых острых и актуальных в современном национальном и международном законотворчестве. К сожалению, сегодня еще нельзя констатировать достижение состояния урегулированности отношений по обеспечению информационной безопасности. Полученные в настоящее время результаты можно охарактеризовать как концептуальные, определяющие основы правового поведения, либо локальные, регулирующие уже сложившиеся отношения, как правило, сопровождающие очередной шаг информатизации общества. Целостного иерархически структурированного правового механизма регулирования обеспечения информационной безопасности в настоящий момент не существует.

В сложившейся ситуации возможны два подхода к правовому регулированию обеспечения информационной безопасности в интересах СНГ и ОДКБ.

Первый — продолжать «штопать» и обновлять действующие законы, и двигаться в уже сложившейся системе национального и модельного нормотворчества, о которой сказано выше. При этом варианте каждый закон выстраивает свой предмет регулирования, свои термины и их понятия, плохо взаимодействует с другими отраслевыми и комплексными нормами, что тормозит включение в практику реально идущих процессов и препятствует имплементации модельных конструкций в национальное законодательство.

Так, практика применения существовавшего с 2005 г. Модельного закона СНГ «Об информатизации, информации и защите информации» (а отчасти и пришедшего ему на смену в 2014 г. нового Модельного закона «Об информации, информатизации и обеспечении информационной безопасности») свидетельствует, что он только по идее является базовым. Но на сегодня этот базовый модельный закон и корреспондирующие ему не создают полноценной юридической базы для системного обеспечения международной информационной безопасности. Они слабо влияют на состояние информационной культуры общества и его основных векторов развития. Ни один существующий сегодня закон не смог решить вопросы наполнения Интернет-среды полезной информацией и снижения ее засорения информацией вредной. В то же время, базовый модельный закон призван обеспечить регулирование отношений в области формирования и использования информационных ресурсов, правил их обработки, компетенций провайдеров и других субъектов информационной среды, безопасности и ответственности за правонарушения в информационной сфере. Аналогичную картину демонстрирует пример слабого воздействия модельного законодательства СНГ на развитие национального законодательства в государствах – участниках Содружества. Сказанное можно также проиллюстрировать на практике обеспечения доступа к информации, предоставления публичных услуг, применения и безопасного сохранения персональных данных, состоянии социальной, идеологической, культурной сфер современного общества.

С позиций накопленного опыта становится всё более очевидным, что подход «методом штопки» сохраняет конкуренцию нормативных актов на национальном и международном уровнях, создаёт их коллизии, что не повышает информационную

защищенность личности, общества и государства и способствует формированию правового нигилизма в данной сфере.

Второй возможный подход к решению вопросов уплотнения и координации национального и модельного законодательного ресурса, повышения его действенности и эффективности в области правового обеспечения информационной безопасности предусматривает отход от штучного, фрагментарного творчества по каждому нормативному акту «самого по себе». Сложившаяся сегодня практика является следствием доминирующей отраслевой «самостоятельности» структур в системе управления, когда отсутствуют интеграционные системы целевого использования информационных ресурсов при наличии огромного количества структурных образований на всех этажах системы государственной власти и международного сотрудничества.

Анализ действующих национальных и модельных законов в области обеспечения информационной безопасности позволяет отдать приоритет второму подходу в решении обсуждаемой проблемы. Действенное совершенствование международного информационного права, а тем более, гармонизация национального законодательства в целях обеспечения международной информационной безопасности требуют учета таких объективных условий, как сопрягаемость концептуальных подходов и теоретических взглядов государств на вектор развития информационного права, цели и принципы обеспечения информационной безопасности, совместимость национальных правовых систем.

Естественному сближению, и особенно, гармонизации подлежат правовые системы, находящиеся на одном этапе своего развития (в противном случае, приходится говорить не о гармонизации, а о теоретико-методологической экспансии более развитой системы в отношении менее развитой, либо о концептуальном заимствовании существующих подходов менее развитой правовой системой у более развитой). Следовательно, как представляется, наиболее эффективному правовому регулированию международного информационного сотрудничества государств – участников СНГ (аналогично и государств – членов ОДКБ) в целях обеспечения информационной безопасности способствовала бы разработка некоего национального стандарта нормативно-правовой обеспеченности в данной области, состоящего из конечного количества заданных параметров, характеристик. Совокупная реализация таких заданных характеристик будет свидетельствовать о достижении удовлетворяющего современным потребностям регионального взаимодействия уровня правового обеспечения информационной безопасности в конкретном государстве. На соответствие такого рода стандарту и должна проводиться оценка национального законодательства государств – участников СНГ (государств – членов ОДКБ) в целях его последующего сближения и гармонизации.

Следует, однако, исходить из того объективного факта, что, как показало проведенное сравнительно-правовое исследование, имеющая место сегодня нормативная и теоретико-правовая обеспеченность информационной безопасности модельным законодательством и рекомендательными актами в СНГ и ОДКБ с отрывом опережает любую из национальных правовых систем союзнических государств. Одновременно было выявлено, что среди государств СНГ и ОДКБ отсутствует несомненный лидер в плане нормативно-правового закрепления отношений в сфере обеспечения информационной безопасности. Такое положение дел позволяет сделать вывод о том, что на современном этапе сближение и гармонизацию законодательства государств – участников СНГ (и государств – членов ОДКБ) в указанной сфере

представляется более целесообразным осуществлять не эталонным путем (пытаясь брать за основу наиболее эффективные механизмы правового регулирования одной из стран – участниц и адаптируя их для других государств), а методом правового моделирования — ставя задачу построить на основе сравнительно-правового анализа механизмов национального правового регулирования обеспечения информационной безопасности не имеющую в настоящее время практических аналогов правовую модельную конструкцию и предложить её для рассмотрения и согласования государствам СНГ и ОДКБ.

3.2. Обоснование системы обеспечения международной информационной безопасности

Анализ нормативной базы государств – участников СНГ и государств – членов ОДКБ, а также актов иных международных и межгосударственных образований, позволяет определить в качестве самостоятельных подсистем: обеспечение национальной информационной безопасноти и обеспечение международной информационной безопасности[55]. При этом соотношение указанных подсистем не может рассматриваться просто как разноуровневое, а их содержание имеет не только территориально-географические (масштабные), но и методологические различия. Соответственно следует различать основные национальные задачи обеспечения информационной безопасности и задачи международного взаимодействия по обеспечению информационной безопасности. На позициях такой дифференциации стоит российский законодатель, закрепивший «внутренние» задачи в Доктрине информационной безопасности России, а «внешние» в Основах государственной политики РФ в области международной информационной безопасности на период до 2020 года.

В Российской Федерации обеспечение международной информационной безопасности осуществляется посредством решения следующих задач[56]:

---

[55] Основными задачами сотрудничества государств-членов ОДКБ в сфере обеспечения информационной безопасности являются (Решение Совета коллективной безопасности Организации Договора о коллективной безопасности, 10 декабря 2010 г. // Документ не публиковался):
1) координация мероприятий по защите информационных ресурсов военного и гражданского назначения от противоправного воздействия;
2) координация мероприятий по противодействию противоправному воздействию на информационно-телекоммуникационное пространство государств-членов ОДКБ;
3) подготовка предложений по информационному взаимодействию и координация при их реализации в целях организации противодействия современным угрозам;
4) координация взаимодействия по распространению в информационном пространстве государств-членов ОДКБ объективной и достоверной информации относительно других членов Организации.
Задачами правового регулирования отношений в сфере обеспечения информационной безопасности государств – участников СНГ являются (Приняты 38 пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ, постановление № 38-20 от 23 ноября 2012 г.):
1) выработка наиболее эффективных правовых механизмов комплексного обеспечения информационной безопасности, укрепления законности и правопорядка;
2) совершенствование взаимодействия государств – участников СНГ по обеспечению информационной безопасности, реагирования на информационные вызовы и угрозы;
3) создание условий для равноправного участия государств – участников СНГ в мировых информационных отношениях.

[56] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года [Электронный ресурс]. — Режим доступа: http://www.scrf.gov.ru/documents/6/114.html. – Дата доступа: 22.09.2015.

- формирование системы международной информационной безопасности на двустороннем, многостороннем, региональном и глобальном уровнях;
- создание условий, обеспечивающих снижение риска использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;
- формирование механизмов международного сотрудничества в области противодействия угрозам использования информационных и коммуникационных технологий в террористических целях;
- создание условий для противодействия угрозам использования информационных и коммуникационных технологий в экстремистских целях, в том числе в целях вмешательства во внутренние дела суверенных государств;
- повышение эффективности международного сотрудничества в области противодействия преступности в сфере использования информационных и коммуникационных технологий;
- создание условий для обеспечения технологического суверенитета государств в области информационных и коммуникационных технологий и преодоления информационного неравенства между развитыми и развивающимися странами.

Обобщение научных подходов[57] и сравнительно-правовое исследование законодательства государств – участников СНГ позволяют выделить основные задачи обеспечения информационной безопасности на национальном уровне[58]. Это: информационное сопровождение государственной политики; защита информационной инфраструктуры; защита информационных ресурсов; пресечение преступлений против

---

[57] Т.А. Полякова к важнейшим задачам системы обеспечения информационной безопасности относит: совершенствование правового регулирования, включая более детальное урегулирование защиты информации; использование наиболее эффективных современных методов и способов защиты информации; совершенствование системы информационной безопасности; внедрение современных информационных технологий в управленческую и судебную деятельность; повышение надёжности и защищенности информации от противоправных посягательств; приоритетность российских информационных технологий, включая и программное обеспечение, инновации и применение нанотехнологий в информационной сфере (Полякова, Т.А. Правовое обеспечение информационной безопасности при построении информационного общества в России: дис. … д-ра юрид. наук: 12.00.14 / Т.А. Полякова. – М., 2008. – С. 158).

[58] Основные задачи обеспечения информационной безопасности Республики Беларусь сводятся к обеспечению реализации конституционных прав и свобод граждан в информационной сфере; обеспечению безопасности процессов информатизации, информационной инфраструктуры и информационных технологий, повышению эффективности использования национальной информационной инфраструктуры; проведению эффективной государственной информационной политики; пресечению преступлений в информационной сфере; обеспечению защиты государственных секретов и иных охраняемых сведений (Об утверждении Концепции национальной безопасности Республики Беларусь: Указ Президента Республики Беларусь, 09 ноября 2010 г., № 575 // Национальный реестр правовых актов Республики Беларусь. – 2010. – № 276. – 1/12080).

Для достижения цели обеспечения информационной безопасности Республики Казахстан предполагается постановка и решение следующего комплекса задач: развитие системы управления информационной безопасностью, позволяющей обеспечить защищенность национальной информационной инфраструктуры страны и единого национального информационного пространства; разработка и реализация единой государственной технической политики в сфере обеспечения информационной безопасности, в т. ч. развитие и укрепление национальной системы защиты информации; защита прав личности и интересов общества и государства в информационной сфере; развитие отечественного информационного пространства; совершенствование законодательства, регулирующего информационную сферу; обеспечение активного участия Республики Казахстан в процессах создания и использования глобальных информационных сетей и систем (международное сотрудничество) (Указ Президента Республики Казахстан, 14 ноября 2011 г., № 174 // Сведений об опубликовании документа нет).

информационной безопасности; обеспечение безопасности информационной среды от деструктивного информационного воздействия; защита прав и интересов субъектов отношений.

С учетом существующих различных подходов к трактовкам и практике обеспечения информационной безопасности российскими и белорусскими учёными сформулированы основные задачи государств – участников СНГ и государств – членов ОДКБ по обеспечению международной информационной безопасности. Они включают:

- построение системы международной информационной безопасности и налаживание в рамках ее эффективного взаимодействия;
- обеспечение информационной безопасности с учетом направлений основных угроз национальной безопасности: терроризм, экстремизм, преступность, посягательства на государственный суверенитет;
- преодоление «цифрового неравенства», равноправное участие в мировых информационных процессах.

Необходимо обратить внимание на то обстоятельство, что если на национальном уровне задачи обеспечения информационной безопасности направлены на общественное развитие, то на международном уровне обеспечение информационной безопасности касается этого аспекта только в ракурсе преодоления препятствий, формирующих отставание государств, а развитие «отдается на откуп» национальным системам. Система же международной информационной безопасности направлена в первую очередь на коллективное противодействие транснациональным угрозам, реализующимся в информационной сфере, то есть носит ярко выраженный «оборонительный» характер. Всё изложенное выше ещё раз подтверждает тезис о том, что национальные и международная системы обеспечения информационной безопасности имеют неоднородную направленность и дифференцируются по основным задачам её обеспечения.

Обеспечение международной информационной безопасности на пространстве ОДКБ и СНГ базируется на следующих основных принципах:

- ✓ рассмотрение деятельности по обеспечению международной информационной безопасности в рамках методологии обеспечения национальной безопасности (что предполагает введение методологической конструкции «*интересы — угрозы — меры*», а также подход, согласно которому обеспечение безопасности не может эффективно осуществляться в рамках самозащиты права только внутренней «иммунной» системой субъекта, а должно обеспечиваться специальной надстроечной системой);
- ✓ соблюдение баланса интересов личности общества и государства в информационной сфере;
- ✓ учет современного состояния, динамики информационной сферы и приоритетных направлений ее развития.

Специальным принципом правового регулирования обеспечения информационной безопасности является принцип «безопасность через развитие», определяющий в качестве основного условия обеспечения информационной безопасности устойчивую динамику развития информационных средств реализации сбалансированных интересов личности, общества и государства[59].

[59] Обоснованность и актуальность рассмотрения данного принципа подтверждается его применением в Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента РФ от 31.12.2015 № 683.

Современное обеспечение международной информационной безопасности на пространстве ОДКБ и СНГ сопряжено с решением с ряда концептуальных проблем. К их числу относятся:

- диссонанс понятийного аппарата (основной теоретической проблемой является отсутствие сегодня единообразного понимания проблемы информационной безопасности; существуют подходы с технической, правоохранительной или гуманитарной доминантой[60]);
- недостаточность правовой базы, необходимой обеспечения информационной безопасности, в том числе нормативных правовых актов прямого действия;
- невыстроенность системы субъектов (сил) обеспечения информационной безопасности;
- несогласованность в определении приоритетных угроз информационной безопасности (имеют место, например, нормативно закрепленные позиции, определяющие, что приоритетными угрозами являются только посягательства на информацию и информационную инфраструктуру);
- отсутствие целеполагания обеспечения информационной безопасности (в то время как информационные отношения уже приобрели целенаправленность своего развития и закрепляются в различных стратегиях и планах, правовое регулирование отношений по обеспечению информационной безопасности не всегда носит концептуальный характер, не определяется, не градируется и не несет в себе индикаторов и показателей состояния информационной безопасности и динамики ее развития);
- невысокая динамика международного сотрудничества, дублирование международных институтов обеспечения информационной безопасности, недостаточно четкое разграничение полномочий между институтами.

Изложенное позволяет выделить следующие приоритетные направления деятельности по обеспечению международной информационной безопасности в формате СНГ и ОДКБ:

1) концептуальное определение на национальном уровне и в рамках межгосударственных образований интегрированного понятия «информационная безопасность», включающего в себя всю совокупность защищаемых прав и интересов личности, общества и государства в информационной сфере;

2) разработка методологии обеспечения информационной безопасности на основе теории национальной безопасности;

3) определение стратегических направлений обеспечения информационной безопасности (основной принцип на данном этапе: «обеспечение информационной безопасности не должно сдерживать развитие информационного общества, а должно способствовать его безопасному построению»);

4) формирование развитой системы субъектов обеспечения информационной безопасности на национальном и международном уровнях, повышение качества их взаимодействия;

---

[60] См. например, О типовых проектах законодательных актов МПА ЕврАзЭС в сфере информационных технологий: постановление Межпарламентской Ассамблеи Евразийского Экономического Сообщества от 28 мая 2004 г. № 5-20 («Об информатизации», «Об информационной безопасности», «Основные принципы электронной торговли») [Электронный ресурс]. — Режим доступа:
http://pravo.levonevsky.org/bazaby09/sbor35/text35341/index4.htm. – Дата доступа: 22.09.2015.

5) выработка правовых мер защиты прав, свобод и правомерных интересов субъектов информационных отношений, законодательное закрепление основных принципов и механизмов обеспечения информационной безопасности;

6) активизация на международном уровне процессов заключения соглашений об обеспечении информационной безопасности, унификация подходов к правовому регулированию обеспечения информационной безопасности, выработка согласованной теоретической, правовой и политической позиции по данной проблеме;

7) активное вовлечение общественности в обеспечение информационной безопасности. Формирование гражданской нетерпимости к проявлениям угроз информационной безопасности, выработка устойчивого социального (духовного, культурного) иммунитета к воздействию информационных угроз.

Информационная безопасность обеспечивается применением следующей системы организационных, правовых и технических мер:

- ✓ меры предупреждения возникновения угроз информационной безопасности, включающие профилактическое воздействие на субъектов информационных отношений, мониторинг угроз информационной безопасности, устранение причин и условий их возникновения;
- ✓ меры локализации угроз и пресечения правонарушений в информационной сфере;
- ✓ компенсационные и иные меры ликвидации последствий реализации угроз информационной безопасности.

К правовым мерам обеспечения информационной безопасности относятся:

1) разработка правовых механизмов регулирования отношений в информационной сфере;
2) определение статуса информации, информационных ресурсов и систем, оснований и порядка доступа к ним;
3) закрепление общеобязательных правил поведения в области обеспечения информационной безопасности, определение круга противоправных деяний, формирование перечня ограничений возможностей реализации информационных отношений в целях защиты прав и законных интересов субъектов взаимодействия; определение условий введения данных ограничений;
4) принятие и обнародование нормативных правовых актов, в том числе, устанавливающих ответственность за преступления против информационной безопасности;
5) определение статуса субъектов обеспечения информационной безопасности, законодательное разграничение их полномочий;
6) определение механизмов выявления и расследования правонарушений в информационной сфере, процедур привлечения к уголовной, административной и иным видам ответственности;
7) осуществление надзора и контроля за законностью деятельности граждан, организаций, государственных органов и должностных лиц в информационной сфере.

Организационные меры обеспечения информационной безопасности включают:

1) 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;

2) 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;

3) установление режимов информационной безопсности, в том числе режимов ограничения доступа к информации;

4) организация и совершенствование деятельности по защите государственных секретов, информации в государственных информационных системах, а также в информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено;

5) 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;

6) разработка программ обеспечения информационной безопасности, совершенствование системы финансирования работ, связанных с реализацией правовых, организационных и технических методов обеспечения информационной безопасности;

7) лицензирование деятельности, регистрации и стандартизация работ и услуг, сертификации товаров в области обеспечения информационной безопасности;

8) создание системы страхования информационных рисков физических и юридических лиц;

9) формирование системы мониторинга показателей и характеристик информационной безопасности в основных сферах жизнедеятельности государства;

10) развитие международного сотрудничества в сфере обеспечения защиты информации в международных телекоммуникационных системах и системах связи.

11) формирование системы информационного противоборства, противодействия информационной деятельности зарубежных государств, международных и иных организаций, отдельных лиц, наносящей ущерб интересам государства.

К техническим мерам обеспечения информационной безопасности относятся:

1) разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения»[61];

2) 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;

3) использование криптографических средств защиты информации, а также систем контроля доступа и регистрации фактов доступа к информационной системе;

---

[61] Добряков, С.А. Административно-правовые меры защиты служебной информации, используемой подразделениями ГИБДД в правоохранительной деятельности: дис. ... канд. юрид. наук: 12.00.14 / С.А. Добряков. – М., 2008. – С. 52.

4) 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;

5) 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 осуществляется посредством:

- определения общедоступной информации[62] и закрепления запрета на ограничения ее распространения;
- определения категорий охраняемой информации и введения запрета на ее распространение[63];
- 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 осуществляется посредством:

- установления требований к надежности и безопасности используемых в ней аппаратных и программных средств (их сертификации), проверки соответствия указанным требованиям;
- установления предписаний на обязательное использование отдельных средств и элементов информационной инфраструктуры;

---

[62] Общедоступную информацию могут составлять сведения:
- 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 состоянии преступности, а также о фактах нарушения законности;
- о чрезвычайных ситуациях, экологической, санитарно-эпидемиологической обстановке, гидрометеорологической и иной информации, отражающей состояние общественной безопасности;
- накапливаемые в открытых фондах библиотек и архивов, информационных системах государственных органов, физических и юридических лиц, созданных (предназначенных) для информационного обслуживания физических лиц.

[63] Охраняемую информацию составляют сведения, содержащие:
- тайну личной жизни лица;
- персональные данные гражданина;
- государственные секреты;
- служебную информацию ограниченного распространения (служебную тайну);
- коммерческую тайну;
- профессиональную тайну.

- 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 осуществляется путем:

- обеспечения свободы средств массовой информации, определения правил распространения массовой информации;
- определения категорий информации, распространение которой оказывает деструктивное информационно-психологическое воздействие на сознание человека, на национальную безопасность[64];
- определения категорий информации, распространение которой нарушает законные права и интересы граждан[65].

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 составной частью системы обеспечения национальной безопасности.

---

[64] Информацию, распространение которой оказывает деструктивное воздействие на сознание человека, национальную безопасность, могут составлять сведения:

- экстремистского характера, порнографического содержания,
- пропагандирующие культ насилия и жестокости,
- содержащие призывы к насильственному свержению конституционного строя,
- содержащие призывы к организации или проведению массовых беспорядков, к незаконным организации или проведению массовых мероприятий;
- 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,
- причиняющие вред здоровью и (или) развитию детей,
- содержащие пропаганду, войны, социальной, национальной, религиозной и расовой вражды или розни;
- содержащие угрозу совершения акта терроризма.

[65] Представляется, что информацией распространение которой нарушает законные права и интересы граждан и организаций, может являться:

- заведомо ложная, позорящая другое лицо информация;
- унижающая честь и достоинство лица, а также честь и достоинство представителя власти;
- дискредитирующая деловую репутацию хозяйственного общества,
- содержащая ложные сведения о товарах и услугах,
- содержащая заведомо ложное сообщение, в том силе об опасности;
- 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.

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

- ✓ подсистема государственного управления в области обеспечения информационной безопасности (субъектами этой подсистемы являются Президент, Кабинет Министров, Совет Безопасности, органы государственного управления, ответственные за осуществление государственной политики в области обеспечения информационной безопасности);
- ✓ подсистема обеспечения информационной безопасности (эту 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 государства[66,67]).

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.

Субъекты системы обеспечения информационной безопасности решают следующие задачи:

- обеспечивают реализацию конституционных прав и свобод граждан в информационной сфере;
- обеспечивают реализацию государственной информационной политики и осуществляют защиту национального сегмента информационного пространства;
- обеспечивают безопасность процессов информатизации, построение национальной информационной инфраструктуры, формирование информационного общества;

---

[66] Недосекова, Е.С. Административно-правовые аспекты обеспечения информационной безопасности таможенных органов Российской Федерации: автореф. дис. ... канд. юрид. наук: 12.00.14 / Е.С. Надосекова. – Люберцы, 2011. – С. 11.

[67] «Система мер обеспечения информационной безопасности включает в себя совокупность правовых, политических и организационных средств, включающих средства технологического, кадрового, материального, финансового, информационного и научного обеспечения информационной безопасности. Система мер обеспечения информационной безопасности является составной частью системы обеспечения информационной безопасности, представляющей собой формы деятельности органов, входящих в систему обеспечения информационной безопасности» (Сахно Э.Х. Административно-правовая организация обеспечения информационной безопасности в Российской Федерации: дис. ... канд. юрид. наук: 12.00.14 / Э.Х. Сахно. – Хабаровск, 2006. – С.97).

- обеспечивают защиту критически важных объектов информатизации;
- обеспечивают защиту информационных ресурсов, в том числе, информационных ресурсов, содержащих информацию о личной жизни граждан, их персональные данные, государственные секреты и иные сведения, охраняемые в соответствии с законодательством;
- оказывают противодействие деструктивному информационному воздействию на сознание человека, информационную инфраструктуру и информационную среду;
- осуществляют борьбу с преступностью в информационной сфере, расследование правонарушений против информационной безопасности, применение мер ответственности за правонарушения в информационной сфере.

Обобщая вышеизложенные подходы можно определить 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 через участие в деятельности институтов гражданского общества осуществляет контроль за деятельностью государства по обеспечению информационной безопасности.[68]

3.3. Формы правового обеспечения информационной безопасности

С позиций права цель обеспечения информационной безопасности может рассматриваться как поддержание сбалансированного состояния урегулированных правом общественных отношений, посредством которых субъекты могут свободно реализовывать свои информационные интересы в условиях информатизации общества.

На региональном уровне СНГ и ОДКБ общими целями правового регулирования обеспечения информационной безопасности является создание правовых условий для системной реализации сбалансированных интересов личности, общества и государства, проведения независимой государственной политики[69], развития информационного общества[70] и расширения международного информационного обмена[71].

---

[68] В этой связи следует отметить, что, например, в тексте обновлённой Стратегии национальной безопасности Российской Федерации прямо указано, что обеспечение национальной безопасности — это реализация органами государственной власти и органами местного самоуправления «во взаимодействии с институтами гражданского общества политических, военных, организационных, социально-экономических, информационных, правовых и иных мер, направленных на противодействие угрозам» [утверждена Указом Президента РФ от 31.12.2015 № 683].

[69] Информационный суверенитет представляется, как исключительное право государства в соответствии с национальным законодательством и нормами международного права самостоятельно реализовывать национальные интересы в информационной сфере, проводить государственную информационную политику, распоряжаться собственными информационными ресурсами; формировать инфраструктуру национального сегмента информационного пространства, создавать условия для интеграции в мировую информационную среду.

[70] Информационное общество может рассматриваться как устойчивой система общественных отношений, позволяющей за счет результатов информатизации на качественно новом уровне обеспечить реализацию сбалансированных интересов личности, общества и государства (Бачило И.Л. Информационное право: учебник / И.Л. Бачило. – М.: Издательство Юрайт; 2011. – 2-е изд., перераб. и доп. – 522 с.; Бачило И.Л. Государство и право XX1в. Реальное и виртуальное / И.Л. Бачило. – М. 2012. – 277 с.)

[71] Данная цель закреплена в Рекомендациях по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности (приняты на тридцать восьмом пленарном заседании МПА СНГ, постановление № 38-20 от 23 ноября 2012 г.).

Сложность правового регулирования 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 запретом на доступ к ней). Отношения, связанные с безопасностью информационной инфраструктуры, подчиняются данному порядку. Вышеизложенное (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.

В числе принципов правового регулирования обеспечения информационной безопасности для условий СНГ и ОДКБ предлагается рассматривать следующие:

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

В качестве важнейших принципов совершенствования законодательства в сфере обеспечения информационной безопасности предлагается рассматривать:

- ✓ создание и поддержание безопасных условий информационного обеспечения для реализации прав и обязанностей граждан, организаций, органов государственной власти и органов местного самоуправления в процессе их жизнедеятельности;
- ✓ принятие правовых норм, предотвращающих использование ИКТ для осуществления враждебных действий, актов агрессии, создания угроз безопасному развитию информационного общества;
- ✓ сдерживание распространения информации террористического, экстремистского и сепаратистского характера, а также деструктивной информации, подрывающей политическую, экономическую и социальную стабильность государства, культурный и духовный уклад обществ;
- ✓ разработка правового обеспечения защиты своего информационного пространства и критически важной инфраструктуры от ущерба, возникшего в результате

реального проявления угроз, деструктивного вмешательства, информационных атак и актов агрессии.

Постулируя, что информационная безопасность — состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере, то есть всех разновекторных интересов в совокупности, осуществление правового регулирования обеспечения международной информационной безопасности представляется возможным посредством введения юридической конструкции «правовой статус информационной безопасности».

При этом правовой статус информационной безопасности понимается как интегрированная совокупность качественных характеристик реализации нормативно закрепленных прав и обязанностей субъекта во всех видах информационных отношений.

Применительно к видам субъектов правоотношений в информационной сфере предлагается использование трех правовых информационных статусов:

- ✓ правовой статус информационной безопасности личности;
- ✓ правовой статус информационной безопасности общества;
- ✓ правовой статус информационной безопасности государства *(«информационный суверенитет»)*.

Изложенное позволяет сформировать функциональное содержание правовых статусов субъектов информационной безопасности.

Правовой статус информационной безопасности личности предусматривает реализацию конституционных прав и свобод гражданина в области получения информации и пользования ею, обеспечение реализации следующих прав:

- получение, хранение и распространение полной, достоверной и своевременной информации;
- защищенность от незаконного вмешательства в личную жизнь;
- защиту персональных данных;
- защиту интеллектуальной собственности;
- социальную защиту;
- информационное участие в государственном управлении;
- «электронную занятость»;
- дистанционное («электронное») образование;
- «электронное здравоохранение».

Полноценный правовой статус информационной безопасности общества позволит:

- сохранить его духовные и нравственные ценности (традиции, культурные ценности);
- развивать его интеллектуальный и духовно-нравственный потенциал;
- реализовывать деятельность институтов гражданского общества и свободное распространение в обществе информации о данной деятельности;
- противостоять деструктивному информационному влиянию на общественное и индивидуальное сознание, насаждению чуждых ценностей и ориентиров;
- обеспечивать получение общедоступной информации о состоянии окружающей среды, демографической и социальной обстановке, социальных, экономических и политических процессах;

- способствовать безопасному развитию электронной торговли, «электронных» образования, занятости, здравоохранения.

Правовой статус информационной безопасности государства («*информационный суверенитет*») — это способность государства самостоятельно осуществлять функции государства в информационной сфере с целью соблюдения прав и свобод граждан, обеспечения национальной и коллективной безопасности.

Можно выделить три основных направления обеспечения государственного информационного суверенитета:

1) законодательное определение стратегических путей построения и развития национальной информационной инфраструктуры, защита информационной инфраструктуры и национальных рынков информационных и телекоммуникационных услуг на основе единой государственной политики;

2) выработка норм, формирование правовых основ и границ деятельности зарубежных и международных субъектов в национальном информационном пространстве;

3) определение и последовательная защита национальных интересов в мировом информационном пространстве и международных информационных отношениях.

Государственный информационный суверенитет призван реализовывать:

- информационное обеспечение реализации государственной политики, способствующее повышению эффективности и безопасности функционирования государственных институтов;
- информационное обеспечение международного сотрудничества, способствующее расширению присутствия государства на мировом рынке, в том числе рынке интеллектуальных продуктов, его равноправному участию в мировых информационных отношениях и информационном обмене, информационному обеспечению внешней политики;
- обеспечение инновационного развития, способствующее развитию современных информационных технологий, индустрии информационных услуг, производству средств информатизации;
- построение и безопасное развитие информационной инфраструктуры, создающие технологическую основу управления государством (как в мирное время, так в условиях чрезвычайных ситуаций и в военное время);
- обеспечение надежности и устойчивости функционирования критически важных объектов информационно-телекоммуникационной инфраструктуры (КВО ИТИ);
- сохранность государственных секретов;
- реализацию отношений в информационной сфере, соблюдение законов информационного общества (прав на доступ к информации, порядка информационного обмена, уважение интеллектуальной собственности, законности информационных экономических сделок и др.).

Правовым средством согласования, гармонизации механизмов правового регулирования обеспечения международной информационной безопасности представляется комплексная интегрирующая категория «стандарт правового обеспечения информационной безопасности».

Стандарт правового обеспечения информационной безопасности представляет собой совокупность правовых средств и методов, результатом применения которых является надлежащее обеспечение безопасности информационного статуса личности,

общества и государства. Представляется, что названный стандарт должен включать несколько параметров:

- ✓ наличие комплекса концептуальных взглядов на систему информационных отношений и способы их правового регулирования, реализованных в документе стратегического планирования, определяющего цель, задачи и направления развития информационных отношений, устанавливающего государственную политику в информационной сфере и механизмы ее организационно-правового обеспечения;
- ✓ наличие минимально необходимого для комплексного правового обеспечения информационных отношений научно обоснованного и непротиворечивого понятийного аппарата;
- ✓ достаточную степень сформированности системы правовых предписаний и запретов, определяющих правила поведения в информационной сфере (это, в свою очередь, предполагает готовность общества к криминализации деяний, посягающих на права и интересы субъектов информационной сферы);
- ✓ наличие правовых режимов, эффективность которых достаточна для признания и установления доверия в рамках межгосударственных отношении и сотрудничества;
- ✓ необходимую степень сформированности системы субъектов обеспечения государственной политики в информационной сфере и разработанности организационно-правовых механизмов их деятельности;
- ✓ наличие системы правосудия, эффективно действующей в специфических условиях информационных отношений.

Перечисленные выше параметры являются, в большей степени, формальными, то есть позволяют определить необходимую конфигурацию национального правового обеспечения информационной безопасности, но не его эффективность. Важной задачей является выработка качественных параметров для оценки состояния правового обеспечения информационной безопасности государств – участников СНГ и государств – членов ОДКБ, таких, например, как эффективность функционирования правоохранительной системы.

Практическим воплощением стандарта правового регулирования обеспечения информационной безопасности является стандарт его нормативной урегулированности. По нашему мнению, оценка состояния существующего нормативно-правового обеспечения информационной безопасности государств – участников СНГ и государств – членов ОДКБ также должна учитывать ряд параметров[72]: К их числу следует отнести:

1) охват нормативного обеспечения всех сфер информационной безопасности, образующих интегрированное состояние информационной безопасности, таких как: защита информационных ресурсов; обеспечение государственной политики в информационной сфере; обеспечение безопасности КВО ИТИ; противодействие деструктивному информационному воздействию; противодействие преступлениям в информационной сфере; обеспечение безопасности международного информационного обмена. Здесь представляется оправданным подход, предполагающий, что должен быть достигнут уровень, когда нормативное регулирование обеспечивается для всех

[72] О принятии Рекомендаций по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности: Постановление МПА СНГ, 23 ноября 2012 г., № 38-20 // Информационный бюллетень МПА СНГ. – 2013, № 57. Часть 2. – С. 161.

сформировавшихся на современном этапе групп однородных общественных отношений (институтов);[73]

2) степень юридической силы нормативных актов, регулирующих отношения в сфере информационной безопасности (вероятно, что верхом нормотворчества мог бы стать Информационный кодекс, однако на современном этапе развития информационного законодательства минимально достаточным может быть признан подход, требующий, чтобы каждая из названных выше категорий информационных отношений была урегулирована законом);

3) конституционная закрепленность отношений, возникающих по поводу защиты базовых прав и интересов взаимодействующих субъектов[74];

4) правовая регламентация системы субъектов обеспечения информационной безопасности и нормативное закрепление их функций и полномочий.

Для оценки состояния нормативно-правового обеспечения информационной безопасности государств могут также применяться параметры имплементации в национальное законодательство модельных законов и рекомендательных актов и параметры ратификации основных международных соглашений в данной сфере (в первую очередь соглашений, заключённых в формате СНГ и ОДКБ)

Основу нормативно-правового обеспечения информационной безопасности составляет законодательное регулирование информационных отношений. Представляется, что стандарт законодательной урегулированности информационных отношений на сегодняшний день должен включать целый спектр законов. Это, в первую очередь законы: об информации; о средствах массовой информации и рекламе; об интеллектуальной собственности; о безопасности информационной деятельности; о тайнах; о связи; о функционировании информационных и телекоммуникационных систем, сетей связи, средств информатизации и обработки информации; о системе органов обеспечения информационного развития и информационной безопасности. К этому списку следует добавить правовые нормы о юридической ответственности за виновное нарушение норм, регулирующих отношения в области противодействия угрозам информационной безопасности, находящихся в составе нормативных правовых актов различных отраслей национального законодательства.

Практическое применение сформированной выше конструкции позволяет определить степень развитости нормативного обеспечения информационной

---

[73] В процессе разработки концепции Информационного кодекса в ИГП РАН осуществлен анализ действующего законодательства в этой сфере, проведена работа по структуризации институтов правового регулирования в информационной сфере. Эти институты охватывают такие области регулирования как цели, субъекты информационных отношений, понятийный аппарат правового регулирования информационных отношений.
В рамках особенной части Информационного кодекса концептуально спрогнозированы следующие суперинституты: 1) регулирование правовых режимов информационных ресурсов, информационных технологий, массовых коммуникаций; 2) реализация прав субъектов в информационной сфере, включая право доступа, хранения, обмена, распространения, использования информации и др.; 3) обеспечение информационной безопасности. Названный подход создает возможность более точно провести внутреннюю систематизацию и гармонизацию правовых норм и актов по каждому суперинституту и упорядочить базовый массив законов и других нормативно-правовых актов в рассматриваемой сфере. Это позволит более организованно осуществлять дальнейшее правовое регулирование с учетом развития внутренних и внешних факторов в развитии информационного общества и реализации соответствующих стратегий (Концепция Информационного кодекса Российской Федерации / Под ред. И.Л. Бачило – М.: ИГП РАН – Изд-во «Канон+» РООИ «Реабилитация», 2014. – 192 с.)

[74] Примером может служить конкуренция двух правовых институтов: свободы доступа граждан к информации о деятельности государства и права государства на государственные секреты. Потребность в конституционном закреплении указанных прав не вызывает сомнений, так как только при их однородном правовом статусе возможен баланс интересов личности и государства, формирующий информационную безопасность.

безопасности для каждого государства, входящего СНГ (или ОДКБ) и готовность его правовой системы к международному сближению и гармонизации.

Способами правового регулирования обеспечения информационной безопасности являются введение необходимых ограничений (запретов) и предписаний (мер позитивного обязывания). Основной формой правового регулирования обеспечения информационной безопасности выступает правовой режим. В качестве основных ограничений в сфере обеспечения информационной безопасности можно выделить следующие:

1) запреты на распространение информации экстремистского характера, порнографического содержания; информации, пропагандирующей культ насилия и жестокости, содержащей призывы к насильственному свержению конституционного строя, содержащей призывы к организации или проведению массовых беспорядков, призывы к незаконным организации или проведению массовых мероприятий; запреты на распространение информации, содержащей сведения, которые могут быть использованы для причинения вреда здоровью или нарушения общественной безопасности, в том числе информации о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ, их прекурсоров и аналогов, а также взрывчатых веществ и огнестрельного оружия; запреты на распространение информации, причиняющей вред здоровью и (или) развитию детей, оказывающей деструктивное информационное воздействие на личность; запреты на распространение информации, содержащей пропаганду, войны, социальной, национальной, религиозной и расовой вражды или розни, информации, содержащей персональные данные гражданина, служебную информацию ограниченного распространения (служебную тайну) коммерческую тайну; запреты на распространение информации, составляющей государственные секреты; запреты на распространение заведомо ложной, позорящей другое лицо информации, информации, унижающей честь и достоинство лица, а также честь и достоинство представителя власти, дискредитирующей деловую репутацию хозяйствующего субъекта; информации, содержащей ложные сведения о товарах и услугах; запреты на распространение информации, содержащей заведомо ложное сообщение, в том силе об опасности; содержащей угрозы причинения вреда правам и интересам лица, в том числе, угрозу убийства или причинения другого вреда здоровью, уничтожения имущества, угрозу совершения акта терроризма; запреты на распространение иной информации при отсутствии у получателя возможности отказаться от её получения;

2) запреты на сбор информации, содержащей тайну личной жизни лица, персональные данные гражданина, служебную информацию ограниченного распространения (служебную тайну), коммерческую тайну, профессиональную тайну; запреты на сбор информации, составляющей государственные секреты, иной информации для передачи ее иностранному государству, иностранной организации или их представителю в ущерб национальной безопасности государства;

3) запреты на использование в нарушение прав её обладателей информации, составляющей объекты авторского права и смежных прав, права промышленной собственности, а также на использование вредоносных компьютерных программ;

4) запреты на сдерживание свободного оборота информации, в том числе, ограничение распространения общедоступной информации и осуществление цензуры.

Представляется, что в сфере обеспечения информационной безопасности базовыми должны выступать следующие предписания:

1) Предписания на обязательное распространение общедоступной информации по запросу граждан, на обязательное распространение информации о правах, свободах и законных интересах физических лиц, правах и законных интересах юридических лиц и о порядке реализации прав, свобод и законных интересов; предписания на обязательное распространение информации о деятельности государственных органов, информации о чрезвычайных ситуациях, экологической, санитарно-эпидемиологической обстановке, гидрометеорологической и иной информации, отражающей состояние общественной безопасности; предписания на обязательное распространение информации о состоянии преступности, а также о фактах нарушения законности; предписания на обязательное распространение информации, накапливаемой в открытых фондах библиотек и архивов, информационных системах государственных органов, физических и юридических лиц, созданных (предназначенных) для информационного обслуживания физических лиц.

2) Предписания на соблюдение порядка распространения продукции средств массовой информации, религиозной информации, информации о нацистской символике или атрибутике; предписания на соблюдение порядка распространения рекламы, документирования информации и её использования, в том числе, на соблюдение порядка получения и использования материалов скрытой аудио- и видеозаписи, кино- и фотосъемок; предписания на соблюдение порядка хранения документированной информации, использования радио-, теле-, видео- и кинопрограмм, документальных и художественных фильмов, а также информационных компьютерных файлов и программ обработки информационных текстов, относящихся к специальным средствам массовой информации; предписания на соблюдение порядка, 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; предписания на соблюдение порядка хранения информации в компьютерной системе, сети или на машинных носителях; предписания на соблюдение возрастных ограничений при распространении продукции средств массовой информации; предписания на соблюдение порядка лицензирования отдельных видов деятельности, сертификации отдельных элементов и комплексов информационно-коммуникационной инфраструктуры.

В целом представляется, что названные выше механизмы и формы правового регулирования будут эффективны как система социально справедливого и отвечающего современному социальному запросу упорядочения порождаемых процессами информатизации информационных отношений.

В современных условиях перед правовой мыслью стоит сложнейшая задача, как практически единовременно повторить классический цикл развития правового регулирования для совершенно нового вида общественных отношений и уже сегодня дать цивилизации устраивающую всех субъектов систему правил поведения в информационной сфере.

* * *

ЧАСТЬ II. ВЕХИ РАЗВИТИЯ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРОСТРАНСТВЕ СНГ и ОДКБ

==========

ГЛАВА 4. МОДЕЛЬНОЕ РЕГУЛИРОВАНИЕ В ОБЛАСТИ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. История развития модельного регулирования в области информации, информатизации и обеспечения информационной безопасности на пространстве СНГ

Межгосударственный обмен информацией в текущих политических и экономических условиях трансформировался для государств СНГ в широкомасштабную задачу формирования информационного пространства. Обустройство и развитие информационного пространства требует от государств – участников СНГ (государств – членов ОДКБ) на национальном и межгосударственном уровнях координации усилий в процессе решения широкого круга нормативно-правовых, организационных, технических и финансовых проблем.

История правового обеспечения информационной безопасности в рамках СНГ и государств – его участников не была гладкой и простой. Одним из первых актов МПА СНГ стал принятый в 1993 г. Рекомендательный законодательный акт «О принципах регулирования информационных отношений в государствах Межпарламентской Ассамблеи». В 1996 г. Решением Совета глав правительств государств – участников СНГ была утверждена Концепция формирования информационного пространства СНГ. Этот документ носил рекомендательный характер и представлял собой систему согласованных взглядов на цели и приоритеты сотрудничества государств – участников СНГ в развитии межгосударственного информационного обмена. В целях правового обустройства общего информационного пространства в СНГ разработаны и приняты Модельные законы: «О персональных данных» (1999), «Об электронной цифровой подписи» (2000), «О международном информационном обмене» (2002), «О телекоммуникациях» (2003), «О праве на доступ к информации» (2004) и др. В тексты законов включаются определения используемых в них понятий. Однако, как показал опыт работы по подготовке словаря-справочника, единство и согласованность понятийного аппарата модельного законодательства МПА СНГ оставляет желать большего[75].

В 2006 г. Советом глав правительств СНГ была утверждена Стратегия сотрудничества государств – участников СНГ в сфере информатизации. Стратегия нацеливала государства на совершенствование нормативно-правовой базы, в том числе, на продолжение работы по созданию модельных законов в области информатизации, формирующих условия для широкого использования ИКТ во всех сферах общественной

[75] 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.

жизни и обеспечивающих единство информационного пространства на территории государств – участников СНГ.

Модельное законотворчество МПА СНГ в сфере информатизации начинается с 2005 г., когда был принят базовый Модельный закон «Об информатизации, информации и защите информации». Этот закон имел целью унификацию правового регулирования отношений, связанных с осуществлением права на поиск, получение, передачу, производство и распространение информации; с использованием информации как объекта гражданских прав; созданием и эксплуатацией информационных систем; применением информационных технологий; обеспечением защиты информации[76]. Краткий анализ роли этого модельного закона приведен в материалах аналитического обзора, подготовленного в Институте законодательства и сравнительного правоведения при Правительстве Российской Федерации[77]. Как следует из материалов упомянутого обзора, законодательных актов аналогичных данному модельному закону, в странах дальнего зарубежья нет (как отмечает автор обзора Л.К. Терещенко: «*…зарубежное законодательство не знает такого термина, как информатизация*»). Этим, можно сказать, определялась оригинальность этого модельного закона, так как использование информационных технологий в жизни общества есть не что иное, как процесс усвоения и использования информации в условиях развития ИКТ. Однако, круг лиц, на которые распространял своё действие модельный закон 2005 г., определен не был, используемые в нем термины не были восприняты в национальных законах, хотя сам термин «информатизация» ими уже использовался.

Проблемы развития информационных технологий, глобальное распространение и нарастание роли Интернет, тенденции в развитии гражданского общества высветили круг проблем, требующих отражения в базовых законах. В русле данной тенденции МПА СНГ были приняты Модельный закон «Об основах регулирования Интернета» (2011) и две части Модельного Информационного кодекса (2008 и 2012).

Вызванный развитием Интернет-среды рост угроз в информационной сфере диктовал необходимость пересмотра традиционной для законов об информации формулы «защита информации», переоценки её достаточности для отражения задач современной ситуации в информационной сфере. В результате научным сообществом и законодателями государств – участников СНГ в качестве актуальной была признана парадигма «информационной безопасности». Впоследствии Советом глав правительств СНГ была утверждена Концепция сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности (2008). Это значительно расширило диапазон внимания к работе с информационными ресурсами в формах защиты**,** привлекло усилия к их безопасному использованию и поиску критериев оценки соответствия законодательства изменяющимся ситуациям в глобальной информационной сфере. Концепция представляла согласованную совокупность официальных взглядов и положений о целях, принципах и основных направлениях

[76] До 2008 г. в модельных и национальных законах вопрос об информационной безопасности формулировался как «защита информации». Перелом в трактовках произошел в 2010 г., когда было заключено Соглашение между Правительством Российской Федерации и Правительством Федеративной Республики Бразилия о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности (от 14. 05.2010 г.). Немного позже, в сентябре 2010 г. в Российской Федерации была принята Концепция об обеспечении международной информационной безопасности.

[77] Терещенко, Л.К. Исследование имплементации модельных законов, принятых МПА СНГ в сфере информатизации и связи, в государствах – участниках СНГ / Л.К. Терещенко. – М.: ИЗИСП, 2013. – С. 61-68.

межгосударственного сотрудничества в сфере обеспечения информационной безопасности.

В 2012 г. Советом глав правительств СНГ была утверждена Стратегия сотрудничества государств – участников СНГ в построении и развитии информационного общества, отражающая общее видение путей его формирования. Отдельным направлением сотрудничества в этом документе обозначена проблема обеспечения информационной безопасности. В 2013 г. рядом государств – участников СНГ было подписано Соглашение о сотрудничестве в области обеспечения информационной безопасности.

25 октября 2013 г. решением Совета глав государств СНГ была принята Межгосударственная программа сотрудничества государств – участников СНГ в области совместных мер по борьбе с преступностью на 2014-2018 гг. Этой программой было предусмотрено внесение изменений в существовавший с 2005 г. Модельный закон «Об информатизации, информации и защите информации». Во исполнение такого решения был подготовлен и на сорок первом пленарном заседании МПА СНГ принят новый Модельный закон «Об информации, информатизации и обеспечении информационной безопасности» (постановление от 28.11.2014 г. № 41-15 СНГ[78]). Рассмотрению концепции и текста этого закона посвящена данная глава.

Развитие информационной сферы формировало новые вызовы правовому регулированию и определяло актуальность работы по совершенствованию модельного информационного законодательства СНГ, где принимались как отдельные законодательные акты, затрагивающие информационную сферу (например, Модельные законы «Об электронной торговле» (2008) и «Об электронных государственных услугах» (2010), так и специализированные кодифицированные — Модельный Информационный кодекс (2008 и 2012) и др. Оценка состояния модельного информационного законодательства МПА СНГ выявила диссонанс между законами об информации, о доступе к информации, о публичных услугах, о персональных данных и иных категориях информации ограниченного доступа, об использовании электронной цифровой подписи и т.д. Данная обстановка обусловила необходимость сопряжения законодательства государств – участников СНГ с учётом его рассогласованности по определению предмета и метода регулирования информационных отношений. В силу этого требовался консолидирующий акт на основе общей терминологии, методов регулирования отношений и удержания процесса в безопасном состоянии, создающий ориентацию на комплексное регулирование социально значимых проблем в информационной сфере всех государств − участников СНГ.

Изменения, проявившиеся за прошедшие более чем десять лет, ускоряющиеся темпы развития информационных отношений и формирования информационного общества требовали, в первую очередь, совершенствования структуры и содержания действовавшего Модельного закона «Об информатизации, информации и защите информации», учета опыта национального законодательства, что создавало основу для его коррекции. Этот вопрос был включен в содержание задания МПА СНГ по совершенствованию информационного законодательства.

В заключении специалистов по информационному праву Института Государства и права РАН были отмечены проблемы, которые требовали первоочередного учета при

---

[78] Бачило, И.Л. К вопросу о развитии информационного законодательства СНГ / И.Л. Бачило, М.А. Вус, О.С. Макаров // Информатизация и связь. – 2014. – № 1. – С. 13-16.

обновлении Модельного закона «Об информатизации, информации и защите информации» (2005). В их числе были названы следующие:

- ✓ обобщение опыта развития информационного общества за последние десятилетия;
- ✓ анализ состояния национального законодательства государств – участников СНГ и обеспечения реальной правовой защищенности общества, государства, человека;
- ✓ выявление новых вызовов информационной безопасности, включая возрастание значения открытой информации, обострение проблем защиты результатов интеллектуального творчества (защита патентов, национального программного обеспечения в национальных ИКТ,) и др.;
- ✓ повышение значения правового регулирования проблем информационной безопасности.

Этот анализ направления подкреплён обобщением опыта в области информатизации Республики Казахстан и Республики Беларусь, а также других государств – участников СНГ, где сложилась достаточно разветвлённая система правовых актов по разным направлениям развития информационного общества, а национальные законы имели существенные особенности правового регулирования. Так, например, действующий с 2007 г. в Республике Казахстан Закон «Об информатизации» получил в 2013 г. свою новую редакцию; Закон Республики Беларусь «Об информации, информатизации и защите информации» (2008.) с изменениями, внесёнными в него в 2014 г., также сохранил приоритет ориентации на проблемы информатизации.

Разработчиками учитывался также опыт применения принятого в 2006 г. в Российской Федерации нового Федерального закона «Об информации, информационных технологиях и о защите информации» (2006).[79,80]

Результаты проведённого анализа необходимо было соотнести с наиболее заметными изменениями в информационных отношениях, произошедшими за последние пятнадцать лет. При этом выявилась актуальность проблемы обеспечения качества функционирования такого института как «электронное правительство», оценки его роли в процессах информатизации всей системы органов государственной власти и органов местного самоуправления, взаимодействия с общественными и негосударственными организациями. Требовалась оценка состояния инфраструктуры ИКТ и ее управляемости со стороны органов исполнительной власти в государствах – участниках СНГ (министерств информации, связи и массовых коммуникаций, других органов государственного управления).

Необходимо было реанимировать некоторые полезные нормы самого первого нормативного акта МПА СНГ в сфере информационных отношений — Рекомендательного законодательного Акта «О принципах регулирования информационных отношений в государствах – участниках Межпарламентской

---

[79] По сравнению с первыми редакциями законов по этой проблеме названный новый закон необоснованно утратил некоторые важные проблемы правоотношений. Сосредоточив внимание на информационных технологиях, он ослабил позиции по регулированию информационных ресурсов, правового режима этих ресурсов, а главное, — к процессу использования информации и информационных технологий. Вопрос об «информатизации» из этого закона выпал. Специалисты отмечали необходимость унификации, как понятийного аппарата, так и уточнения содержательной его части: принципов и правил взаимодействия в данной сфере, устранения ряда пробелов и приближения к международной практике регулирования информационных отношений. В последующие годы в российский закон «Об информации, информационных технологиях и о защите информации» предлагались и вносились изменения и дополнения, что видно на исследованиях правовой основы информационных отношений в связи с разработкой концепции информационного кодекса (авт.).

[80] Королёв, А.Н. Комментарий к Федеральному закону «Об информации, информационных технологиях и о защите информации» (постатейный) / А.Н. Королёв, О.В. Плешакова. – М.: ЗАО Юстицинформ, 2007. – 128 с.

Ассамблеи» (от 23.05.1993 г.), который предшествовал первому российскому закону «Об информации, информатизации и защите информации» (1995).[81, 82]

При разработке изменений и дополнений в Модельный закон «Об информатизации, информации и защите информации» (2005) на первый план вышли такие проблемы как:

а) статус системы нормативно-правовых актов, положенных в основу формирования отрасли законодательства по информационному праву;

б) легитимное закрепление общего понятия информация, с учетом того, что большинство государств, входящих в состав СНГ, от определения информации как «сведений о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления» не отказалось и устойчиво сохраняют в определении области регулирования процесс «информатизации» (Республика Казахстан, Республика Беларусь, Кыргызская Республика и др.).

в) определение в качестве предмета регулирования не любой информации, а информации документированной, образующей информационные ресурсы, фиксируемые на материальных носителях с реквизитами, позволяющими её идентифицировать;

г) введение в систему модельного правового регулирования института «правовой режим информационных ресурсов». При таком определении информация рассматривается как информационный ресурс, выступающий в форме отдельных документов, их массивов в информационных системах, электронных документов и информационных систем (баз данных в том числе);

д) закрепление положений о праве собственности и интеллектуальной собственности субъектов на свой информационный ресурс, включаемый в состав института правового режима информационных ресурсов. Это важно в связи с тем, что после принятия в России Федерального закона "Об информации, информационных технологиях и о защите информации" (от 27.07.2006 г. № 149-ФЗ) в Российской Федерации этот вопрос трактуется как «право обладания» без указания статуса субъектов и юридической характеристики акта «обладания» ресурсом;

е) обязательное включение в состав правового режима информации (информационного ресурса субъекта) установления порядка отношений субъектов при соблюдении гарантий права на информацию. Здесь важен не только режим информации ограниченного доступа — с одной стороны, но не менее значим режим информации, которая не подлежит ограничению — с другой. В итоге обозначились новые информационные институты: открытых данных и открытого правительства, включая такую информацию, которая может быть отнесена к национальному достоянию.

---

[81] К середине второго десятилетия текущего столетия можно констатировать, что сформировалась отрасль ИКТ в качестве отрасли экономики государства, функционирующая по законам мирового рынка. Стал более заметным объективно обусловленный разрыв между инфраструктурой ИКТ и задачами функциональной информационной инфраструктуры аппарата в системе органов исполнительной власти. Функциональная информационная инфраструктура органов государственной власти не может быть ограничена работой по развитию и обустройству информационных систем, специально организованными департаментами, управлениями и т.п. Практика показывает, что информатизация — это постоянная и непрерывная деятельность всех администраций и их подразделений на основе использования потенциала ИКТ, и она не может быть ограничена только насыщением управленческих структур средствами информационных технологий и базироваться на договорах по созданию информационных систем и их сопровождению в процессе использования (*авт.*).

[82] В свое время названный российский закон, принятый как базовый, создал основу для упорядочения отношений в информационной сфере и служил более десяти лет ориентиром для последующего развития информационного законодательства большинства государств СНГ.

(В России обсуждалась необходимость закрепления в законодательной форме условий использования информационного ресурса определенного субъекта, гарантий реальных условий для обеспечения всех форм права на информацию[83], что невозможно обеспечить без учета легитимации «открытой информации» и «открытого правительства».);

ж) необходимость определить правовой статус субъектов информационных отношений,

з) потребность в достаточном и непротиворечивом понятийном аппарате[84];

и) учет динамики информационных отношений, расширение их диапазона, преодоление ситуационных решений законодателя (чтобы избежать непрерывного внесения поправок в действующие законы). Это поставило вопрос о систематизации законодательства и выработке подходов к его стабилизации;

к) вовлечение информационной продукции в экономический оборот, что актуализировало проблему реализации имущественных прав (сфера гражданского законодательства) и прав на информацию (сфера публичного регулирования). Проблема осложнялась необходимостью законодательного обеспечения широкого доступа к информации, с одной стороны, и определения границ такого доступа с учетом интересов государства, структур, занятых разработкой и созданием информационных технологий (особенно программного обеспечения), юридических и физических лиц, с другой;

л) необходимость создания и совершенствования правовых мер борьбы с новыми видами преступлений в информационной сфере.

При проработке концепции совершенствования названного модельного закона разработчики исходили из позиции, что такой закон должен ориентировать на единые рекомендуемые термины и понятия, четко определять цели и назначение правового регулирования отношений, перспективных и важных для развития СНГ. В нём должна быть выражена концепция, направленная на усиление информационного взаимодействия государств – участников СНГ в процессе решения задач Содружества, и в первую очередь, задач создания единого экономического пространства, сближения информатизации социального сектора, сближения культур и иных направлений плодотворного взаимодействия.

Чтобы системно увязать основные акты в области информатизации и заложить основу для дальнейшего развития информационного законодательства государств − участников СНГ, важно было закрепить в модельном законе наличие таких трех правовых категорий как «информация», «информатизация» и «обеспечение информационной безопасности». В связи с этим, решением профильной комиссии МПА СНГ было одобрено изменение названия нового Модельного закона, уточнение его структуры и содержания отдельных статей. Предложенное изменение названия (вместо Закона «Об информатизации, информации и защите информации» — Закон «Об информации, информатизации и обеспечении информационной безопасности») явилось реакцией на ситуацию в области формирования и развития информационного общества, которая требует не консервировать информацию и держать её в режиме контроля за доступом, а обеспечивать эффективное включение информации в системы решения задач национального и международного взаимодействия государств − участников СНГ.

---

[83] Городов, О.А. Комментарий к Федеральному закону «Об информации, информатизации и защите информации» / О.А. Городов. – СПб.: Питер, 2003. – 272 с.

[84] Сергиенко, Л.А. История формирования информационного права в СССР и Российской Федерации 1960-2000 гг.: монография Л.А. Сергиенко. – М.: ЮРКОМПАНИ, 2013. – 272 с.

В конечном итоге разработанный российскими и белорусскими учёными новый Модельный закон «Об информации, информатизации и обеспечении информационной безопасности» был принят на 41-м пленарном заседании МПА СНГ (постановление от 28.11.2014 г. № 41-15).[85]

По замыслу разработчиков сферой действия данного модельного закона выступили правовые 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. Целью разработки данного закона декларируются усилия по сближению национального законодательства и организации информационного взаимодействия субъектов в процессе формирования единого информационного пространства государств − участников СНГ.

В качестве основополагающих были определены следующие концептуальные положения нового закона:

1) суверенитет государства обеспечивается при реализации норм международного права, норм национального законодательства в области организации и реализации потенциала ИКТ и в процессе информационного взаимодействия органов государственной власти в информационном пространстве Интернет и в информационном пространстве СНГ при обеспечении информационной безопасности государства, общества и личности;

2) информационное пространство рассматривается как область информационного взаимодействия государств − участников СНГ, коммуникационные связи которых реализуются преимущественно через сеть Интернет и государственные системы СМИ, телекоммуникационные системы, мобильные формы связи, локальные информационные системы межгосударственного и внутригосударственного общения;

3) в целях повышения уровня организации и эффективности информатизации межгосударственного сотрудничества модельный закон определяет правовой порядок взаимодействия двух 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;

4) порядок организации распространения информации в сети Интернет и идентификации лиц, осуществляющих деятельность по обеспечению функционирования информационных систем, опосредующих прием, передачу, доставку или обработку электронных сообщений пользователей сети Интернет, предполагается урегулировать национальным законодательством государств − участников СНГ. Национальным законодательством также определяются права и обязанности организаторов распространения информации в сети Интернет (владельцев сайта и/или страницы сайта, блогеров);

5) правовое регулирование в области развития информационного общества должно осуществляться с позиций, рассматривающих производство и эксплуатацию потенциала ИКТ как единый народно-хозяйственный комплекс, объединяющий государственные, корпоративные и частные производства и средства их обеспечения. Государственное

[85] Информационный бюллетень МПА СНГ. – 2015, № 62. Часть 2. – С. 97-121.

регулирование при этом должно быть направлено на обеспечение конкурентоспособности отрасли информационных технологий, нацеленной на повышение качества жизни граждан, развитие экономической, социально-политической, научно-технической и культурных сфер жизни общества;

6) направления обеспечения информационной безопасности должны охватывать все программные решения в области развития информационного общества и все направления национальной безопасности каждого государства. Предполагается их реализация через перспективные программы и планы развития информационного общества, включая проблемы безопасности информационной среды с учетом масштабов и форм использования сети Интернет;

7) руководство государства устанавливает орган, ответственный за координацию и обеспечение безопасности по всем направлениям развития информационного общества, включая направления международного сотрудничества и взаимодействия в информационном пространстве государств − участников СНГ;

8) в качестве важнейшего объекта информационной безопасности рассматривается сознание и психическое здоровье человека и населения каждого государства.

4.2. Структура и содержание Модельного закона СНГ «Об информации, информатизации и обеспечении информационной безопасности»

В ходе подготовки изменений и дополнений в действовавший ранее Модельный закон «Об информатизации, информации и защите информации» авторами выработан ряд подходов к построению и наполнению проекта нового модельного закона. Указанные подходы находятся в русле единой концептуальной позиции группы разработчиков и усиливают её. В таблице приведено сравнение структур Модельного закона «Об информатизации, информации и защите информации» (2005) и разработанного нового Модельного закона «Об информации, информатизации и обеспечении информационной безопасности» (2014).

«Об информатизации, информации и защите информации» (2005)	«Об информации, информатизации и обеспечении информационной безопасности» (2014)
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 Закона Ст.2. Основные термины и понятия, используемые в Законе Ст.3. Субъекты отношений в сфере действия настоящего Закона. Ст.4. Законодательство в области информации, информатизации и информационной безопасности Ст.5. Принципы правового регулирования отношений в рамках настоящего Закона Ст.6. Основные принципы государственной политики в области информации и информатизации
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 представление информации Ст.12. Представление 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 и 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

Глава 3. Информатизация, информационные системы и информационные технологии Ст.15. Государственная политика и полномочия государства в сфере информатизации Ст.16. Информационные системы 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 регулирование информационной инфраструктуры системы государственного управления Ст.16. Взаимодействие органов государственного управления и органов местного самоуправления со структурами, создающими базу ИКТ Ст.17. Юридическое оформление отношений субъектов в процессе информатизации: договоры, соглашения, регламенты.
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. Основы правового регулирования обеспечения информационной безопасности и ответственности за правонарушения в процессах информатизации** Ст.18. Организационно-правовое обеспечение политики в области информационной безопасности Ст.19. Направления, цели и задачи обеспечения информационной безопасности Ст.20. Методы организационно-правового регулирования обеспечения информационной безопасности Ст.21. Обеспечение безопасности информационно-коммуникационной инфраструктуры Ст.22. Обеспечение безопасности критически важных объектов информационно-коммуникационной инфраструктуры Ст.23. Защита информационных ресурсов, меры ограничения доступа Ст.24. Обеспечение безопасности информационной среды Ст.25. Защита от распространения вредной информации и использования деструктивной информации Ст.26. Виды и формы юридической ответственности за правонарушения в области информационных отношений.
Глава 5. Ограничения на доступ к информации и на распространение информации Ст.27. Конфиденциальная информация Ст.28. Информация о частной жизни и информация персональная Ст.29. Коммерческая тайна Ст.30. Профессиональная тайна Ст.31. Государственная и служебная тайны Ст.32. Ограничения на распространение информации	
Глава 6. Защита информации Ст.33. Государственное регулирование зашиты информации Ст.34. Обеспечение информационной безопасности Ст.35. Защита информации в информационных системах Ст.36. Ответственность за правонарушения в сфере защиты информации и права на информацию. Ст.37. Вступление в силу настоящего Закона	

В сравнении с ранее действовавшим Модельным законом «Об информатизации, информации и защите информации» новый Модельный закон «Об информации, информатизации и обеспечении информационной безопасности» представлен более лаконичным и компактным как по числу глав (4 вместо 5), так и по числу статей (23 против 37 у его предшественника). Рассмотрение структуры и содержания Модельного закона «Об информации, информатизации и обеспечении информационной безопасности» (2014) позволяет отметить его новизну с учетом нижеследующего:

- одновременно со сменой названия самого закона уточнен предмет правового регулирования за счет расширения сферы его применения — отношений в области информационно-коммуникационного взаимодействия государств в едином информационном пространстве СНГ, что позволяет конкретизировать и гармонизировать информационный и технологический ресурсы этих государств;
- проведено частичное изменение перечня терминов и их определений с учетом глобального использования Интернета в инфраструктуре информационного пространства (отражено в Статье 2);
- сам термин «информационная безопасность» определяется как «состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве». При этом обеспечение информационной безопасности охватывает 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 угроз в национальном и международном информационном пространстве;
- введено новое определение понятия — «официальная информация», которая рассматривается как 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.

В первой главе закона «Общие положения» введена новая статья о субъектах отношений. Глава 2 Модельного закона имеет более ёмкое название: «Информация, информационные ресурсы, основы правового режима информационных ресурсов» и охватывает вопросы связи информации и информационных ресурсов, а также вопросы о видах информационных ресурсов, правовом режиме информационных ресурсов, включая установление форм собственности и исключительных прав на объекты интеллектуальной собственности, используемые в сети Интернет и других электронных информационных системах.

Глава 3 «Информатизация, информационные системы и информационные технологии» охватывает вопросы:

- информационной политики и организационно-правового обеспечения ее реализации в области информатизации;
- формирования и освоения информационного пространства, как области информационного взаимодействия государств-участников СНГ;
- организационно-правового развития информационной инфраструктуры отрасли ИКТ и инфраструктуры системы органов государственного управления в условиях информатизации.

Здесь же в отдельной статье регламентированы проблемы информационного взаимодействия органов государственного управления и местного самоуправления; более основательно проработаны нормы о юридическом оформлении отношений участников процессов информатизации: вопросы договоров, соглашений, регламентов.

Уже само название четвёртой главы нового закона — «Правовое регулирование обеспечения информационной безопасности и ответственности за правонарушения в процессах информатизации» соответствует концепции закладываемых в законодательное регулирование изменений.

В новом законе представлены специальные статьи о государственной политике и о методах обеспечения информационной безопасности. Проблема обеспечения информационной безопасности рассматривается как важнейшая составляющая национальной и международной безопасности, что прослеживается в используемых определениях терминов «информационная безопасность» и «обеспечение информационной безопасности».

В завершение сказанного следует подчеркнуть значение норм: о государственной политике по обеспечению информационной безопасности; о направлениях, задачах и методах обеспечения информационной безопасности; об обеспечении безопасности информационной инфраструктуры и информационной среды; о правах граждан и организаций; об открытой и общедоступной информации; о защите от распространения и использования вредной и деструктивной информации, нашедших своё отражение в тексте нового Модельного закона «Об информации, информатизации и обеспечении информационной безопасности».

* * *

ГЛАВА 5. МОДЕЛЬНОЕ РЕГУЛИРОВАНИЕ НА ПРОСТРАНСТВЕ СНГ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАЦИОННО - КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ

5.1. Обоснование и структурно-сущностная характеристика модельного регулирования в области обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры

Модельное регулирование в области обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры (КВО ИКИ) осуществлялось на основании положений Межгосударственной программы совместных мер борьбы с преступностью на 2014-2018 годы, утвержденной решением Совета глав государств СНГ 25 октября 2013 г. В рамках этой Межгосударственной программы был разработан и принят на сессии МПА СНГ Модельный закон «О критически важных объектах информационно-коммуникационной инфраструктуры» (постановление от 28.11.2014 г № 41-14). [86]

Данный Модельный закон основывается на принятых ранее Модельном Информационном кодексе для государств – участников СНГ, Модельных законах «Об информации, информатизации и защите информации» и «О международном информационном обмене», Рекомендациях по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности, а также учитывает положения действующих в национальных государствах – участниках нормативных правовых актов: Закона Азербайджанской Республики «Об информации, информатизации и защите информации» (от 3 апреля 1998 г. № 460 IQ); Закона Республики Армения от «О телекоммуникации» (от 17 февраля 1998 г.); Закона Республики Беларусь «Об информации, информатизации и защите информации» (10 ноября 2008 г. № 455-З); Закона Республики Казахстан «О связи» (от 5 июля 2004 г. № 567-II); Законов Республики Молдова «Об информатике» (от 22 июня 2000 г.) и «О предупреждении и борьбе с преступностью в сфере компьютерной информации» (от 3 февраля 2009 г.); Федерального закона Российской Федерации «Об информации, информационных технологиях и о защите информации» (от 27 июля 2006 г. № 149-ФЗ); Законов Украины «О защите информации в информационно-телекоммуникационных системах» (от 5 июля 1994 г. № 80/94-ВР) и «О телекоммуникациях» (от 18 ноября 2003 г. № 1280-IV); Указа Президента Республики Беларусь «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации» (от 25 октября 2011 г. № 486); а также положениях Указа Президента Российской Федерации «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (от 15 января 2013 г. № 31с).

Необходимость разработки закона о КВО ИКИ была обусловлена:

- ✓ увеличением числа КВО в системе объектов ИКИ государств – участников СНГ;

[86] Информационный бюллетень МПА СНГ. – 2015, № 62. Часть 2. – С. 57-96.

- ✓ повышением уровня опасности последствий для государства, общества и отдельных лиц в случае нарушения (прекращения) нормального функционирования КВО ИКИ;
- ✓ расширением спектра угроз безопасности таким объектам, изменением их характера и интенсивности;
- ✓ отсутствием в большинстве государств – участников СНГ нормативно закреплённых основ деятельности по обеспечению нормального функционирования КВО ИКИ, а также по предупреждению, выявлению и локализации угроз их безопасности.

Основной целью подготовки модельного закона явилась выработка новой согласованной политики на пространстве СНГ в сфере информационной безопасности, гармонизация законодательных решений государств – участников СНГ в области обеспечения безопасности КВО ИКИ. Основные задачи при этом были определены как:

- установление единых (общих) основных положений законодательства в области безопасности КВО ИКИ, обеспечивающих регулятивную мобильность уполномоченных государственных органов государств – участников СНГ;
- определение общих положений правового статуса субъектов обеспечения безопасности объектов КВО ИКИ;
- выработка механизма установления эквивалентности и взаимного согласования систем обеспечения безопасности КВО ИКИ в государствах – участниках СНГ;
- формирование единой, скоординированной и сопряженной системы правовых, организационных, инженерно-технических, программно-аппаратных и специальных мер обеспечения безопасности КВО ИКИ в государствах – участниках СНГ.

В качестве предмета правового регулирования предусматривались правовые, организационно-управленческие и иные отношения, связанные с организацией и осуществлением деятельности по обеспечению нормального функционирования и безопасности КВО ИКИ.

Принятие Модельного закона «О критически важных объектах информационно-коммуникационной инфраструктуры» позволило: создать эффективные организационно-правовые механизмы, способствующие формированию и развитию системы обеспечения безопасности КВО ИКИ; обеспечить комплексную реализацию положений Стратегии сотрудничества государств – участников СНГ в построении и развитии информационного общества; повысить действенность системы мер интеграционного сотрудничества государств – участников СНГ в рамках сближения законодательства в сфере обеспечения информационной безопасности; повысить качество принимаемых нормативных правовых актов в сфере информационной безопасности; обеспечить защищённость информационных интересов граждан, общества и государства, адресность государственной информационной политики; обеспечить гармонизацию национальных законов и нормативных актов в области информационной безопасности в целях формирования единого (общего) информационного пространства государств – участников СНГ; расширить интеграцию информационных сфер государств – участников СНГ; урегулировать вопросы, касающиеся отношений в информационной сфере, которые должны единообразно решаться всеми государствами – участниками СНГ; согласовать подходы к подготовке специалистов в области обеспечения информационной безопасности и др.

Модельный закон «О критически важных объектах информационно-коммуникационной инфраструктуры» имеет следующую структуру.

Преамбула, которая определяет предмет правового регулирования. Здесь охарактеризованы состояние и тенденции правового регулирования соответствующей сферы общественных отношений.

Глава 1 «Общие положения», которая закрепляет основные понятия и их определения выработанные на основе терминологии, используемой в международных соглашениях и в законодательстве государств – участников СНГ, а также принципы и законодательство в области обеспечения безопасности КВО ИКИ. Основной целью закрепления унифицированной терминологии является обеспечение единообразного толкования и применения правовых норм национального законодательства стран СНГ, а также международных соглашений.

В Главе 2 «Государственное управление и полномочия государственных органов в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры» описываются основные направления государственной политики в области обеспечения безопасности КВО ИКИ, а также полномочия государственных органов и иных организаций в данной области.

Глава 3 «Отнесение объектов информационно-коммуникационной инфраструктуры к критически важным» содержит положения, определяющие общие критерии, порядок отнесения объектов информатизации к КВО ИКИ, а также определения категории КВО ИКИ.

Глава 4 регламентирует вопросы организации функционирования критически важных объектов информационно-коммуникационной инфраструктуры. Нормативные предписания, закрепленные в этой главе, описывают порядок и требования по обеспечению надежного и устойчивого функционирования КВО ИКИ, а также особенности внутреннего и внешнего контроля безопасного функционирования КВО ИКИ.

Положения Главы 5 «Обеспечение безопасности критически важных объектов информационно-коммуникационной инфраструктуры» устанавливают нормы, определяющие систему обеспечения безопасности КВО ИКИ: объекты, субъекты, задачи, принципы, а также конкретные правовые, организационные, инженерно-технические, программно-аппаратные и специальные меры, которые должны реализовываться в рамках данного правового режима. В этой же главе описаны полномочия собственников КВО ИКИ, государственных органов и иных организаций по обеспечению безопасности КВО ИКИ.

Нормы Главы 6 «Государственная система реагирования на инциденты безопасности критически важных объектов информационно-коммуникационной инфраструктуры» предусматривают создание Национального центра реагирования на инциденты безопасности КВО ИКИ и порядок реагирования на инциденты безопасности КВО ИКИ.

Глава 7 определяет основания и порядок привлечения к ответственности лиц, виновных в нарушении законодательства в области обеспечения безопасности КВО ИКИ. Здесь же устанавливается обязательность страхования при эксплуатации КВО ИКИ, характеризуются страховые риски, минимальные размеры страховых сумм (лимитов ответственности) и др..

Глава 8 содержит положения, определяющие основания и порядок исключения объектов ИКИ из числа критически важных.

Глава 9 «Государственный контроль за обеспечением безопасности критически важных объектов информационно-коммуникационной инфраструктуры» определяет государственный орган, уполномоченный осуществлять государственный надзор в сфере обеспечения безопасности КВО ИКИ, его полномочия, а также основы и порядок осуществления такого контроля.

5.2. Понятие и содержание критически важных объектов информационно-коммуникационной инфраструктуры

В современных условиях интенсивное развитие инфраструктур в различных сферах жизнедеятельности государства, в том числе ИКИ обуславливает увеличение числа различного рода 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 актуализируется проблема формирования обоснованной и оптимальной системы КВО ИКИ в целях обеспечения должного и надёжного функционирования всех общественных и государственных институтов.

Учитывая, что нормативно ИКИ не определена, 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 информационно-коммуникационной инфраструктуры 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.

Объекты ИКИ целесообразно рассматривать как критически важные, 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 последствиям в политической, экономической, социальной, информационной, экологической и иных сферах.

С учетом сказанного 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 — см.: Статьи 2 и 3 Модельного закона СНГ «Об основах регулирования Интернета»[87]);

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.)).

5.3. Формирование системы критически важных объектов информационно-коммуникационной инфраструктуры

Целью системы обеспечения безопасности КВО ИКИ является обеспечение должного функционирования соответствующих объектов, в том числе, в случае реализации угроз их безопасности. При обеспечении безопасности КВО ИКИ должен достигаться баланс интересов государства и общества и интересов собственников (владельцев) таких объектов.

Основными задачами обеспечения функционирования КВО ИКИ являются:

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

Формирование системы КВО ИКИ включает 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.

2 этап: определение признаков критичности ИКИ.

Для того, чтобы определить критичность ИКИ, требуется разработка соответствующих признаков. В качестве признаков критичности ИКИ необходимо рассматривать:

- наличие взаимосвязанной совокупности объектов такой инфраструктуры;
- возможность наступления тяжких последствий для отрасли при нарушении (прекращении) нормального функционирования одного или части объектов.

3 этап: выделение из числа критических инфраструктур государства объектов 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.

---

[87] 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.

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 их взаимодействия 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:

- ✓ определение недопустимого ущерба[88];
- ✓ определение важности объекта[89].

Вместе с тем анализ содержания обоих названных способов оценки объектов 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, характеризуемую 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.

Для оценки важности объекта в масштабе соответствующих групп (в частности, и в рамках ИКИ) может быть разработана система рамочных критериев, которые характеризуются следующими показателями[90]:

- 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.); П3 – балансовая стоимость основных производственных фондов (млн. руб.); П4 – доля основной продукции объекта в продукции того же вида, выпускаемой в государстве (в процентах);
- 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

---

[88] Концепция категорирования потенциально опасных объектов национальной транспортной инфраструктуры / Д.С. Черешкин [и др.] // Труды Ин-та систем. анализа Рос. Академии Наук. – 2007. – Т. 31. – С. 5–20

[89] Методический подход к отнесению объектов к категории критически важных. – М.: ФГУ ВНИИ ГОЧС (ФЦ) МЧС России, 2006. – 50 с.

[90] Методический подход к отнесению объектов к категории критически важных. – М.: ФГУ ВНИИ ГОЧС (ФЦ) МЧС России, 2006. – С. 2.

вооруженных сил; П9 – нарушение стабильности финансовой или банковской систем);

- 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 ИКИ к КВО, который включает в себя следующие стадии[91]:

- установление оснований для отнесения объекта ИКИ к КВО;
- принятие решения о включении объекта в перечень КВО ИКИ;
- учёт объекта, отнесённого к КВО, в Государственном реестре КВО ИКИ;
- 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 своих нормативных актах.

6 этап: определение отраслевых критериев в ИКИ.

В ИКИ сосредоточены КВО различных групп и различного уровня. 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.

Вследствие сказанного 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

---

[91] 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. – С. 75-78, 81-94.

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[92]:

- 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. Общие требования закрепляются, как правило, в законодательных актах, конкретные — в технических нормативных правовых актах. Кроме этого, 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 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.

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

В процессе правового обеспечения создания КВО на первое место следует поставить разработку и утверждение в установленном порядке уставов или положений о конкретных КВО, которые предусматривают:

- задачи субъектов КВО, которые в силу своей особой значимости требуют безусловного исполнения их заинтересованными предприятиями, организациями, государственными органами, иными юридическими и физическими лицами;
- объём полномочий таких субъектов и их работников и сотрудников, то есть совокупность их прав и обязанностей, обеспечивающих возможность решения установленных задач;

---

[92] Там же. – С. 61-68.

- подведомственность, которая определяет сферу реализации полномочий заинтересованными юридическими и физическими лицами.

Всем субъектам, осуществляющим деятельность в области КВО ИКИ (собственники (владельцы) таких объектов, уполномоченные государственные органы, привлекаемые юридические и физические лица), предписывается в пределах своих полномочий и компетенции обеспечивать как целевое функционирование данных объектов, так и их безопасность.

5.4. Обеспечение безопасности критически важных объектов информационно-коммуникационной инфраструктуры

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. Внимание к данному виду объектов обусловлено двойственностью их социальной природы: повышенной социальной значимостью и потенциальной способностью своей дисфункцией причинить существенный ущерб общественным интересам. Анализ угроз безопасности КВО ИКИ позволяет представить их классификацию:

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 технологические 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.

Реализация названных угроз 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 им

организациями при осуществлении компьютерной атаки на государственные информационные системы и т.п.);

- ✓ возникновения 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.).

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

В связи со сказанным государство выделяет в особую область регулирования вопросы безопасности КВО ИТИ и ставит соответствующие задачи безопасной эксплуатации таких объектов.

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 в определенный промежуток времени в случае реализации угроз его безопасности;
- ✓ полное или частичное возмещение винновыми субъектами вреда, причиненного интересам государства и общества, интересам объекта в результате нарушения (прекращения) его функционирования.

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

1) организационное — 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) правовое — обеспечение безопасности КВО ИКИ на основе обеспечения правомерной деятельности работников таких объектов, их служб 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.).

В состав системы обеспечения безопасности КВО ИКИ в общем случае должны входить следующие элементы:

1) нормативно-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;

2) 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;

3) 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 соответствии 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);

4) 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.

Применение мер обеспечения безопасности КВО ИКИ является достаточным, если исключает нарушение (прекращение) функционирования такого объекта. Содержание мер безопасности для конкретного КВО ИКИ определяется собственником (владельцем) такого объекта и (или) его руководством в соответствии с действующим законодательством государства.

Непосредственное создание системы обеспечения безопасности КВО ИКИ включает в себя следующую совокупность мероприятий[93]:

1) 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;

2) анализ, определение и моделирование угроз безопасности КВО ИКИ и инцидентов безопасности;

3) проведение первоочередных мероприятий на КВО ИКИ, основными из которых являются разработка:

---

[93] 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. / Матусевич С.В., Михаленок С.А., Перевалов Д.В., Тепляков А.А., Титлов Д.В. / Ин-т нац. безопасности Респ. Беларусь; рук. задания Д.В. Перевалов. – Минск, 2013. – 677 с. – Инв. №№ 111920, 111921, 112174. – С. 271–272.

- 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.

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[94]. 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:

1) оценка достаточности реализуемых мер обеспечения безопасности КВО ИКИ;

2) 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;

3) определения порядка введения в действие соответствующих типовых планов;

4) определение порядка взаимодействия с уполномоченными государственными органами и организациями, иными субъектами обеспечения безопасности КВО ИКИ.

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

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. В состав такого центра должен входить Национальный центр реагирования на компьютерные инциденты.

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

Уполномоченными государственными органами в области безопасности КВО ИКИ осуществляется внешний контроль безопасного функционирования таких объектов в

---

[94] Там же. – С. 271.

целях определения соответствия их функциональных характеристик требованиям, установленным законодательством в области безопасности КВО ИКИ.

Внешний контроль осуществляется соответствующими уполномоченными государственными органами 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 выявления по результатам контроля безопасного функционирования КВО ИКИ нарушений законодательства в области обеспечения безопасности КВО ИКИ виновные лица могут быть привлечены к установленным видам ответственности в соответствии с действующим законодательством.

5.5. Модельное регулирование административных процедур, осуществляемых уполномоченными органами в сфере обеспечения информационной безопасности

В соответствии с Межгосударственной программой совместных мер борьбы с преступностью на 2014-2018 г. (утвержденной решением Совета глав государств СНГ) коллективом российских и белорусских учёных был разработан Модельный регламент административных процедур, осуществляемых уполномоченными органами в сфере обеспечения информационной безопасности государств – участников СНГ. Этот межгосударственный документ был принят МПА СНГ на её 41-м заседании (постановление от 28.11.2014 № 41-17)[95].

Разработка Модельного регламента велась с учётом положений национального законодательства государств – участников СНГ. При его подготовке непосредственно использовались также основополагающие положения межгосударственных актов, принятых МПА СНГ: Модельного Информационного кодекса для государств – участников СНГ (2008 и 2012), Модельных законов «Об информатизации, информации и защите информации» (2005), «О международном информационном обмене» (2002), Рекомендаций по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности (2012), а также проекта разрабатывавшегося в тот период Модельного закона «О критически важных объектах информационно-коммуникационной инфраструктуры».

[95] Информационный бюллетень МПА СНГ. – 2015, № 62. Часть 2. – С. 145-151.

Необходимость разработки регламента обусловлена следующими факторами:

- ✓ ростом числа КВО в системе объектов ИКИ государств – участников СНГ;
- ✓ целесообразностью формализации механизма реализаций полномочий государственных органов и заинтересованных субъектов в данной сфере;
- ✓ отсутствием в большинстве государств – участников СНГ нормативно закреплённых основ деятельности по обеспечению нормального функционирования КВО ИКИ;
- ✓ важностью установления общих подходов к содержанию административных процедур, перечню органов их осуществляющих и ожидаемых результатов их реализации.

Целью разработки регламента являлось формирование механизма реализации полномочий государственных органов, прав и законных интересов субъектов, действующих в сфере эксплуатации КВО и ответственных за обеспечение информационной безопасности и нормального функционирования КВО ИКИ.

Основные задачи разработки были сформулированы следующим образом:

- установление единого подхода к перечню административных процедур и уровней их реализации, с учетом основных положений законодательства в области безопасности КВО ИКИ 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 КВО и особенностей ИКИ в государствах – участниках СНГ;
- разработка единой и скоординированной системы правовых, организационных, инженерно-технических, программно-аппаратных и специальных мер безопасности КВО ИКИ в государствах – участниках СНГ, обеспечения безопасного ввода в эксплуатацию, безопасной эксплуатации и безопасного вывода из эксплуатации соответствующих объектов;
- определение органа, уполномоченного на проведение административной процедуры и сроков ее осуществления.

Предметом правового регулирования в рамках обсуждаемого регламента явились правовые и организационно-управленческие отношения и действия, связанные с формированием механизма реализации полномочий государственных органов, а также прав и законных интересов заинтересованных субъектов в сфере эксплуатации КВО.

Принятие проекта регламента позволило создать эффективный организационно-правовой механизм реализации полномочий государственных органов в сфере эксплуатации КВО, обеспечивающий формирование и развитие системы обеспечения безопасности КВО ИКИ и 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.

Модельный регламент административных процедур, осуществляемых уполномоченными органами в сфере обеспечения информационной безопасности государств – участников СНГ, структурно состоит из общих положений, в которых определяются подходы к формированию системы КВО ИКИ, и переченя конкретных административных процедур, которые необходимо осуществлять соответствующим уполномоченным государственным органам при обеспечении безопасности КВО ИКИ.

Модельный регламент определяет:

- уровень проводимой административной процедуры;
- перечень документов и (или) сведений, представляемых в уполномоченный орган для осуществления административной процедуры;
- перечень операций, проводимых в рамках административной процедуры;
- срок осуществления административной процедуры;
- её ожидаемый результат.

Представленный в регламенте концептуальный подход может быть реализован при осуществлении административных процедур в отношении различных объектов ИКИ, обеспечивающих информационную безопасность государства, а также при реализации полномочий государственных органов в сфере информационной безопасности (например, в сфере внешнего контроля (аудита) защищенности объектов ИКИ). Естественно, что ключевой административной процедурой в рассматриваемой области является практическая реализация комплекса мер по обеспечению информационной безопасности объектов ИКИ, требующая системного подхода.

* * *

ГЛАВА 6. СОВЕРШЕНСТВОВАНИЕ И ГАРМОНИЗАЦИЯ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ЭКСПЛУАТАЦИИ ОТКРЫТЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ ДЛЯ ПРЕДУПРЕЖДЕНИЯ ИХ ИСПОЛЬЗОВАНИЯ В ТЕРРОРИСТИЧЕСКИХ И ИНЫХ ПРОТИВОПРАВНЫХ ЦЕЛЯХ

6.1. Необходимость совершенствования и гармонизации национального законодательства в сфере эксплуатации открытых телекоммуникационных сетей для предупреждения их использования в террористических и иных противоправных целях

Необходимость совершенствования и гармонизации национального законодательства государств – участников СНГ в сфере эксплуатации открытых телекоммуникационных систем (ОТКС), для предупреждения их использования в террористических и иных противоправных целях, обусловлена рядом факторов.

Прежде всего, необходимо отметить, что современное общество характеризуется дальнейшим развитием процессов глобализации, возрастающим влиянием новых информационно-коммуникационных технологий на все сферы общественной жизни.

Информационным ресурсам, размещённым в открытых телекоммуникационных системах, присущи характерные особенности, во многом нивелирующие их доступность и анонимность, затрудняющие возможности контроля и др. Всё это позволяет террористам, террористическим группам или иным подобным организациям модифицировать классические формы террористической деятельности, и создаёт возможность использования их для осуществления преступлений террористического характера и иных противоправных проявлений, способных угрожать целостности государств и дестабилизировать международную обстановку.

Особенностью современного терроризма является активное использование им как информационно-психологического воздействия, являющегося важным элементом манипулирования сознанием и поведением людей, так и информационно-технического воздействия на отдельные элементы информационно-телекоммуникационной инфраструктуры государств, с целью нанесения им ущерба, а также их подавления и (или) уничтожения. Новейшие информационные технологии и ОТКС всё чаще используются террористами, террористическими группами или организациями для пропаганды, обмена информацией, привлечения финансовых ресурсов, планирования и осуществления актов терроризма.

В условиях современного глобального мира проблема предотвращения использования ОТКС в террористических и иных противоправных целях может быть решена государствами – участниками СНГ путём применения комплекса мер, принимаемых как каждым государством самостоятельно, так коллективно в рамках Содружества. Для этой цели может быть задействован широкий спектр сил, средств и методов противодействия со стороны государства и общества.

Важное место в ряду таких методов и средств занимают выработка и использование в законодательстве и юридической практике стран Содружества общих правовых подходов, применяемых в области правового регулирования использования ОТКС, что и определяет актуальность разработки соответствующих Рекомендаций.

Законодательство государств – участников СНГ в области эксплуатации ОТКС, для предупреждения их использования в террористических и иных противоправных целях, должно основываться на конституциях своих государств, общепризнанных принципах и нормах международного права, международных договорах государства и включать в себя национальные нормативные правовые акты, содержащие соответствующие положения отраслевого законодательства.

В настоящее время национальное законодательство стран Содружества в рассматриваемой области в целом является недостаточно совершенным (или практически отсутствует). Оно базируется на различных подходах к правовому регулированию использования ОТКС, недостаточно гармонизировано с основополагающими международными документами.

В свете обсуждаемой проблемы основными недостатками существующих сегодня национальных законодательств являются:

- ✓ отсутствие целостного правового механизма по предупреждению и пресечению использования ОТКС в террористических и иных противоправных целях (отсутствуют специальные акты законодательства в данной области);
- ✓ наличие разночтений в законодательно закреплённом понятийном аппарате (в терминах, используемых в национальных нормативных правовых актах, и их определениях);
- ✓ отсутствие эффективных правовых механизмов межведомственной координации деятельности государственных органов и иных организаций по предупреждению использования ОТКС в террористических и иных противоправных целях, а также чёткого разграничения полномочий и ответственности субъектов, реализующих указанную деятельность (специальные международные правовые акты в данной области не приняты);
- ✓ несогласованность ряда норм национальных нормативных правовых актов в области правового регулирования эксплуатации ОТКС с правовыми предписаниями, регламентирующими деятельность государственных органов в других областях обеспечения безопасности и государственного управления.

6.2. Структура Рекомендаций по правовому регулированию эксплуатации ОТКС для предупреждения их использования в террористических и иных противоправных целях

Определение направлений по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере эксплуатации ОТКС с целью предупреждения их использования в террористических и иных противоправных целях предусматривалось Программой сотрудничества государств – участников Содружества Независимых Государств в борьбе с терроризмом и иными насильственными проявлениями экстремизма на 2011–2013 гг. и Перспективным планом модельного законотворчества в СНГ на 2011–2015 годы. В соответствии с указанным Перспективным планом, с учётом положений международных правовых актов и рекомендаций международных организаций по вопросам совершенствования правового регулирования в этой области, коллективом российских и белорусских учёных разработаны Рекомендации по правовому регулированию эксплуатации открытых телекоммуникационных сетей для предупреждения их использования в

террористических и иных противоправных целях, принятые МПА СНГ (постановление от 29.11.2013 № 39-25)[96].

Текст Рекомендаций включает шесть разделов, ниже приводится их краткая характеристика.

В разделе «Общие положения» обоснованы актуальность и указаны правовые основания разработки Рекомендаций.

Второй раздел документа характеризует цели и задачи совершенствования законодательства в области предупреждения использования ОТКС в противоправных целях. Целью совершенствования правового регулирования эксплуатации ОТКС государствами – участниками СНГ, для предупреждения их использования в террористических и иных противоправных целях, является создание необходимых условий для реализации конституционных прав и свобод граждан стран Содружества в информационной сфере, устойчивого развития информационного общества, обеспечения защищенности национальных интересов всех государств – участников СНГ в информационной области.

Третий раздел Рекомендаций, озаглавленный «Принципы совершенствования правового регулирования эксплуатации ОТКС», определяет такие принципы:

1) соблюдение норм международного права и выполнение международных обязательств;

2) рациональное разграничение компетенции государственных органов различного уровня и иных организаций, действующих в рассматриваемой области, совершенствование их координации и взаимодействия;

3) установление и соблюдение государственных стандартов, включающих комплекс гарантий, ограничений и запретов в приоритетных сферах правового регулирования эксплуатации ОТКС для предупреждения их использования в террористических и иных противоправных целях;

4) соразмерность временно вводимых ограничений прав и свобод человека, применяемых в связи с ограничением права на получение и распространение информации, характеру и уровню связанных с ними угроз;

5) криминализация общественно опасных деяний (преступлений), связанных с использованием ОТКС в террористических и иных противоправных целях; установление адекватных мер административной и дисциплинарной ответственности за административные правонарушения и дисциплинарные проступки; обеспечение неотвратимости наказания;

6) приоритет мер профилактического характера для предупреждения использования ОТКС в террористических и иных противоправных целях; в их числе меры, направленных на повышение эффективности деятельности и авторитета власти, оздоровление социально-психологической обстановки в обществе.

Приоритетные направления правового регулирования эксплуатации ОТКС с целью предупреждения их использования в террористических и иных противоправных целях изложены в четвёртом разделе Рекомендаций.

Содержание пятого раздела охватывают первоочередные меры по совершенствованию правового регулирования эксплуатации ОТКС для предупреждения их использования в террористических и иных противоправных целях.

---

[96] Информационный бюллетень МПА СНГ. – 2014, № 60. Часть 2. – С. 459.

Заключительный шестой раздел Рекомендаций содержит перечень отдельных организационно-методических решений по их реализации.

6.3. Приоритетные направления и основные меры правового регулирования эксплуатации ОТКС для предупреждения их использования в террористических и иных противоправных целях

Закрепление основных направлений правового регулирования эксплуатации ОТКС в государствах – участниках СНГ, для предупреждения их использования в террористических и иных противоправных целях, должно обеспечивать:

- определение рисков, источников угроз, угроз в рассматриваемой области и их видов, раскрытие их характера;
- определение деяний, признаваемых правонарушениями в рассматриваемой области;
- выявление и последующее устранение причин и условий, способствующих использованию ОТКС в террористических и иных противоправных целях;
- предупреждение распространения террористических и иных противоправных информационных материалов с использованием ОТКС;
- предупреждение и пресечение деяний, направленных на нанесение ущерба отдельным физическим элементам ОТКС, осуществляемых в террористических и иных противоправных целях;
- недопущение использования ОТКС для создания помех, реализации специальных программ, стимулирующих разрушение систем управления, или, наоборот, для получения внешнего управления техническими объектами в террористических и иных противоправных целях;
- предотвращение уничтожения или активного подавления линий связи, искусственной перегрузки узлов коммутации, осуществляемых в террористических и иных противоправных целях и т.д.;
- выявление и пресечение террористической и иной противоправной деятельности общественных объединений, религиозных и иных организаций, физических лиц, осуществляемой с использованием ОТКС.

Приоритетные направления совершенствования и гармонизации национального законодательства государств – участников СНГ в сфере эксплуатации ОТКС, в соответствии с общепризнанными принципами и нормами международного права, предусматривают определение понятийного аппарата, используемого при правовом регулировании эксплуатации ОТКС в указанных целях. При этом представляется необходимым принимать во внимание основные формы и характер использования ОТКС в террористических и иных противоправных целях на территориях государств – участников СНГ. При разработке конкретных международных и национальных нормативных правовых актов настоятельно необходимо обеспечить ориентацию всех участников на использование единого понятийного аппарата.

Одним из важнейших аспектов в данной работе является уточнение закрепляемых в национальном законодательстве стран Содружества положений, предусматривающих перечни правонарушений в области эксплуатации ОТКС. Соответствующую разработку и доработку законодательных актов в данной области целесообразно осуществлять с учётом отличительных признаков конкретных действий по использованию ОТКС в террористических и иных противоправных целях, позволяющих идентифицировать их и

выделить из спектра сходных по объективной стороне преступлений и правонарушений. Это является необходимым условием повышения эффективности правоприменительной деятельности по предупреждению и пресечению террористической и иной противоправной деятельности в ОТКС.

Требуют разработки и закрепления в специализированных нормативных правовых актах или в отдельных правовых нормах следующие направления деятельности компетентных государственных органов в области эксплуатации ОТКС для предупреждения их использования в террористических и иных противоправных целях:

- мониторинг информационных ресурсов, размещённых в ОТКС, на предмет содержания в них террористических и иных противоправных материалов;
- мониторинг ОТКС на предмет выявления признаков правонарушений, в том числе преступлений, которые признаны как использование ОТКС в террористических и иных противоправных целях;
- определение характера и пределов реализации мер, направленных на пресечение указанных правонарушений, в том числе, преступлений;
- определение объёма полномочий и распределение ответственности между компетентными государственными органами, которые предоставляют услуги по технологическому использованию ОТКС; осуществляют контроль за их эксплуатацией; устанавливают критерии неправомерности использования ОТКС и выносят решения о прекращении функционирования определенных ресурсов в телекоммуникационных сетях открытого пользования.

Не должно оставаться вне сферы правового регулирования эксплуатации ОТКС в государствах – участниках СНГ, для предупреждения их использования в террористических и иных противоправных целях, взаимодействие государства и общественных институтов в данной области. Наиболее эффективным при этом является оказание государственной поддержки общественным объединениям, осуществляющих деятельность по выявлению террористических и иных противоправных материалов, правонарушений, в том числе, преступлений в ОТКС и предупреждение их распространения (совершения).

В целях повышения эффективности и координации работы по предупреждению использования ОТКС в террористических и иных противоправных целях в национальном законодательстве государств – участников СНГ может быть предусмотрено создание постоянно действующих рабочих групп по осуществлению мониторинга национальных доменов ОТКС. Задачей таких групп может быть выявление держателей сайтов, провайдеров и отдельных лиц, размещающих и распространяющих материалы в противоправных целях, и выработка согласованных предложений по их нейтрализации.

В этой связи представляется очевидным, что национальное законодательство стран Содружества должно содержать положения, устанавливающие механизмы закрытия таких сайтов, ограничения доступа пользователей к ресурсам, содержащим материалы террористической и иной противоправной направленности, а также меры ответственности за их размещение в ОТКС.

Для повышения эффективности предупреждения и пресечения использования ОТКС в террористических и иных противоправных целях требуется принятие нормативных предписаний, предусматривающих создание в системе государственных экспертных учреждений института компетентной (судебной, правоохранительной, иной) экспертизы по вопросам, связанным с установлением наличия в тех или иных действиях

признаков правонарушений, в том числе, преступлений, при использовании ОТКС в террористических и иных противоправных целях. В качестве одного из возможных решений этого вопроса целесообразно предусматривать создание при органах исполнительной власти специальных межведомственных экспертных комиссий, определение их полномочий и порядка функционирования. К компетенции таких экспертных комиссии целесообразно отнести проведение психологических, психолингвистических и других экспертиз (в том числе комплексных) на предмет квалифицированной оценки информационных, аудио- и видеоматериалов, размещенных в ОТКС, экспертиз на предмет установления признаков деяния, указывающих на использование ОТКС в террористических и иных противоправных целях.

Важным аспектом предупреждения использования ОТКС в террористических и иных противоправных целях является нормативное закрепление основных направлений международного сотрудничества в сфере правового регулирования эксплуатации ОТКС. Основными направлениями международного сотрудничества в сфере правового регулирования эксплуатации ОТКС в целях предупреждения их использования в террористических и иных противоправных целях, являются:

- проведение согласованной политики по гармонизации национального законодательства в рассматриваемой области;
- совместная работа по предотвращению и устранению причин и условий, способствующих использованию ОТКС в террористических и иных противоправных целях;
- обмен информацией по вопросам предупреждения и пресечения эксплуатации ОТКС в террористических и иных противоправных целях;
- оказание взаимной правовой, методической, технической и иной помощи;
- координация деятельности компетентных государственных органов, осуществляющих деятельность по предупреждению и пресечению использования ОТКС в террористических и иных противоправных целях;
- проведение совместных процессуальных, оперативно-розыскных и иных мероприятий по пресечению использования ОТКС в террористических и иных противоправных целях;
- сближение подходов, применяемых при принятии решений о запрете деятельности на территории государства международных и иных общественных объединений, религиозных и иных организаций, использующих ОТКС в террористических и иных противоправных целях;
- согласование позиций по реализации мер, направленных на изъятие, ликвидацию или прекращение деятельности ресурсов ОТКС, содержащих информацию террористического и иного противоправного характера и зарегистрированных за рубежом.

Необходимо обеспечить введения мер ответственности за распространение или размещение в ОТКС материалов, преследующих террористические и иные противоправные цели. За распространение или размещение в ОТКС подобных материалов граждане государства – участника СНГ, а также иностранные граждане и лица без гражданства в соответствии с национальным законодательством должны нести уголовную, административную и иную ответственность, в зависимости от тяжести совершённого деяния или наступивших последствий. В частности, необходимо установление уголовной и иных видов юридической ответственности за распространение и размещение на информационных ресурсах ОТКС материалов, преследующие такие цели, как:

- насильственное изменение основ конституционного строя, нарушение территориальной целостности и суверенитета государства;
- публичное оправдание терроризма или публичные призывы к осуществлению террористической и иной противоправной деятельности;
- разжигание социальной, расовой, национальной или религиозной вражды или розни;
- нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, этнической, религиозной или языковой принадлежности или отношения к религии;
- воспрепятствование осуществлению гражданами их избирательных прав и права на участие в референдуме или нарушение тайны голосования, соединенные с насилием либо угрозой его применения;
- воспрепятствование законной деятельности государственных органов, органов местного самоуправления, избирательных комиссий, общественных объединений, религиозных или иных организаций, должностных лиц указанных органов, комиссий, объединений или организаций, совершенное с применением насилия либо угрозой его применения;
- нанесение ущерба отдельным физическим элементам ОТКС в террористических и иных противоправных целях;
- создание помех с использованием специальных программ, стимулирующих разрушение систем управления, или, наоборот, осуществление внешнего террористического управления техническими объектами с использованием ОТКС;
- уничтожение или активное подавление линий связи, искусственная перегрузка узлов коммутации в террористических и иных противоправных целях;
- финансирование и иное содействие террористической и иной противоправной деятельности и т.д.

Для повышения эффективности деятельности компетентных государственных органов и системы мер, направленных на предупреждение и пресечение деяний по использованию ОТКС в террористических и иных противоправных целях, представляется необходимым обеспечить согласование и гармонизацию правовых норм в рамках специальных законов, в том числе, соответствующих норм уголовного законодательства стран Содружества.

Предложенный подход к решению проблем правового регулирования в области обеспечения информационной безопасности будет способствовать развитию сотрудничества государств – участников СНГ по противодействию другим вызовам и угрозам.

* * *

ГЛАВА 7. СОВЕРШЕНСТВОВАНИЕ И ГАРМОНИЗАЦИЯ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ЗАЩИТЫ ГОСУДАРСТВЕННОЙ ТАЙНЫ НА ПРОСТРАНСТВЕ ОДКБ

7.1. Основания для гармонизации правового регулирования защиты государственной тайны

Феномен государственных секретов (государственной тайны) — объективная реальность в сфере межгосударственных отношений. Посягательства на государственные тайны в развитых государствах рассматриваются как преступления против основ конституционного строя и безопасности государства. В системе обеспечения национальной и коллективной безопасности государств – членов ОДКБ защита государственной тайны представляется одной из важнейших её составляющих, призванных обеспечить гарантии обороноспособности, а также сохранение приоритета новейших научных и технологических разработок в ряде отраслей экономики.

По своей природе тайна — не простое и противоречивое социально-правовое явление. В легальной интерпретации тайна — это информация, доступ к которой ограничен. Государственная тайна — это та часть информации, которая изъята из свободного оборота. Она ограничивает конституционные права граждан, интересы в научной, экономической и иных сферах и приводит к конфликту интересов, в котором приоритет отдается интересам безопасности государства. Законодательное регулирование не может обойти сферу защиты государственной тайны, которая, хотя и отражается на степени открытости государства перед обществом, но является важным и необходимым элементом обеспечения суверенитета и безопасности государства.

Институт защиты государственной тайны привлекает внимание исследователей и общественности. Имея своей целью обеспечение безопасности государства, государственная тайна не должна препятствовать развитию экономики, росту деловой и интеллектуальной активности граждан. В силу этого недопустим расширительный подход к определению её понятия и круга относимых к ней сведений. Критерии государственной тайны должны быть понятными и приемлемыми не только для государства, но и для гражданина и общества.

За последние десятилетия появился целый ряд открытых публикаций, в том числе монографий, были успешно защищены диссертации, предметом рассмотрения в которых являются различные аспекты защиты государственной тайны. Среди вышедших в свет публикаций есть работы теоретического характера, в которых анализируется как сам феномен «тайна», так и предпринимаются попытки исследовать «тайноведческий процесс»[97]. В 2008 г. в Российской Федерации были проведены научно-практическая конференция «15 лет российскому Закону «О государственной тайне» и парламентские слушания «Законодательство о государственной тайне: вчера, сегодня, завтра», давшие полезный материал для анализа и совершенствования

[97] См., например: Рабкин, В.А. Исторический генезис правового регулирования защиты государственной тайны в России В.А. Рабкин // Информационное право. – 2006. – 4 (7). – С. 7-11; Государственная тайна и ее защита в Российской Федерации / М.А. Вус [и др.]; под ред. М.А. Вуса и А.В. Фёдорова. – СПб.: Изд-во «Юридический центр Пресс», 2007. – 3-е изд. – 752с; Рябчук, В.Н. Государственная измена и шпионаж / В.Н. Рабчук. – СПб.: Изд-во «Юридический центр Пресс», 2007. – 1102 с.; Дьяков, С.В. Преступления против основ конституционного строя и безопасности государства / С.В. Дъяков. – СПб.: Изд-во «Юридический центр Пресс», 2009. – 267 с.

действующего законодательства о защите государственной тайны. Материалы конференции и парламентских слушаний опубликованы[98].

Сравнительно-правовое исследование обеспечения защиты государственных секретов государств – членов ОДКБ позволяет на основе сопоставления различий и тождества национальных механизмов регулирования отношений в данной сфере выстроить логический ряд базовых категорий, определяющих современное состояние и векторы развития правовой защиты государственных секретов государств – членов ОДКБ:

- ✓ организационно-правовой механизм защиты секретов в том виде, в котором он существует в настоящее время в государствах – членах ОДКБ, является порождением правовой системы защиты охраняемой информации в СССР. Несмотря на изменения, связанные с развитием и особенностями национальных правовых систем, концептуальная платформа данного социально-правового института осталась прежней. Данный тезис подтверждается сходством подходов к определению понятия предмета регулирования, а также идентичностью онтологического ряда базовых категорий в сфере защиты государственных секретов;
- ✓ политические и правовые условия в государствах – членах ОДКБ, с точки зрения защиты государственных секретов, существенно не различаются. Организационно-правовой механизм защиты секретов государств – членов ОДКБ испытывает воздействие одинаковых внешних и внутренних факторов, являющихся порождением современного этапа развития общества.

Изложенное позволяет выдвинуть предположение, что в единой среде, одинаковых условиях, родственные правовые системы должны сохранить свою идентичность. Однако в реальности национальные особенности выходят за рамки погрешности, налицо тенденция к дифференциации правового регулирования защиты государственных секретов государств – членов ОДКБ. Кроме этого, просматривается глобальное снижение эффективности института государственных секретов, вызванное воздействием вышеназванных факторов (коммерциализация информации, информатизация общества и др.).

В складывающихся условиях обозрима перспектива реформирования института государственных секретов, пересмотра его места в системе обеспечения национальной безопасности, ревизии методов его обеспечения. Существует несколько вариантов выхода из сложившейся ситуации:

- заимствование концептуально-правовой платформы защиты государственных секретов (тайны) у других стран (блоков);
- выработка универсальной международной платформы защиты государственных секретов (тайны) государств – членов ОДКБ (по примеру стран НАТО);
- развитие национальных механизмов защиты государственных секретов (тайны) государств – членов ОДКБ на основе обмена методиками и опытом и, как следствие, развитие международных правовых механизмов защиты государственных секретов (тайны) в рамках ОДКБ.

---

[98] От культа секретности к информационной культуре (К 15-летию российского Закона «О государственной тайне»). – СПб.: ОНТЗ, 2006. – 116с.; Законодательство о государственной тайне: вчера, сегодня, завтра. – М.: Издание Государственной Думы, 2009. – 96с.

Последний из предложенных вариантов представляется наиболее перспективным, но он предполагает более глубокое сотрудничество.

7.2. Становление и развитие правового регулирования защиты государственной тайны

Системы защиты государственных секретов в государствах, образовавшихся на пространствах бывшего СССР, объективно имеют общие корни, происходящие от системы защиты информации, ранее имевшей место в нашей стране. Однако, как известно, законодательного определения государственной тайны ни в Российской империи, ни в СССР не было.

Первым национальным законодательным актом на постсоветском пространстве в обсуждаемой сфере стал Закон «О защите государственных секретов Республики Казахстан», принятый в 1993 г. В том же году в Российской Федерации был принят первый на постсоветском пространстве Закон «О государственной тайне» (в 1997 г. этот закон получил новую редакцию). Российский закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации. Понятие «государственная тайна» определено как «защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации». Для сведений, составляющих государственную тайну, в Российской Федерации предусмотрены три степени и три грифа секретности.

В 1994 г. были приняты Закон «О защите государственных секретов Кыргызской Республики» и первый Закон «О государственных секретах» в Республике Беларусь. Закон «О государственной и служебной тайне» (1996) был принят в Республике Армения; при этом законодатель объединил сферы правового регулирования обеспечения защиты государственной и служебной тайны (рассматривая служебную тайну как часть государственной). В том же году был принят первый национальный Закон «О государственной тайне» в Республике Таджикистан, в 2003 г. в него были внесены изменения.

Действующий сегодня в Республике Казахстан Закон «О государственных секретах» (1999) определяет правовые основы и единую систему защиты государственных секретов в интересах обеспечения национальной безопасности. При этом понятие «государственные секреты» определяются как «защищаемые государством сведения, составляющие государственную и служебную тайны, распространение которых ограничивается государством с целью осуществления эффективной военной, экономической, научно-технической, внешнеэкономической, внешнеполитической, разведывательной, контрразведывательной, оперативно-розыскной и иной деятельности, не вступающей в противоречие с общепринятыми нормами международного права». Государственная тайна — сведения военного, экономического, политического и иного характера, разглашение или утрата которых наносит или может нанести ущерб национальной безопасности Республики Казахстан. Служебная тайна — сведения, имеющие характер отдельных данных, которые могут входить в состав государственной тайны, разглашение или утрата которых может нанести ущерб национальным интересам государства, интересам государственных органов и организаций Республики Казахстан. Сведениям, составляющим государственную тайну, присваиваются грифы секретности

«особой важности», «совершенно секретно». Сведениям, составляющим служебную тайну, присваивается гриф секретности «секретно».

Законодательство в сфере защиты государственных секретов совершенствуется; за прошедшие годы в национальные законодательные акты неоднократно вносились изменения. В Республике Беларусь принят новый Закон «О государственных секретах» (2010), а в Таджикской Республике на смену ранее действовавшему Закону «О государственной тайне» пришёл новый, базирующийся уже на иной правовой модели, Закон Республики Таджикистан «О государственных секретах» (2014).

Следует, однако, отметить, что в законах всех государств – участников ОДКБ в той или иной мере определены перечни сведений, относимых к государственной тайне, что может рассматриваться как непосредственное закрепление принципа законности при построении системы правового регулирования защиты государственных тайн. Нашел свое закрепление в законодательных актах государств также и принцип обоснованности засекречивания сведений, что позволяет легализовать содержательную оценку относимости к государственной тайне конкретных сведений.

Хотя сами законодательства государств – членов ОДКБ и методологии защиты государственных секретов в этих государствах имеют общую предысторию и теоретическую базу, концептуальные подходы в ряде случаев являются оригинальными, отражающими результаты самостоятельного, на протяжении почти двух десятилетий, развития собственных правовых систем этих независимых государств. Вследствие этого в действующем сегодня законодательстве государств – членов ОДКБ существуют как отдельные концептуальные различия, так и различия в структуре элементов правового регулирования. Вместе с тем процессы, происходящие в рамках правового регулирования международного сотрудничества, носят характер упорядочивания и унификации.

Вопросам гармонизации законодательства в сфере защиты государственной тайны уделяется значительное внимание в работе МПА СНГ и ПА ОДКБ. На первом этапе развития законотворчества эти вопросы были учтены при разработке уголовно-правовых и уголовно-процессуальных модельных законодательных актов. Вопросы защиты государственной тайны нашли отражение в принятых в качестве рекомендательных законодательных актов модельном Уголовном и Уголовно-процессуальном кодексах (1996). Однако не все прогрессивные новации модельных законов нашли отражение в национальных законах, и по-прежнему обоснована постановка вопроса об их реализации в рамках развития национальных законодательств. Применительно к Российской Федерации это актуально, прежде всего, в части касающейся уголовно-процессуального законодательства. Специалисты-аналитики отмечают, например, что сегодня требуют совершенствования уголовное и уголовно-процессуальное законодательства. «*Практика сталкивается, например, с серьёзнейшей проблемой доказывания состава государственной измены, когда иностранным адресатом являются, например, экологическая организация,* благотворительный *фонд, средство массовой информации, коммерческая фирма*»[99]. Знаковым этапом международного сотрудничества стало принятие на 21-м пленарном заседании МПА СНГ Модельного закона «О государственных секретах» (постановление от 16 июня 2003 г. № 21-10)[100]. Этот Закон «определяет правовые основы и единую систему защиты

[99] Фёдоров, А.В. Гармонизация и унификация законодательства о государственной тайне в государствах – участниках содружества независимых государств / А.В. Федоров // Материалы конференции «Информационная безопасность регионов России (ИБРР-2009)». – СПб.: СПОИСУ, 2009. – С. 21-22.

[100] Информационный бюллетень МПА СНГ. – 2003. – № 31. – С. 230-261.

государственных секретов в интересах обеспечения национальной безопасности, регулирует общественные отношения, возникающие в связи с отнесением сведений к государственным секретам, их засекречиванием, распоряжением ими, защитой и рассекречиванием».[101]

Развитие сотрудничества государств – членов ОДКБ сделало актуальным вопрос о принятии решений в рамках ОДКБ по совершенствованию и гармонизации национальных законодательств о защите сведений, составляющих государственную тайну; это необходимо в целях выработки и реализации согласованной политики и совместных мер защиты таких сведений. В 2004 г. в Астане государствами – членами ОДКБ было заключено соглашение о взаимном обеспечении сохранности секретной информации в рамках ОДКБ. Рабочая группа при Совете ПА ОДКБ по вопросам унификации и гармонизации национальных законодательств, внедрению модельных законов и рекомендаций приняла в 2008 г. постановление «О разработке проекта Рекомендаций по сближению законодательства государств – членов ОДКБ по вопросам государственной тайны». Такие Рекомендации, разработанные совместно российскими и белорусскими учёными, были приняты Парламентской Ассамблеей ОДКБ в 2010 г. (постановлением ПА ОДКБ от 27.10.2010 г. № 4-7).

В настоящее время в рамках Договора о коллективной безопасности действует ряд двусторонних межправительственных соглашений о защите секретной информации. К их числу относится, например, соглашение о взаимном обеспечении защиты государственной тайны Российской Федерации и государственных секретов Республики Беларусь, которое было заключено 20 января 2003 г. в Минске. Еще ранее (2002) было подписано соглашение о защите секретной информации между Российской Федерацией и Республикой Армения. В 2003 г. аналогичные соглашения подписаны также между Российской Федерацией и Республикой Таджикистан; между Российской Федерацией и Киргизской Республикой; а в 2004 г. — между Российской Федерацией и Республикой Казахстан.

7.3. Основные направления совершенствования и гармонизации законодательства в сфере защиты государственной тайны на пространстве ОДКБ

Сближение законодательства о государственной тайне предполагает такие направления как:

- унификация терминологии, используемой в национальных законодательствах государств-членов ОДКБ,
- активизация договорного процесса между государствами с целью заключения двусторонних и многосторонних договоров по различным аспектам защиты секретной информации,
- совершенствование аналитической и научно-исследовательской деятельности,
- осуществление контроля, мониторинга и прогнозирования угроз безопасности охраняемой информации.

[101] В 2015 г. вышла в свет работа российских и белорусских учёных: Комментарий к Модельному закону МПА СНГ «О государственных секретах» / [Вус М.А., Макаров О.С.] Предисловие Р.М. Юсупова.- СПб.: СПИИРАН, 2015. – 136 с.

Базовое значение для сближения правового регулирования отношений в сфере оборота государственных секретов в государствах – членах ОДКБ сегодня несет толкование основных понятий. Это можно проиллюстрировать, например, обратившись к сравнительному анализу ныне действующих базовых законов России и Беларуси. Сегодня основы отношений в сфере защиты государственных секретов у партнеров по Союзному государству регламентируются Законом Российской Федерации «О государственной тайне»[102] и Законом Республики Беларусь «О государственных секретах»[103]. Различия видны уже в самом названии базовых законов. Российское законодательство использует единое неделимое понятие: «государственная тайна», в то время как в белорусском законодательстве о государственных секретах выделены две правовые категории: «государственная тайна» и «служебная тайна». При этом, как трактует белорусский закон, «служебная тайна может являться составной частью государственной тайны, не раскрывая её в целом». Отметим, что в действующем сегодня в Российской Федерации законодательстве нет закона о служебной тайне.

Отдельные различия в понятийном аппарате и подходах к правовому регулированию можно также обнаружить, обратившись к базовым законам других государств – членов ОДКБ. В Законе Республики Казахстан «О государственных секретах», например, понятие «служебная тайна» определяется как «сведения, имеющие характер отдельных данных, которые могут входить в состав государственной тайны, разглашение или утрата которых может нанести ущерб национальным интересам государства, интересам государственных органов и организаций Республики Казахстан», а Закон «О защите государственных секретов Кыргызской Республики» к служебной тайне относит информацию, разглашение которой может оказать «отрицательное воздействие на обороноспособность, безопасность, экономические и политические интересы государства».[104] В Модельном же законе МПА СНГ это понятие определено как «сведения в сферах деятельности государственных органов, доступ к которым ограничивается служебной необходимостью, разглашение или утрата которых может нанести ущерб государственным органам или государству»..[105] Все вышесказанное только подчеркивает необходимость актуализации внимания к вопросам совершенствования и гармонизации законодательства о защите государственной тайны.

Разработка предложений по совершенствованию и гармонизации законодательства о защите государственной тайны для государств – членов ОДКБ потребовала осмысления современного состояния и систематизации понятийного аппарата в сфере защиты государственной тайны (в более общем случае — в сфере информационной безопасности). В рамках совместной работы, начатой российскими и белорусскими коллегами, подготовлен Глоссарий (словарь) базовых терминов, толкование которых закреплено юридически в законодательных актах государств – участников ОДКБ. Представляется, что такой материал будет полезен в повседневной работе руководителям всех уровней как справочное практическое пособие. При разработке нормативной основы, и особенно, в международных договорах и соглашениях принципиально важно грамотное толкование и использование терминов и понятий.

---

[102] О государственной тайне: Федеральный закон Российской Федерации, 21 июля 1993 г., № 5485-1 (ред. от 01.12.2007 с изм. и доп.) // Собрание законодательства РФ. – 1997. – № 41. – С. 8220-8235.

[103] О государственных секретах: Закон Республики Беларусь, 04 янв. 2003 г., № 172–З // Нац. реестр правовых актов Респ. Беларусь. – 2003. – № 8. – 2/921.

[104] Глоссарий основных понятий в законодательстве о государственной тайне государств – членов ОДКБ. – СПб.: СПИИРАН, 2011. С. 64.

[105] Комментарий к Модельному закону МПА СНГ «О государственных секретах» / М.А. Вус, О.С. Макаров . Предисловие Р.М. Юсупова . – СПб.: СПИИРАН, 2015. – 136 с.

Государственная тайна — это межотраслевой правовой институт. Поэтому правовое регулирование оборота государственной тайны должно быть комплексным, т.е. осуществляться нормами различных отраслей права. При этом вопросы разрешения противоречий между правом на информацию и необходимыми его ограничениями, в целях обеспечения баланса интересов субъектов информационных отношений, становятся все более сложными и комплексными.

В целях совершенствования механизмов правового регулирования отношений в области государственных секретов, а также унификации профильного законодательства государств – членов ОДКБ целесообразно наладить сотрудничество в вопросах изучения наработанного в независимых государствах опыта и его взаимное заимствование.

В качестве одного из приоритетных направлений совершенствования и гармонизации законодательства в сфере защиты государственной тайны на пространстве ОДКБ представляется выделение наиболее опасных правонарушений в области государственных секретов, что предполагает перманентный обмен информацией о выявленных и устраненных уязвимостях систем защиты данных информационных ресурсов и типичных инцидентах.

* * *

ЧАСТЬ III. СТРАТЕГИЧЕСКИЙ ВЕКТОР ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРОСТРАНСТВЕ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

==========

ГЛАВА 8. О СТРАТЕГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ГОСУДАРСТВ – УЧАСТНИКОВ СНГ

8.1. Предпосылки для разработки Стратегии информационной безопасности

Научная и нормотворческая активность в области обеспечения международной информационной безопасности имеет исторический задел и тенденцию к нарастанию. В 2008 г. Советом глав правительств СНГ утверждена Концепция сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности, представляющая согласованную совокупность официальных взглядов и положений о целях, принципах и основных направлениях межгосударственного сотрудничества в сфере обеспечения информационной безопасности. В 2012 г. Советом глав правительств СНГ утверждена Стратегия сотрудничества государств – участников СНГ в построении и развитии информационного общества, отражающая общее видение путей построения информационного общества. Одним из основных направлений сотрудничества в этом документе определена гармонизация законодательства и нормативно-технической базы в области информационно-коммуникационных технологий. Отдельным направлением обозначена проблема обеспечения информационной безопасности.

Современный период развития правового регулирования обеспечения информационной безопасности характеризуется прорывным скачком в построении системы международного законодательства. В последнее время наблюдается активность в правовом обеспечении международной информационной безопасности уже на уровне документов прямого действия. Так, например, в 2014 г. ратифицировано Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности[106], а в 2015 г. — Соглашение между Правительством Республики Беларусь и Правительством Российской Федерации о сотрудничестве в области обеспечения международной информационной безопасности[107].

В результате формируется альтернатива «западному подходу», рассматривающему информационную безопасность только как защиту от преступных посягательств на информационные ресурсы и инфраструктуру и при этом, не желающему видеть в правовом поле информационное воздействие на психику человека, его духовные

---

[106] Закон Республики Беларусь № 179-З 14.07.2014 О ратификации Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в области обеспечения информационной безопасности

[107] Закон Республики Беларусь № 234-З 04.01.2015 «О ратификации Соглашения между Правительством Республики Беларусь и Правительством Российской Федерации о сотрудничестве в области обеспечения международной информационной безопасности».

ценности, настойчиво ведется работа по переводу информационного противоборства из военной сферы в правоохранительную. Государствами Содружества предпринимаются усилия, направленные на введение международного запрета на применение информационного оружия. Продолжается работа по преодолению позиций Будапештской конвенции, позволяющих вмешиваться в суверенитет других государств. Задекларирована и проходит апробацию инициатива введения понятия «информационный суверенитет», на сегодняшний день ведется работа по внедрению данного подхода в систему правовых воззрений союзников. Продвигается позиция, согласно которой информационная безопасность является состоянием, достигаемым только симметричной защищенностью совокупности прав и интересов субъектов, как в плане обеспечения защиты информационных ресурсов, инфраструктуры, технологий, так и в аспекте защиты конституционного строя, устоев общества, культурных ценностей, нравственности, морали, психического здоровья человека.

В русле данных тенденций по заказу МПА СНГ интернациональным коллективом ученых, включающим представителей ФГБУН «Институт государства и права Российской академии наук», ФГБУН «Санкт-Петербургский институт информатики и автоматизации Российской академии наук», ГУО «Институт национальной безопасности Республики Беларусь», ГУО «Академия милиции МВД Республики Беларусь», а также УО «Центр повышения квалификации руководящих работников и специалистов «Центр специальной подготовки» (Республика Беларусь) разработан проект Стратегии обеспечения информационной безопасности государств – участников Содружества Независимых Государств, который был одобрен на 41-м пленарном заседании МПА СНГ (постановление от 28.11.2014 г. № 41-13). [Приложение].

Значение подготовленной Стратегии обеспечения информационной безопасности государств – участников СНГ (далее по тексту — Стратегия) состоит в том, что этот документ представляет платформу для дальнейшего развития исследований и решения проблем укрепления информационной безопасности на пространстве взаимодействия государств – участников Содружества.

Сегодня актуальность этого стратегического документа возрастает в связи с переходом к новому этапу развития информационного общества, расширением информационного обмена между государствами – участниками СНГ, а также с развитием других многосторонних форм международного взаимодействия в области использования потенциала ИКТ в целях сохранения мира и прогрессивного развития социума.

Ожидания от реализации данной Стратегии связаны с возможностью использования опыта СНГ в процессе формирования правовой, организационной и технологической основ обеспечения информационной безопасности. Как представляется, это может быть особенно важно для новых международных ассоциаций (таких как ЕАЭС, БРИКС) в условиях нарастающих угроз в области информационной безопасности вследствие имеющего место внешнего агрессивного, вредного для общества и разрушительного информационного взаимодействия с использованием ИКТ и Интернет-среды.

Разработка проекта Стратегии была обусловлена:

- ✓ актуальностью дальнейшего развития системы организационно-правовых мер обеспечения информационной безопасности государств – участников СНГ и перехода от концептуально-доктринального определения теоретических основ

информационной безопасности к стратегическому планированию направлений достижения приемлемого (заданного) уровня информационной безопасности[108];

- ✓ необходимостью охраны и защиты информационных интересов национальных государств – участников СНГ и Содружества в целом в контексте динамичного изменения геополитической обстановки и возникновения новых угроз информационному развитию и государственному суверенитету, расширения спектра информационных угроз, реализующихся в экономической, политической, социальной, научно-технологической, военной и иных сферах;
- ✓ необходимостью унификации подходов к защите информации, защите информационных прав и интересов и формированию безопасной информационной среды в рамках комплексных интегрированных статусов информационной безопасности личности, общества и государства;
- ✓ важностью международной интеграции законодательства государств – участников СНГ в сфере информационной безопасности, согласования подходов правового регулирования национального и модельного законодательства;
- ✓ значимостью правового и организационного обеспечения реализации национальных стратегий и планов развития информационного общества;
- ✓ необходимостью обеспечения должной реализации конституционных прав граждан и гарантий по созданию условий для свободного и достойного информационного развития личности;
- ✓ потребностью повышения эффективности деятельности государственных органов, связанной с обеспечением информационной безопасности личности, общества и государства.

При подготовке проекта Стратегии её разработчики ставили перед собой следующие задачи:

1) определить предметные сферы обеспечения информационной безопасности, предложить рабочее определение понятия «обеспечение информационной безопасности»; нацелить обеспечение информационной безопасности на создание условий сотрудничества при создании единого экономического и таможенного пространства; выделить обеспечение безопасного информационного взаимодействия в социальной сфере СНГ;

2) при формулировании целей Стратегии необходимо было определить интересы государств – участников СНГ на уровне Содружества (в сфере коллективного взаимодействия) и проанализировать основания государственной информационной политики каждого государства в области обеспечения информационной безопасности в целях поиска путей обеспечения согласованного взаимодействия в определенных предметных сферах правового регулирования; выработать скоординированные представления и предложения по укреплению международного сотрудничества в области обеспечения информационной безопасности;

3) определить методы и средства гармонизации законодательства и направления практических действий по обеспечению информационной безопасности, с учетом специфики предметных областей обеспечения безопасности информационного пространства СНГ и в свете решения задач по формированию единого экономического, таможенного и определенных участков единого социального и культурного пространства Содружества;

---

[108] Ясенев, В.Н. Информационная безопасность в экономических системах: учебное пособие / В.Н. Ясенев. – Н.Новгород: Изд-во ННГУ, 2006. – С. 33.

4) сформулировать принципы, на которых государства – участники СНГ включаются в глобальные и международные сетевые системы и своими усилиями и средствами готовы их реализовывать в интересах всего Содружества и каждого государства – участника СНГ в отдельности, при соблюдении условий обеспечения информационной безопасности.

Работа по формированию проекта Стратегии предусматривала следующие этапы:

- выработка (согласование) понятийного аппарата. Определение структурно-необходимого минимума критериев, образующих информационную безопасность, и закрепление этих позиций в Стратегии;
- обоснование основных интересов на уровне Содружества, в сфере коллективного взаимодействия (С учётом того обстоятельства, что система отношений по обеспечению информационной безопасности вторична по отношению к базовым системам экономических, политических и социальных отношений, представилось целесообразным построение системы информационной безопасности коррелировать с векторами развития базовых систем);
- построение матрицы глобальных угроз (При построении матрицы угроз разработчики исходили из их градации на угрозы базовым интересам и угрозы способам их реализации в информационной сфере.);
- определение механизмов противодействия угрозам.

8.2. Концептуальный подход к разработке Стратегии информационной безопасности

В состав предметной области, охватываемой замыслом Стратегии, разработчиками её проекта были отнесены следующие проблемы:

а) в организационно-управленческой области:

- требования к безопасности деятельности всех структур массовых коммуникаций с учетом расширения зон сотрудничества государств –участников СНГ;
- установление и соблюдение правил открытости и безопасности сферы массовой информации;
- создание центров открытого доступа к информационным справочным системам во всех странах СНГ;
- соблюдение порядка обработки и использования персональных данных, а также других категорий информации в режиме ограниченного доступа;
- согласование порядка установления и оценки состояния национальных факторов, затрудняющих реализацию сотрудничества в области обеспечения информационной безопасности;
- организация системы учета угроз регулярному порядку взаимодействия в области обеспечения информационной безопасности в рамках СНГ;
- организация и согласование компетенций рабочих органов государств –участников СНГ в области обеспечения информационной безопасности;

б) в организационно-технической области:

- установление состава автоматизированных систем управления и информационных систем, действующих в масштабе СНГ и отдельных его государств – участников;

- установление порядка согласования требований к безопасности программного обеспечения информационного взаимодействия в пространстве СНГ;
- установление и соблюдение порядка обеспечения информационной безопасности при трансграничных отношениях бизнес-структур и их партнерства независимо от формы собственности на основе соблюдения правил применения электронных документов и электронной подписи;
- установление порядка ведения регистров нарушений правил обеспечения информационной безопасности в рамках сотрудничества государств-участников СНГ;

в) в области борьбы с правонарушениями в информационной сфере:

- согласование методик противодействия и борьбы с экстремизмом, коррупцией и киберпреступностью в рамках информационных пространств государств – участников СНГ;
- согласование порядка рассмотрения судебных споров, возникающих в области обеспечения информационной безопасности;
- создание и публикация сравнительных справочных материалов по реестрам информационного законодательства государств – участников СНГ; публикация материалов о состоянии законодательства, его нарушениях в рамках информационного пространства СНГ, а также в Интернет-сегментах государств – участников; публикация материалов о состоянии информационной безопасности в зонах информационного сотрудничества и обеспечения информационной безопасности на пространстве СНГ.

Стратегия концептуально отвечает следующим требованиям:

- ✓ предусматривает поступательное устойчивое развитие информационных отношений государств − участников СНГ;
- ✓ её положения нацелены на воспрепятствование реализации угроз интересам государств − участников СНГ в информационной сфере;
- ✓ программирует способность базовых систем экономических, политических, социальных и иных отношений государств − участников СНГ противостоять информационным угрозам и их готовность к противодействию такого рода угрозам.

Правовая основа разработанного проекта Стратегии опирается на фундаментальные базовые положения активно развивающейся новой отрасли права — «Информационное право». Методическая основа базируется на концептуальных положениях заключённых государствами – участниками Содружества договоров и соглашений и на национальных концепциях безопасности.

Нормативную базу проекта Стратегии составляют Конституции стран Содружества, общепризнанные принципы и нормы международного права, международные договоры государств – участников СНГ, стратегии, концепции и доктрины развития информационного общества, национальное законодательство государств – участников СНГ, регулирующее вопросы формирования и развития системы обеспечения национальной и информационной безопасности.

Разработанный и одобренный МПА СНГ проект документа (Стратегия) отражает согласованную «…*совокупность официально принятых государствами взглядов на состояние, цели, задачи, основные направления и первоочередные мероприятия по*

дальнейшему развитию системы обеспечения информационной безопасности»[109]. Названный документ создает методологическую основу согласования деятельности государств в области совершенствования организационного и правового обеспечения информационной безопасности Содружества и может быть использован при планировании деятельности по обеспечению информационной безопасности государств – участников СНГ.

Целью Стратегии является выработка и правовое закрепление концептуальных подходов к определению согласованных приоритетов обеспечения безопасности складывающихся общественных отношений в информационной сфере, определение актуальных направлений обеспечения информационной безопасности, форм и методов ее обеспечения.

Предметом Стратегии выступают общественные отношения, складывающиеся в сфере обеспечения информационной безопасности по следующим основным направлениям[110]:

- соблюдение конституционных прав и свобод человека и гражданина в области сбора, обработки, хранения и распоряжения информацией;
- совершенствование информационного обеспечения и развития гражданского общества государств – участников и Содружества в целом;
- достижение заданного уровня информационного обеспечения реализации согласованной политики государств – участников;
- совершенствование информационного обеспечения международного сотрудничества;
- совершенствование информационного обеспечения инновационного развития Содружества Независимых Государств;
- совершенствование информационной инфраструктуры национальных государств – участников СНГ и Содружества в целом, обеспечение её безопасности;
- обеспечение информационного развития национальных экономик;
- обеспечение безопасности критически важных объектов информационно-телекоммуникационной инфраструктуры государств – участников СНГ и Содружества в целом;
- защита государственных секретов и противодействие иностранным техническим разведкам.

Структурными компонентами Стратегии являются:

- ✓ официальные взгляды на проблему информационной безопасности и цели её обеспечения, закрепленные в профильных концепциях и доктринах информационного развития государств Содружества;
- ✓ методики и методы обеспечения безопасности, закрепленные в концепциях обеспечения безопасности;
- ✓ субъекты отношений информационной безопасности (Государство является системообразующим субъектом обеспечения информационной безопасности, реализующим стратегические задачи посредством осуществления

[109] Концепция совершенствования правового обеспечения информационной безопасности Российской Федерации: проект. – Режим доступа: http://www.agentura.ru/dossier/russia/sovbez/docs/concept/. – Дата доступа: 22.09.2015.

[110] Закреплены в Рекомендациях по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности (приняты на 38 пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ (постановление от 23 ноября 2012 № 38-20).

государственного управления в рамках соответствующей государственной политики.);[111]

- ✓ силы и средства, служащие обеспечению видов безопасности;
- ✓ интересы личности, общества и государства как объекты информационной безопасности;
- ✓ обобщённая информация, дающая представление об опасностях и угрозах интересам личности, общества и государства и об источниках этих угроз;
- ✓ алгоритмы деятельности по обеспечению информационной безопасности и ее прогнозные результаты.

Основным правовым средством согласования, гармонизации механизмов регулирования информационных отношений, в соответствии с обсуждаемой Стратегией, представляется объединение правового регулирования по выделенным направлениям в единый правовой статус (личности, общества и государства).

В качестве правового информационного статуса государства Стратегия определяет информационный суверенитет, достижение и поддержание которого должно обеспечить исключительное право государства в соответствии с национальным законодательством и нормами международного права самостоятельно и независимо, с соблюдением баланса интересов объектов безопасности, определять и реализовывать национальные интересы в информационной сфере, проводить внутреннюю и внешнюю государственную информационную политику, распоряжаться собственными информационными ресурсами; формировать инфраструктуру национального информационного пространства, создавать условия для интеграции в мировое информационное пространство.

В настоящее время вопросы формирования активной согласованной информационной политики государств – участников СНГ, развития общего информационного пространства, создания совместного потенциала по противодействию информационным угрозам правам и свободам граждан и интересам государства и общества, защищенности информационных ресурсов и коммуникаций национальных органов власти и управления приобретают особую актуальность. Одобрение МПА СНГ проекта рассматриваемой Стратегии придало данным усилиям новый импульс, обозначило вектор их приложения, сформировало цели реализации.

8.3. О перспективах реализации Стратегии

После прохождения процедур парламентской экспертизы и межпарламентского согласования разработанный коллективом российских и белоруских учёных проект Стратегии обеспечения информационной безопасности государств – участников Содружества Независимых Государств был одобрен Межпарламентской Ассамблеей и направлен в Исполнительный комитет Содружства Независимых Государств для рассмотрения в установленном порядке. (постановление от 28.11.2014 г. № 41–13)[112]

В 2014 – 2016 гг. рассмотрение Стратегии проходило в рабочих органах Экономического совета и Исполнительного комитета СНГ.

---

[111] Основным институциональным элементом взаимодействия в Стратегии являются субъекты. В стратегиях обеспечения безопасности, в отличие от программ и доктрин развития, градация субъектов осуществляется не по правовому статусу, а по иерархии подчинения: субъекты управления процессами безопасности, субъекты обеспечения безопасности, субъекты исполнения решений. (*авт.*)

[112] Информационный бюллетень МПА СНГ. – 2015, № 62. Часть 2. – С. 27-28.

Экспертная группа Исполкома СНГ учла замечания, поступившие от ряда государств Содружества, доработала документ и согласовала его (май 2015 г.). Экономический совет СНГ предложил Исполнительному комитету совместно с Межпарламентской Ассамблеей СНГ доработать Стратегию и внести её окончательный вариант на рассмотрение Совета министров иностранных дел СНГ. Созданная под эгидой Исполнительного комитета СНГ экспертная группа ещё раз доработала документ. В мае 2016 г. его проект был направлен в Совет постоянных полномочных представителей государств - участников Содружества при уставных и других органах Содружества для включения вопроса о рассмотрении Стратегии в повестку дня очередного заседания Совета министров иностранных дел стран СНГ

С момента одобрения МПА СНГ проекта Стратегии прошло два года, однако вопрос внедрения данной разработки в практику международного взаимодействия государств – участников СНГ и сегодня остаётся актуальным. Возрастающие темпы формирования информационного общества и ускоряющаяся динамика развития информационных отношений настойчиво требуют активизации разработки и практического внедрения концептуальных и правовые основы информационной безопасности. В этой связи представляется, что длительность процесса принятия обсуждаемой Стратегии является сдерживающим фактором развития сотрудничества в области совершенствования международной информационной безопасности на пространстве Содружества.

* * *

ПРИЛОЖЕНИЕ:

СТРАТЕГИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВ – УЧАСТНИКОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

Проект документа представлен в его редакции, одобренной на 41-м пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ [постановление № 41-13 от 28 ноября 2014 года][113]

I. ОБЩИЕ ПОЛОЖЕНИЯ

Стратегия информационной безопасности государств – участников Содружества Независимых Государств (далее – Стратегия) представляет собой совокупность официальных взглядов на сущность и содержание межгосударственного сотрудничества по обеспечению информационной безопасности государств − участников СНГ.

Стратегия служит основой для консолидации усилий и повышения эффективности межгосударственного сотрудничества государств – участников СНГ по обеспечению информационной безопасности; формирования межгосударственной политики в сфере обеспечения информационной безопасности, прежде всего на основе системы мер стратегического планирования; подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности государств – участников СНГ.

Сохраняя преемственность по отношению к основным положениям Концепции сотрудничества государств – участников Содружества Независимых Государств в сфере обеспечения информационной безопасности, подписанной в Бишкеке 10 октября 2008 года, учитывая положения Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности, подписанного в Санкт-Петербурге 20 ноября 2013 года, иных ранее принятых основополагающих документов в сфере национальной и информационной безопасности государств – участников СНГ, Стратегия исходит из основных тенденций развития государств Содружества, их места и роли в современном мире.

В настоящей Стратегии используются следующие основные понятия:

государственная политика обеспечения информационной безопасности – деятельность государственных органов по определению содержания (форм, методов, средств, задач, субъектов, функций и др.) мер обеспечения информационной безопасности и последовательности их реализации;

информационная безопасность – состояние защищенности личности, общества и государства и их сбалансированных интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве;

информационная война – противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационной структуре и информационным системам, процессам и ресурсам, критически важным и иным структурам для подрыва политической, экономической и социальной систем, массированной психологической обработки населения, направленной на дестабилизацию общества и государства, а также

---

[113] Иформационный бюллетень МПА СНГ. – 2015, № 62. Часть 2. – С. 28- 57.

принуждения его военно-политического руководства к принятию решений в интересах противоборствующей стороны;

информационная инфраструктура – совокупность технических средств и систем формирования, создания, преобразования, передачи, использования и хранения информации;

информационная преступность – использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях;

информационная технология – совокупность методов, производственных процессов и программно-технических средств, объединенных в технологический комплекс, обеспечивающий сбор, создание, хранение, накопление, обработку, поиск, вывод, копирование, передачу, распространение и защиту информации;

информационная угроза национальной безопасности – потенциальная или реально существующая опасность нанесения ущерба национальным интересам государств – участников СНГ;

информационное оружие – информационные технологии, средства и методы, применяемые в целях ведения информационной войны;

информационное пространство – сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию;

информационно-коммуникационные технологии (ИКТ) – информационные процессы и методы работы с информацией, осуществляемые с применением средств вычислительной техники и средств телекоммуникации;

информационный суверенитет государств – участников СНГ – способность и возможность самостоятельно осуществлять функции государства в информационной сфере с целью соблюдения прав и свобод граждан, обеспечения национальной и коллективной безопасности;

информационный терроризм – использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях;

информация ограниченного доступа – информация, доступ к которой ограничен законодательством государств – участников СНГ либо их межгосударственными договорами;

контент – любое информационно значимое наполнение информационного ресурса, которое может быть предоставлено пользователю;

критическая информационная инфраструктура – совокупность технических средств и систем формирования, создания, преобразования, передачи, использования и хранения информации, являющихся жизненно важными для государства, отказ или разрушение которых может оказать существенное отрицательное воздействие на национальную безопасность;

международная информационная безопасность – состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве;

национальные интересы в информационной сфере – совокупность потребностей государства по реализации сбалансированных интересов личности, общества и государства в информационной сфере;

неправомерное использование информационных ресурсов – использование информационных ресурсов без соответствующих прав или с нарушением установленных правил, законодательства государств либо норм международного права;

обеспечение информационной безопасности – система мер и мероприятий организационно-технического и организационно-экономического характера по выявлению угроз информационной безопасности, их предупреждению, предотвращению их реализации, пресечению и ликвидации последствий реализации таких угроз;

правовой информационный статус – интегрированная совокупность возможностей реализации субъектом своих прав и интересов во всех видах информационных отношений.

II. СОВРЕМЕННОЕ СОСТОЯНИЕ РАЗВИТИЯ ОБЩЕСТВА И НАЦИОНАЛЬНЫЕ ИНТЕРЕСЫ ГОСУДАРСТВ – УЧАСТНИКОВ СНГ В ИНФОРМАЦИОННОЙ СФЕРЕ

Современный этап развития государств – участников СНГ характеризуется возрастающей ролью информационной сферы, являющейся важнейшим фактором общественной жизни, во многом определяющим перспективы успешного осуществления социально-политических и экономических преобразований. В условиях глобализации и жесткой международной конкуренции информационная безопасность приобретает первостепенное значение в обеспечении национальных интересов государств – участников СНГ.

Это обусловлено прежде всего следующими основными обстоятельствами:

а) в условиях объективно расширяющихся возможностей реализации конституционных прав граждан на свободу экономической, информационной, интеллектуальной и иной деятельности существенно возрастают потребности социально активной части общества в активизации и расширении информационного взаимодействия как внутри государств – участников СНГ, так и с внешним миром, иными межгосударственными образованиями;

б) интенсивное развитие информационной инфраструктуры, прежде всего информационно-телекоммуникационных систем, средств и систем связи, интеграция в мировое информационное пространство, а также информатизация всех сторон общественной жизни и деятельности государств существенно усилили зависимость эффективности функционирования политических систем от состояния информационной сферы;

в) индустрия информатизации, телекоммуникации и связи, информационных услуг на современном этапе развития человечества является одной из наиболее динамично развивающихся сфер мировой экономики;

г) информационная инфраструктура и информационные ресурсы во все большей степени становятся ареной межгосударственной борьбы за мировое лидерство, за достижение противоборствующими государствами определенных политических и экономических целей;

д) индивидуальное и общественное (групповое и массовое) сознание людей все в большей степени зависит от деятельности средств массовой информации.

Принимая во внимание вышеизложенные обстоятельства, к основным национальным интересам государств – участников СНГ в информационной сфере следует отнести:

– реализацию конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации;

– формирование и поступательное развитие информационного общества в государствах – участниках СНГ;

– равноправное, недискриминационное участие государств – участников СНГ в мировых информационных отношениях;

– эффективное информационное обеспечение государственной политики государств – участников СНГ;

– обеспечение надежности и устойчивости функционирования критически важных объектов информатизации.

Целью обеспечения безопасности государств – участников СНГ в информационной сфере является достижение и поддержание информационного суверенитета. Информационный суверенитет при этом понимается как исключительное право государства в соответствии с национальным законодательством и нормами международного права, с соблюдением баланса интересов субъектов безопасности определять и реализовывать национальные интересы в информационной сфере; право самостоятельно и независимо проводить внутреннюю и внешнюю государственную информационную политику, распоряжаться собственными информационными ресурсами, формировать инфраструктуру национального информационного пространства, создавать условия для интеграции в мировое информационное пространство. Информационный суверенитет достигается в рамках реализации информационных национальных интересов государств – участников СНГ в основных сферах жизнедеятельности.

Исходя из вышеизложенного можно считать, что достижению целей государственной политики государств – участников СНГ будет способствовать их равноправное участие в решении следующих задач:

а) формирование системы международной информационной безопасности на двустороннем, многостороннем, региональном и глобальном уровнях;

б) создание условий, обеспечивающих снижение риска использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

в) формирование механизмов международного сотрудничества в области противодействия угрозам использования информационных и коммуникационных технологий в противоправных и террористических целях;

г) создание условий для противодействия угрозам использования информационных и коммуникационных технологий в экстремистских целях, в том числе в целях вмешательства во внутренние дела суверенных государств;

д) повышение эффективности международного сотрудничества в области противодействия преступности в сфере использования информационных и коммуникационных технологий;

е) создание условий для обеспечения технологического суверенитета государств в области информационных и коммуникационных технологий и преодоления информационного неравенства между развитыми и развивающимися странами.

Основным правовым средством согласования, гармонизации механизмов регулирования информационных отношений представляется объединение правового регулирования по выделенным направлениям в единый правовой статус (личности, общества и государства). При этом выделяются следующие основные правовые информационные статусы:

1) информационный статус личности;

2) «безопасное информационное общество»;

3) информационный суверенитет государств – участников СНГ.

Информационный статус личности предусматривает реализацию конституционных прав и свобод гражданина в следующих областях:

– защищенность от незаконного вмешательства в личную жизнь, реализация прав на персональные данные;

– интеллектуальная собственность;

– поиск, получение, хранение, передача и распространение полной, достоверной и своевременной информации;

– информационное участие в государственном управлении;

– «электронная занятость», дистанционное («электронное») образование, электронное здравоохранение;

– социальная защита.

Правовой статус «безопасное информационное общество» – это информационный правовой статус общества, позволяющий:

– сохранить его духовные и нравственные ценности (традиции, культурные ценности);

– развивать его интеллектуальный и духовно-нравственный потенциал;

– реализовывать деятельность институтов гражданского общества и свободное распространение в обществе достоверной информации о данной деятельности;

– противостоять деструктивному информационному влиянию на общественное и индивидуальное сознание, насаждению чуждых ценностей и ориентиров;

– обеспечивать получение достоверной информации о состоянии окружающей среды, об экономических, политических и социальных процессах, о демографической и социальной обстановке.

Правовой статус безопасности государств − участников СНГ («информационный суверенитет») нацелен на обеспечение решения следующих задач:

– создание условий для информационного обеспечения реализации государственной политики, способствующей повышению эффективности функционирования государственных институтов;

– создание условий для информационного обеспечения международного сотрудничества, способствующего расширению присутствия государств − участников СНГ на мировом экономическом рынке и рынке интеллектуальных продуктов, их равноправному и недискриминационному участию в мировых информационных отношениях и информационном обмене, информационному обеспечению внешней политики;

– самостоятельное инновационное развитие, способствующее развитию современных информационных технологий, индустрии информационных услуг, производству средств информатизации;

– построение и безопасное развитие информационной инфраструктуры, создающее технологическую основу управления государствами (в мирное время, в чрезвычайных ситуациях и в военное время) и способствующее их взаимодействию в рамках СНГ в едином информационном пространстве;

– обеспечение надежного и устойчивого функционирования критически важных объектов информационно-телекоммуникационной инфраструктуры (КВОИ) государств − участников СНГ;

– реализация правоотношений в информационной сфере с соблюдением законов информационного общества: права на доступ к информации, недискриминационный порядок информационного обмена, законность информационных экономических сделок, уважение интеллектуальной собственности;

– обеспечение правового режима информации ограниченного доступа, сохранность государственных секретов государств − участников СНГ.

III. ИНФОРМАЦИОННЫЕ УГРОЗЫ, ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ГОСУДАРСТВ − УЧАСТНИКОВ СНГ

В настоящее время информационные технологии находят все более широкое применение в управлении различными важнейшими объектами жизнеобеспечения государств − участников СНГ. Вместе с тем такие объекты нередко становятся более уязвимыми перед возможными случайными и преднамеренными воздействиями.

Информационные факторы приобретают все большее значение в политической сфере. В традиционном противостоянии политических соперников растут удельный вес и значимость информационного воздействия. Возрастает уязвимость экономических структур от недостоверности, запаздывания и незаконного использования экономической информации. Информационные технологии во многом определяют структуру и качество вооружений, оценку уровня их необходимой достаточности, эффективность действий Вооруженных сил государств – участников СНГ.

В социальной сфере возрастает опасность развития в обществе агрессивной потребительской идеологии, тотальной коммерциализации культуры, распространения идей насилия и нетерпимости, деструктивного воздействия на психику людей. В силу отмеченного прогрессивное и устойчивое развитие государств − участников СНГ возможно только при условии наиболее полного обеспечения надлежащего уровня информационной безопасности и противодействия источникам угроз в информационной сфере.

Основными потенциальными угрозами национальной безопасности в информационной сфере являются, а нередко сегодня становятся реальными:

– посягательства на информационный суверенитет государств – участников СНГ, на их право самостоятельно владеть, пользоваться и распоряжаться своими информационными ресурсами;

– деструктивное информационное воздействие на личность, общество, государственные институты и их информационную инфраструктуру, наносящее ущерб национальным интересам государств;

– нарушение функционирования критически важных объектов информатизации;

– недостаточные масштабы и уровень внедрения передовых информационно-коммуникационных технологий в отдельных государствах − участниках СНГ;

– снижение или потеря конкурентоспособности информационно-коммуникационных технологий, информационных ресурсов и национального контента государств − участников СНГ;

– деятельность организованных преступных групп и сообществ, в том числе экстремистской и террористической направленности, в информационной сфере СНГ;

– утрата либо разглашение сведений ограниченного доступа, способных причинить ущерб национальной безопасности государств.

В свете современных глобальных тенденций общественного развития основными угрозами в области международной информационной безопасности становится использование информационно-коммуникационных технологий:

а) в качестве информационного оружия в военно-политических целях, противоречащих международному праву;

б) для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

в) в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды идей терроризма и вовлечения новых субъектов в террористическую деятельность;

г) для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию;

д) для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ.

Источники угроз в свете условий обеспечения основных правовых информационных статусов

1. Основными источниками угроз с позиций возможности реализации информационного статуса личности являются:

– нарушение конституционных прав личности на поиск, получение, хранение, передачу и распространение полной, достоверной и своевременной информации;

– создание и развитие технологий манипулирования информацией, дающих возможности для деструктивного информационного воздействия посредством их применения;

– широкое распространение в мировом информационном пространстве низкопробных образцов массовой культуры, вступающих в противоречие с общечеловеческими и национальными духовно-нравственными ценностями.

2. Основными источниками угроз с позиций реализации правового статуса «безопасное информационное общество» являются:

– недостаточная эффективность использования информационной инфраструктуры в интересах прогрессивного общественного развития и в целях консолидации гражданского общества в государствах − участниках СНГ;

– несовершенство системы формирования, сохранения и рационального использования информационных ресурсов, составляющих основу духовно-нравственного потенциала государств − участников СНГ;

– внешнее информационное воздействие и давление, осуществляемое в целях изменения мировоззренческих установок, политических взглядов и морально-психологического состояния людей;

– возможность деформации системы массового информирования как вследствие монополизации средств массовой информации и коммуникации в государствах − участниках

СНГ, так и вследствие неконтролируемого расширения сектора средств массовой информации и коммуникации третьих стран в информационном пространстве государств − участников СНГ;

– недостаточно высокое качество национального информационного контента, продуцируемого в государствах − участниках СНГ;

– низкий уровень взаимодействия государственных органов и общественных организаций государств − участников СНГ в вопросах развития информационного общества.

3. Основные источники угроз с позиций реализации статуса информационного суверенитета государств − участников СНГ.

3.1. К основным источникам угроз в свете информационного обеспечения государственной политики стран СНГ можно отнести:

– недостаточную эффективность информационного обеспечения государственной политики;

– открытость и, как следствие, уязвимость информационного пространства государств − участников СНГ перед внешним информационным воздействием;

– распространение недостоверной или умышленно искаженной информации, способной причинить ущерб национальным интересам государств − участников СНГ;

– деятельность в информационной сфере третьих стран, международных и иных организаций, отдельных лиц, наносящая ущерб национальным интересам государств − участников СНГ, целенаправленное формирование информационных поводов для дискредитации государств Содружества;

– нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение третьими странами борьбы за возможность влияния на процессы в информационном пространстве;

– попытки несанкционированного доступа извне к информационным ресурсам государств − участников СНГ, приводящие к причинению ущерба их национальным интересам.

3.2. Основными источниками угроз в отношении развития индустрии информации государств − участников СНГ являются:

– зависимость государств − участников СНГ от импорта информационных технологий, средств информатизации, технологий и средств защиты информации, неконтролируемое их использование в системах, отказ или разрушение которых способны причинить ущерб безопасности государств − участников СНГ;

– недостаточный уровень развития системы контроля и регулирования процесса внедрения и использования информационных технологий в государствах – участниках СНГ;

– доминирование ведущих зарубежных государств в мировом информационном пространстве, монополизация ключевых сегментов информационных рынков зарубежными информационными структурами.

3.3. Основными источниками угроз в отношении обеспечения безопасности информационных и телекоммуникационных средств и систем критически важных объектов информатизации, формирования системы информационной безопасности, обеспечения защиты сведений, составляющих охраняемую законодательством тайну, являются:

– криминализация информационной сферы и рост преступности с использованием возможностей современных информационно-коммуникационных технологий;

– недостаточность прилагаемых скоординированных усилий государств − участников СНГ в борьбе с преступлениями в информационной сфере;

– несовершенство системы обеспечения безопасности критически важных объектов информатизации;

– нарушение регламентов создания, обработки, хранения, передачи и защиты информации, содержащейся в информационных ресурсах государственных органов и иных организаций государств − участников СНГ, в том числе включающих информацию о личной жизни граждан;

– использование несертифицированных импортных программно-технических средств в информационных системах, опосредующих информационные отношения;

– умышленные или непреднамеренные действия персонала или пользователей, приводящие к нарушению требований безопасности информационных систем;

– несанкционированный доступ к информационным ресурсам, воздействие на информационные системы с целью перехвата управления ими или блокирования их работы;

– деятельность третьих стран, их специальных служб, преступных групп и формирований, противозаконная деятельность отдельных лиц в области информационных отношений;

– отказы технических средств и сбои в работе программного обеспечения в информационных системах и сетях.

Информационные источники угроз безопасности государств – участников СНГ в основных сферах жизнедеятельности

1. Политическая сфера:

– недостаточная информированность населения государств − участников СНГ и мирового сообщества о политике, проводимой в СНГ;

– деструктивная информационно-пропагандистская деятельность отдельных субъектов гражданского общества, средств массовой информации и коммуникации и отдельных лиц, дискредитирующая основные положения политики, проводимой в СНГ;

– ненадлежащее исполнение государственными органами и организациями государств − участников СНГ законодательства, регулирующего отношения в информационной сфере;

– воспрепятствование реализации субъектами гражданского общества государств − участников СНГ законных прав на использование средств массовой информации и коммуникации для осуществления в порядке, установленном законодательством государств − участников СНГ, общественной и политической деятельности;

– нарушение установленного порядка формирования, сбора, обработки, хранения и передачи информации в уполномоченных государственных органах и в организациях государств – участников СНГ;

– умышленное распространение в информационной сфере тенденциозной, искаженной либо недостоверной информации в целях инспирирования проявлений политического, национального или религиозного экстремизма;

– искажение третьими странами информации о внешней и внутренней политике государств − участников СНГ;

– несанкционированный доступ к информационным ресурсам, иные противоправные действия, существенно затрудняющие реализацию политики государств − участников СНГ.

2. Экономическая сфера:

– недостаточный уровень информатизации экономической сферы, прежде всего кредитно-финансовой системы, отраслей промышленности и сельского хозяйства;

– недостаточный государственный контроль в сфере создания, использования и защиты систем сбора, обработки, хранения и передачи статистической, финансово-экономической и иной социально значимой информации;

– несовершенство законодательства, определяющего ответственность субъектов хозяйствования за недостоверность или сокрытие сведений об их коммерческой деятельности и инвестициях, о результатах хозяйственной деятельности, о потребительских свойствах производимых ими товаров и услуг;

– нарушение конфиденциальности, целостности и доступности экономической информации, совершение правонарушений, связанных с доступом к информационным ресурсам кредитно-финансовой системы государств − участников СНГ, иное противоправное воздействие на информационные отношения в экономической сфере, коммерческий шпионаж;

– использование нелицензионного и несертифицированного программного обеспечения средств обработки информации в отраслях экономики государств − участников СНГ, могущее повлечь за собой активацию недекларированных возможностей, сбои в работе систем, а также утрату важной информации;

– усилия третьих стран, нацеленные на монополизацию отдельных областей информационного рынка государств – участников СНГ.

3. Научно-технологическая сфера:

– недостаточный уровень защиты информации в учреждениях и организациях научно-технологической сферы, неудовлетворительное состояние патентной защиты результатов научной деятельности в государствах – участниках СНГ, наносящие ущерб национальным интересам и престижу государств Содружества;

– несбалансированность информационного обмена научной и научно-технологической информацией между государствами – участниками СНГ как внутри Содружества, так и с третьими странами;

– утечка результатов фундаментальных, поисковых и прикладных научных исследований, содержащих информацию, потенциально важную для научно-технологического и социально-экономического развития государств − участников СНГ;

– хищение, незаконное распространение или использование приоритетных технологий;

– промышленный шпионаж: стремление третьих стран, различных субъектов хозяйственной деятельности получить незаконный доступ к научным ресурсам государств − участников СНГ с целью использования полученных учеными СНГ результатов в собственных интересах.

4. Социальная сфера:

– информационное воздействие, оказываемое посредством современных средств массовой коммуникации, способствующее девальвации у населения, прежде всего в молодежной среде, жизнесберегающих нравственных ценностей, установок патриотизма и гражданской ответственности;

– целенаправленное распространение в информационной среде государств − участников СНГ агрессивно-деструктивного, негативного контента в целях изменения мировоззренческих установок граждан, ухудшения морально-психологического состояния населения;

– пропаганда в средствах массовой информации и телекоммуникации государств − участников СНГ идей эгоизма, индивидуализма, потребительства, социальной безответственности, иждивенческих принципов, культивирование аморального, девиантного поведения и иных установок, ведущих к деградации личности и института семьи;

– деятельность деструктивных религиозных объединений, распространение псевдорелигиозных культов, влекущие за собой опасность нанесения вреда здоровью и жизни граждан в государствах СНГ;

– негативные тенденции по вытеснению из информационного культурного пространства национальных художественных произведений, народного творчества государств − участников СНГ;

– недостаточная эффективность мер по сохранению культурного наследия, включая архивы, музейные и библиотечные фонды, памятники архитектуры и иные культурные ценности, хранящиеся на информационных носителях в государствах − участниках СНГ;

– низкая результативность деятельности служб изучения и анализа общественного мнения, недостаточная эффективность контр-пропагандистского воздействия на формирование общественного мнения в государствах − участниках СНГ.

5. Военная сфера:

– политика третьих стран, нацеленная на использование мониторинга политических и военных процессов в государствах − участниках СНГ данных для получения односторонних преимуществ в военно-политических отношениях;

– недостаточный уровень развития информационных технологий в государствах СНГ, сложившаяся ориентация на широкое использование импортных технических средств и систем информатизации, программного обеспечения (часто — не прошедших государственный контроль), а также расширение участия компаний третьих стран в развитии информационной инфраструктуры военной сферы;

– возможные отказы технических средств и сбои в работе программного обеспечения в информационных системах оборонного комплекса;

– несовершенство в государствах − участниках СНГ нормативно-правовой базы, регулирующей межгосударственные отношения в области обеспечения информационной безопасности в военной сфере;

– отсутствие в государствах − участниках СНГ эффективной системы защиты объектов интеллектуальной собственности предприятий оборонного сектора экономики;

– информационно-пропагандистская деятельность организаций и отдельных лиц деструктивной направленности, а также психологические операции третьих стран, осуществляемые специальными методами и через средства массовой информации и коммуникации, направленные на подрыв престижа и боеготовности Вооруженных сил государств − участников СНГ и дискредитирующие политику этих государств в оборонной и военной сферах;

– разведывательная деятельность третьих стран и международных организаций, направленная на нанесение ущерба обороноспособности государств − участников СНГ;

– информационно-техническое воздействие (осуществляемое посредством методов радиоэлектронной борьбы, проникновения в компьютерные сети, внедрения программ-вирусов и программных закладок в общее и прикладное программное обеспечение и средства защиты информации) со стороны третьих стран и организаций, наносящее ущерб оборонной безопасности государств − участников СНГ;

– возможные преднамеренные деструктивные действия и непреднамеренные ошибки персонала информационных систем оборонного комплекса.

6. Экологическая сфера:

– ненадлежащий уровень технологического контроля безопасности опасных производственных объектов, возможные нарушения функционирования автоматизированных систем сбора и обработки информации о реальных или потенциальных источниках возникновения чрезвычайных ситуаций в государствах − участниках СНГ;

– возможное неправомерное вмешательство в штатный режим работы информационных систем и сетей, обеспечивающих принятие управленческих решений при ликвидации чрезвычайных ситуаций в государствах − участниках СНГ;

– нарушение конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации о состоянии окружающей среды, приемах и способах снижения негативных экологических воздействий;

– деструктивная деятельность отдельных субъектов, направленная на изменение морально-этических норм и устойчивых поведенческих стереотипов экологически безопасной жизнедеятельности общества;

– ненадлежащий уровень ответственности должностных лиц за сокрытие, искажение, несвоевременность предоставления информации о неблагоприятной экологической ситуации, угрожающей жизни и здоровью граждан государств − участников СНГ.

IV. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВ – УЧАСТНИКОВ СНГ

Понятие и содержание обеспечения информационной безопасности

Целью обеспечения национальной безопасности государств в рамках СНГ является достижение и поддержание такого уровня защищенности государств Содружества, который гарантирует их устойчивое развитие. Обеспечение информационной безопасности представляет собой деятельность субъектов по защите национальных интересов государств – участников СНГ от внутренних и внешних информационных угроз в рамках реализации национальных интересов в основных сферах жизнедеятельности. При этом обеспечение информационной безопасности осуществляется посредством противодействия информационным источникам угроз в основных сферах безопасности государств – участников СНГ.

Информационная безопасность служит целям обеспечения национальных интересов в основных сферах жизнедеятельности. Основными задачами ее обеспечения для государств – участников СНГ являются: разработка государственной политики обеспечения

информационной безопасности, создание системы обеспечения информационной безопасности и организация ее эффективного функционирования.

К основным принципам обеспечения информационной безопасности в государствах – участниках СНГ относятся:

– правовое равенство всех участников процесса информационного взаимодействия;

– добровольность принятия и выполнения каждым государством – участником СНГ обязательств, касающихся совместного обеспечения информационной безопасности;

– разработка и реализация совместных мероприятий по обеспечению информационной безопасности, осуществляемых на равноправной основе, с учетом обеспечения гармонизации интересов государств, с соблюдением норм международного права, требований нормативных правовых актов СНГ и национального законодательства государств – участников СНГ;

– последовательная реализация государствами – участниками СНГ мер по обеспечению информационной безопасности, направленных на нейтрализацию угроз в информационной сфере, приоритетность предупредительных мер;

– взаимная ответственность личности, общества и государства и регулярное информирование общества о состоянии информационной безопасности и о деятельности по ее обеспечению.

Обеспечение информационной безопасности осуществляется по направлениям, определяемым концептуальными документами в соответствии с основными сферами жизнедеятельности и областями обеспечения информационной безопасности государств – участников СНГ.

Основные направления обеспечения информационной безопасности для государств – участников СНГ.

1. Политическая сфера:

– разработка и реализация основных направлений организационного и технического обеспечения информационного сопровождения внутренней и внешней политики государств – участников СНГ;

– выработка комплекса мер по обеспечению безопасности информационных ресурсов, имеющих важное государственное значение для государств – участников СНГ;

– активизация контрпропагандистской деятельности и дипломатических усилий по предотвращению информационно-пропагандистского вмешательства во внутренние дела государств – участников СНГ с использованием возможностей современных информационно-телекоммуникационных средств и технологий;

– совершенствование системы информационно-аналитической поддержки принятия управленческих решений по обеспечению реализации интересов личности, общества и государства в информационной сфере государств – участников СНГ;

– организационно-техническое, информационное и ресурсное содействие государства средствам массовой информации и коммуникации, включая интернет-ресурсы, которые формируют положительный имидж государств – участников СНГ.

2. Экономическая сфера:

– совершенствование нормативно-правовой базы, регулирующей вопросы информационных отношений в экономической сфере;

– создание на основе программных и технологических решений, выработанных в государствах – участниках СНГ, государственных (межгосударственных) систем защиты сбора, обработки, хранения, накопления и передачи статистической, финансово-экономической, налоговой, таможенной и иной социально значимой экономической информации;

– разработка и внедрение средств защиты экономической информации ограниченного доступа;

– разработка и внедрение защищенных систем электронных платежей;

– создание и совершенствование специальных средств защиты финансовой и коммерческой информации;

– совершенствование методик отбора, подготовки, переподготовки и аттестации технического персонала для работы в системах создания, обработки, хранения, передачи и защиты экономической информации ограниченного доступа.

3. Научно-технологическая сфера:

– формирование социально-экономических условий для осуществления и развития научно-технической деятельности и эффективного функционирования учреждений науки в государствах – участниках СНГ;

– повышение эффективности использования интеллектуального потенциала государств – участников СНГ, предотвращение оттока за границу научных кадров и правообладателей интеллектуальной собственности;

– предотвращение экспансии современных информационных технологий третьих стран, создающей предпосылки технологической зависимости;

– развитие информационной инфраструктуры государств – участников СНГ на принципах стимулирования производителей и пользователей новейших информационно-телекоммуникационных средств и технологий, компьютерных программ и сетей;

– создание системы оценки возможного ущерба от реализации угроз информационной инфраструктуре в сфере науки и техники.

4. Социальная сфера:

– разработка действенных организационно-правовых и технологических механизмов доступа к официальной и открытой документированной информации;

– обеспечение достоверности сведений о социально значимых событиях общественной жизни, распространяемых через средства массовой информации и коммуникации;

– разработка правовых, организационных и технологических механизмов противодействия деструктивным информационным воздействиям на индивидуальное, групповое и массовое сознание;

– создание социально-экономических условий для осуществления творческой деятельности и функционирования учреждений культуры с использованием всего спектра современных передовых информационных и научно-технологических решений;

– использование современных информационных технологий для упреждения и противодействия информационно-психологической экспансии в отношении государств – участников СНГ, деструктивному влиянию религиозных организаций и миссионеров иных государств;

– пропаганда, с использованием возможностей современных информационно-коммуникационных технологий, здорового образа жизни и нравственного потенциала семьи как важнейшего института развития и социализации детей и подростков, проведение мероприятий по профилактике социально опасных заболеваний, алкоголизма, наркомании, токсикомании, компьютерной зависимости;

– рациональное использование и техническая защита накопленных в государствах – участниках СНГ информационных ресурсов, составляющих национальное и культурное достояние;

– осуществление, с использованием ИКТ, мониторинга процессов в демографической сфере.

5. Военная сфера:

– совершенствование форм и способов активного противодействия операциям информационной войны противоборствующей стороны, направленным на ослабление обороноспособности государств – участников СНГ;

– разработка и осуществление с применением всего арсенала современных ИКТ мер по выявлению, нейтрализации, локализации и противодействию деструктивному воздействию на информацию и информационно-психологическому воздействию на личный состав вооруженных сил государств – участников СНГ и население;

– совершенствование приемов и способов стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы, методов и средств активного противодействия деструктивному информационному воздействию;

– разработка и совершенствование нормативно-правовой базы, координация деятельности государственных органов и органов военного управления при решении задач обеспечения информационной безопасности в военной сфере государств – участников СНГ;

– совершенствование системы органов обеспечения информационной безопасности в военной сфере;

– проведение систематического анализа применения средств, форм и способов информационного противоборства в военной сфере государств – участников СНГ;

– совершенствование форм и создание национальных средств защиты информации в информационно-телекоммуникационных сетях от несанкционированного доступа, развитие защищенных систем связи и управления войсками государств – участников СНГ;

– разработка, внедрение и совершенствование средств сертификации и защиты информации, развитие защищенных систем управления оборонным комплексом государств – участников СНГ;

– экспертиза и сертификация общего и специального программного обеспечения, средств защиты информации в системах управления оборонным комплексом государств – участников СНГ.

6. Экологическая сфера:

– повышение надежности систем и средств сбора, обработки, хранения, передачи и защиты информации в экологической сфере;

– разработка и реализация мер по защите систем управления опасными производственными объектами, исключающих несанкционированные доступ и воздействие на них;

– применение современных геоинформационных средств и технологий для комплексного мониторинга, профилактики и своевременного реагирования на чрезвычайные ситуации в государствах – участниках СНГ;

– совершенствование системы информирования населения государств – участников СНГ об угрозах возникновения чрезвычайных ситуаций;

– организация информационно-пропагандистской работы по формированию в обществе морально-нравственных ценностей и устойчивых поведенческих стереотипов, направленных на сохранение и улучшение национального природного достояния.

Приоритетные направления реализации правовых информационных статусов

1. Приоритетными направлениями в реализации информационного статуса личности являются:

– расширение возможностей доступа граждан к мировому информационному пространству;

– обеспечение установленного законодательством порядка доступа к государственным информационным ресурсам, в том числе удаленного, и возможностей получения информационных услуг;

– совершенствование механизмов реализации прав граждан на поиск, получение, хранение, пользование и распоряжение информацией, в том числе с использованием современных информационно-коммуникационных технологий.

2. Приоритетными направлениями в реализации правового статуса «безопасное информационное общество» являются:

– разработка действенных организационно-правовых механизмов доступа к открытой документированной информации, обеспечение достоверности сведений о социально значимых событиях общественной жизни, распространяемых через средства массовой информации;

– выработка цивилизованных форм и способов общественного контроля за формированием в массовом сознании идеологических ценностей, отвечающих устойчивым целям общественного развития, воспитание чувства патриотизма и гражданской ответственности;

– разработка правовых и организационных механизмов противодействия деструктивным информационно-психологическим воздействиям на индивидуальное, групповое и массовое сознание.

3. Приоритетные направления реализации информационного суверенитета.

3.1. В качестве приоритетных направлений в реализации информационного обеспечения государственной политики государств – участников СНГ рассматриваются:

– разработка и реализация стратегии всеобъемлющей информатизации, ориентированной на развитие электронной системы осуществления административных процедур и услуг, оказываемых гражданам и бизнесу государственными органами и иными организациями, перевод государственного аппарата на работу в режиме электронного информационного взаимодействия;

– создание и использование межгосударственных, международных глобальных информационных сетей и систем государств – участников СНГ;

– создание системы противодействия монополизации третьими странами составляющих информационной инфраструктуры, включая рынок информационных услуг и средства массовой информации;

– участие государств – участников СНГ в международных договорах, регулирующих на равноправной основе мировой информационный обмен;

– доведение до граждан государств – участников СНГ и международной аудитории объективной информации о деятельности СНГ, официальной позиции по общественно значимым событиям внутри страны и за рубежом;

– последовательное увеличение объема, повышение качества и конкурентоспособности национального информационного контента государств – участников СНГ;

– активизация контрпропагандистской деятельности, направленной на предотвращение негативных последствий распространения дезинформации о политике государств – участников СНГ;

– создание системы страхования информационных ресурсов государств – участников СНГ.

3.2. Приоритетными направлениями развития индустрии информации для государств – участников СНГ являются:

– развитие индустрии информационных и телекоммуникационных технологий и услуг, широкомасштабное использование информационных технологий и сетевых телекоммуникаций в сфере государственного управления, повышение эффективности использования государственных, корпоративных и частных информационных ресурсов;

– опережающее развитие и модернизация информационно-коммуникационной инфраструктуры на началах стимулирования производителей и пользователей новейших информационно-телекоммуникационных средств и технологий, компьютерных систем и сетей государств – участников СНГ;

– поддержка высокотехнологического производства в государствах – участниках СНГ, прежде всего в области информационно-телекоммуникационных средств и технологий, активное участие в международной кооперации их производителей;

– интеграция государств – участников СНГ в международные информационно-телекоммуникационные структуры и организации на началах равноправия, экономической целесообразности и сохранения информационного суверенитета;

– формирование в научно-технологической сфере сегмента инновационной инфраструктуры, обеспечивающей создание малых технологических предприятий, и условий для их динамичного развития и привлечения прямых инвестиций в экономику государств – участников СНГ;

– повышение конкурентоспособности информационного продукта и информационных услуг государств – участников СНГ;

– достижение и поддержание мирового уровня и паритета в отраслях ИКТ, наиболее важных для обеспечения национальной безопасности, экономического и научно-технического прогресса государств – участников СНГ;

– создание и использование соответствующего современным условиям механизма финансирования науки в сфере ИКТ на основе сочетания целевых государственных расходов

государств – участников СНГ с возрастающей долей частного финансирования научных исследований прикладного характера;

– сохранение кадровой основы научного потенциала государств – участников СНГ, противодействие оттоку научных сил за границу, систематическое воспроизводство научных кадров (прежде всего на приоритетных направлениях фундаментальной и прикладной науки), создание условий, способствующих повышению престижа научной деятельности в информационной сфере.

3.3. Приоритетными направлениями в реализации обеспечения безопасности информационных и телекоммуникационных средств и систем критически важных объектов информатизации, формировании системы информационной безопасности, обеспечении защиты информации ограниченного доступа являются:

– совершенствование нормативно-правовой базы государств – участников СНГ, регламентирующей защиту информационных отношений, соответствующих установленным требованиям безопасности;

– создание и развитие организационных структур системы обеспечения информационной безопасности, завершение формирования комплексной системы обеспечения информационной безопасности государств – участников СНГ;

– стандартизация информационных технологий, применяемых в информационных системах и сетях государств – участников СНГ и обеспечивающих их безопасность;

– совершенствование разрешительной деятельности (лицензирование деятельности) предприятий государств – участников СНГ в области защиты информации;

– разработка и внедрение современных методов и средств защиты информации в информационных системах критически важной инфраструктуры государств – участников СНГ, отказ или разрушение которой может оказать отрицательное воздействие на национальную безопасность;

– сертификация средств защиты информации и контроль за эффективностью обеспечения информационной безопасности в информационных системах и сетях государств – участников СНГ в части защищенности информации от утечки по техническим каналам;

– применение специальных методов, технических мер и средств защиты, исключающих перехват информации, передаваемой по информационным сетям;

– противодействие негативному воздействию на информационные системы и сети, создание условий для восстановления их работоспособности;

– предупреждение и пресечение несанкционированного доступа к защищаемым информационным ресурсам государств – участников СНГ, выявление и устранение возможных каналов утечки информации;

– предупреждение, выявление и пресечение преступлений против информационной безопасности, а также надежное обеспечение безопасности информации, охраняемой в соответствии с действующим законодательством;

– развитие системы подготовки, профессиональной переподготовки и повышения квалификации кадров государств – участников СНГ, занятых в области информатизации и обеспечивающих информационную безопасность;

– развитие международного научно–технического сотрудничества государств – участников СНГ в сфере обеспечения защиты информации в международных телекоммуникационных системах и системах связи.

V. МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО ГОСУДАРСТВ – УЧАСТНИКОВ СНГ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Международное сотрудничество в сфере обеспечения информационной безопасности – неотъемлемая составляющая политического, экономического и других видов взаимодействия стран, входящих в мировое сообщество. Характерной особенностью международного сотрудничества государств – участников СНГ в сфере обеспечения информационной

безопасности является то, что оно осуществляется в условиях обострения международной конкуренции за обладание информационными ресурсами и доминирования на рынках западных информационных технологий, технических и программных продуктов. Эти факторы определяют спектр источников угроз в сфере обеспечения международной информационной безопасности.

В современных условиях к основным направлениям международного сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности следует отнести:

– определение, согласование и осуществление государствами – участниками СНГ необходимых совместных мер в сфере обеспечения международной информационной безопасности;

– обеспечение безопасности международного информационного обмена, включая сохранность информации при ее передаче по национальным информационно-телекоммуникационным каналам и каналам связи;

– разработку и осуществление согласованной политики и организационно-технических процедур по реализации возможностей использования электронной (электронной цифровой) подписи и защиты информации при трансграничном информационном обмене;

– разработку и осуществление мер доверия, способствующих обеспечению международной информационной безопасности;

– выработку совместных решений по развитию норм международного права в области ограничения распространения и применения информационного оружия, создающего угрозы национальной безопасности государств;

– содействие обеспечению безопасного и устойчивого функционирования Интернета и интернационализации управления глобальной сетью, недопущение использования ее потенциала в антиконституционных целях;

– противодействие угрозам использования информационно-коммуникационных технологий в террористических целях;

– противодействие преступности в информационной сфере;

– обмен оперативной информацией по проблемным вопросам обеспечения информационной безопасности между государствами – участниками СНГ, проведение экспертиз, исследований и оценок в сфере обеспечения информационной безопасности.

VI. СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВ – УЧАСТНИКОВ СНГ

Систему обеспечения информационной безопасности государств – участников СНГ составляет совокупность взаимодействующих национальных 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 составной частью системы обеспечения национальной безопасности.

Национальная система субъектов обеспечения информационной безопасности включает в себя:

– органы государственного управления в области обеспечения информационной безопасности (президент, правительство, Совет безопасности) и органы государственного управления, ответственные за осуществление государственной политики в области обеспечения информационной безопасности;

– органы обеспечения информационной безопасности (государственный орган – координатор этой деятельности и национальные исполнительные органы в области обеспечения информационной 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 показателей оценки состояния информационной безопасности, критериев эффективности деятельности субъектов ее обеспечения.

Полномочия субъектов обеспечения информационной безопасности определяются законодательством. Для предотвращения и нейтрализации угроз информационной безопасности применяются правовые, организационно-технические, организационно-экономические и иные методы.

В целях повышения эффективности обеспечения информационной безопасности осуществляются согласование, систематизация и координация усилий на соответствующих направлениях деятельности национальных уполномоченных органов государств – участников СНГ, а также других заинтересованных органов СНГ.

VII. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Общее руководство и контроль за реализацией настоящей Стратегии осуществляет Совет глав правительств государств – участников СНГ.

В целях реализации положений настоящего документа представляется рациональным (учитывая истечение сроков исполнения плана мероприятий на период 2008–2010 годов по реализации Концепции сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности) подготовить и принять план мероприятий по реализации Стратегии информационной безопасности государств – участников Содружества Независимых Государств.

Заседание экспертной группы по обсуждению проекта Стратегии обеспечения информационной безопасности в Исполкоме СНГ (г. Москва, 19 мая 2015 г.)

Вручение доктору юридических наук Илларии Лаврентьевне Бачило высшей награды Межпарламентской Ассамблеи СНГ — Ордена «Содружество»

Научно-практическое издание

Бачило Иллария Лаврентьевна
Бондуровский Владимир Владимирович
Вус Михаил Александрович
Макаров Олег Сергеевич
Лепёхин Александр Николаевич
Перевалов Дмитрий Васильевич
Юсупов Рафаэль Мидхатович

ISBN 978-5-7452-0036-6

СТРАТЕГИЧЕСКИЙ ВЕКТОР ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сборник

Редактор: Григорьева М.В.

Фото: Вус М.А.

Набор, оформление, корректура рукописи: Денисова Е.М.

Королёва Р.А.

199178, Россия, Санкт-Петербург,
14 линия, д. 39. СПИИРАН
E-mail: spiiran@iias.spb.su

Подписано в печать 20.10.2016. Формат 60x90 1/16
Бумага офсетная. Усл. печ.л. 7,1. Тираж 120 экз.
Оригинал-макет подготовлен в СПбОНТЗ
Отпечатано с оригинал-макета в типографии «Полиграфические технологии»
СПб, ул. Курчатова, д. 9.

ISBN 978-5-7452-0036-6