НЕКОТОРЫЕ АСПЕКТЫ ОРГАНИЗАЦИОННО-ПРАВОВОЙ ЗАЩИТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Е.Н. Яковец
Российская таможенная академия, г. Люберцы
email: koshka997@mail.ru

Аннотация. В данной статье анализируется содержание нормативно-правовой основы защиты информационно-телекоммуникационных систем в Российской Федерации. Особое внимание в плане формирования единого информационного пространства России уделяется защите государственных виртуальных сетей, в первую очередь – критической информационной инфраструктуры. Делается вывод о необходимости определения приоритетных направлений развития законодательной основы этой деятельности. Ещё одной нерешённой проблемой является импортозамещение в сфере производства компьютерной техники и разработки программного обеспечения.

Ключевые слова: информационно-телекоммуникационные системы, закрытые негосударственные (корпоративные) системы, критическая информационная инфраструктура, импортозамещение.

Информационно-телекоммуникационные системы (ИТКС) являются тем средством, которое обеспечивает удовлетворение потребностей субъектов информационных отношений на расстоянии. Защищаемые ИТКС и возникающие в ходе их охраны отношения являются самостоятельным объектом права в области информационной безопасности.

Вместе с тем, полностью исключить «информационный» элемент из рассматриваемого понятия нельзя, поскольку виртуальная информация, циркулируя по «кровеносной системе» ИТКС и подчиняясь особым закономерностям применяемых в ней информационных технологий, становится её неотъемлемым атрибутом.

Правовая охрана прав обладателя на ИТКС возникает с момента её создания (приобретения) и действует в объёме и порядке, предусмотренном вторым разделом части первой Гражданского кодекса РФ (Право собственности и другие вещные права). Вместе с тем, в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изм. и доп.)[1] говорится лишь о правах обладателя информации, содержащейся в базах данных информационной системы, которые подлежат охране независимо от авторских и иных прав на такие базы данных (ст. 13, п. 3), а право собственности на саму ИТКС не регламентировано. В данной связи делается лишь оговорка, что «если иное не установлено федеральным законом, оператором информационной системы является собственник используемых для обработки содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы» (ст. 13, п. 2). Однако понятия «оператор» и «обладатель (собственник)» не являются тождественными.

Определённую ясность в сущность вопроса вносит ст. 14 данного Закона, именуемая «Государственные информационные системы», определяя, по крайней мере, обладателя (собственника) информационных систем в государственном секторе общественных отношений в лице самого государства. Этот статус требует, чтобы государство определило свою заинтересованность и степень участия в охране и защите государственных ИТКС. Главенствующая роль государства, прежде всего,

[1] Российская газета. 2006. 29 июля.

должна чётко прослеживаться в осуществлении следующих организационно-правовых функций:

1. организация научных исследований и разработок в данной сфере, где при общем сокращении объёмов финансирования отсутствует должная координация, вследствие чего даже малозначительные выделяемые средства распыляются и не дают положительного эффекта;
2. установление льгот по инвестированию в сферы информационных технологий и развития ИТКС. Если у государства не имеется достаточных средств для их создания, то, по всей видимости, необходимо установить льготный режим кредитования для отечественных и иностранных инвесторов с учётом установления следующих ограничений для иностранцев:

– сохранения государственного контроля и участия в управлении предприятиями в инвестируемой отрасли индустрии и дальнейшей реализации произведённой продукции;

– проведения обязательной экспертизы и сертификации применяемых иностранных технологий элементной базы, а также отдельных видов оборудования и средств связи;

– использования исключительно отечественных технологий и инструментария защиты информации;

3. подготовка кадров, без чего трудно реализовать задачи обеспечения безопасности информационных систем;
4. определение перечня ИТКС, где государство должно нести стопроцентную ответственность за их охрану и защиту (системы управления федеральных органов государственной власти, управления войсками и оружием, обеспечения банковской и финансовой стабильности и т.п.), и критерии безопасности таких систем;
5. определение степени своего участия в регулировании процессов создания и функционирования закрытых негосударственных (корпоративных) систем, а также открытых систем, создаваемых в интересах защиты прав граждан;
6. установление более чётких правовых регуляторов, запретов и ограничений на осуществление международного информационного обмена [1].

Некоторые из этих задач уже успешно решены или находятся в стадии решения. Например, в целях создания системы управления приоритетами информатизации государственных органов и обеспечения эффективности бюджетных расходов на информатизацию было издано постановление Правительства РФ от 24 мая 2010 г. № 365 «О координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов» (с изм. и доп.)[1]. Постановлением Правительства России от 10 октября 2020 г. № 1646 данный документ признан утратившим силу, вместе с тем он сыграл свою положительную роль в решении поставленных задач. В нём были закреплены механизмы планирования информатизации, экспертизы планов и мероприятий информатизации, а также контроля реализации этих планов и мероприятий. В обязательном порядке для всех мероприятий, связанных с информатизацией государственных органов, ещё на этапе принятия решений оценивались их целесообразность и предполагаемая эффективность.

Сроки разработки, представления на экспертную оценку и рассмотрения проектов планов информатизации, представления отчётов об их выполнении определялись в графике подготовки и утверждения планов информатизации, который ежегодно утверждался Правительственной комиссией по внедрению информационных технологий в деятельность государственных органов и органов местного самоуправления. Действие указанного Постановления распространялось на

[1] Российская газета. 2010. 6 июля.

все государственные органы. Основными субъектами, призванными обеспечивать и контролировать данный процесс, наряду с указанной Правительственной комиссией являлись Минцифры России, Минфин России и Минэкономразвития России.

Другой пример. Ещё четверть века назад для оптимизации подготовки специалистов в сфере защиты информации приказом Министерства общего и профессионального образования РФ от 20 августа 1997 г. № 1781, наряду с существовавшими на тот период учебными заведениями по подготовке указанных кадров, в структуре МО, ФСБ и МВД России была создана и функционирует до сих пор сеть из 14 региональных учебно-научных центров по проблемам информационной безопасности. Кроме того, разработана специальная федеральная целевая программа, предусматривающая подготовку специалистов (на условиях госзаказа) с учётом потребностей как государственных, так и негосударственных структур в этой области.

Ещё один положительный момент – реальные успехи в создании ИТКС специального назначения в интересах федеральных органов государственной власти, о которых речь впервые зашла более четверти века назад после издания Указа Президента РФ от 3 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» (с изм. и доп.)[1]. В МВД России, например, начала создаваться Единая информационно-телекоммуникационной система (ЕИТКС) органов внутренних дел, и создаваемая на ее базе Единая система информационно-аналитического обеспечения деятельности МВД России; в Федеральной таможенной службе России – Единая автоматизированная информационная система (ЕАИС), действующая в рамках Ведомственной интегрированной телекоммуникационной сети (ВИТС) таможенных органов, и др.

Указом Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» (с изм. и доп.)[2] были введены определённые запреты и ограничения на осуществление международного информационного обмена, касающегося ведомственных ИТКС, оперирующих сведениями, составляющими государственную и служебную тайну. Его пп. 2 и 3 в соответствии с Указом Президента РФ от 22 мая 2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации»[3] признаны утратившими силу. Последним Указом введён также в действие Порядок подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети «Интернет» и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети «Интернет».

Кроме того, следует отметить, что в рамках реализации п. 6 ст. 14 Федерального закона «Об информации, информационных технологиях и о защите информации» постановлением Правительства РФ от 10 сентября 2009 г. № 723 «О порядке ввода в эксплуатацию отдельных государственных информационных систем» утверждено Положение о регистрации федеральных государственных информационных систем (с изм. и доп.)[4], устанавливающее порядок регистрации федеральных государственных информационных систем, формирования и ведения реестра федеральных государственных информационных систем, а также обеспечения доступа к информации, содержащейся в указанном реестре.

---

[1] Собр. законодательства Рос. Федерации. – 1995. – № 15, ст. 1285.
[2] Собр. законодательства Рос. Федерации от 24 марта 2008 г. № 12, ст. 1110.
[3] Российская газета. 2015. 26 мая.
[4] Российская газета. 2009. 18 сентября.

В рамках реализации требований данного Положения распоряжением Правительства РФ от 27 декабря 2011 г. № 2387-р утверждена Концепция создания и развития государственной информационной системы учёта информационных систем, разрабатываемых и приобретаемых за счёт средств бюджетов бюджетной системы Российской Федерации[1]. Опытная эксплуатация проекта началась в I кв. 2012 г., а промышленная – в I кв. 2013 г. Всем информационным системам госведомств стали присваиваться индивидуальные номера. Минкомсвязь России (в настоящее время – Минцифры России) классифицирует эти системы, рейтингует их по эффективности, устраняет дублирование, сочетая эти мероприятия с экономией госсредств.

Следует отметить, что уголовно-правовая защита ИТКС, причём, независимо от их принадлежности тем или иным субъектам, осуществляется в рамках статей 274 и 274.1 УК РФ. На их содержание следует обратить особое внимание. Статья ст. 274 УК РФ (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей) устанавливает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо ИТКС и оконечного оборудования, а также правил доступа к ИТКС, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб. Эта статья не даёт определения нарушения правил эксплуатации отмеченных в её диспозиции объектов, она раскрывает лишь его последствия: уничтожение, блокирование или модификацию компьютерной информации. Таким образом, данная диспозиция носит бланкетный (отсылочный) характер. Специалисты полагают, что это одно из наиболее слабых мест действующего уголовного законодательства в области защиты компьютерной информации.

Рассматриваемая уголовно-правовая норма отсылает нас к ведомственным инструкциям и правилам, определяющим порядок эксплуатации средств хранения, обработки или передачи компьютерной информации, информационно-телекоммуникационных сетей и оконечного оборудования. Указанные документы должны разрабатываться специально уполномоченными на то лицами и доводиться до сведения пользователей-исполнителей, на которых и возлагается обязанность по соблюдению соответствующих норм.

Следует привести некоторые пояснения и по сущности объектов защиты. Если прежняя редакция ст. 274 УК РФ под «сетями системы ЭВМ» понимала только внутренние компьютерные сети отдельных ведомств или организаций (учреждений, предприятий), и на глобальные сети типа Интернет её действие не распространялось, то в действующей редакции ситуация кардинальным образом изменилась. Обобщённым понятием «информационно-телекоммуникационные сети» охватывается теперь и глобальная сеть Интернет. Несмотря на то, что Интернет является децентрализованным, и единого общеобязательного свода правил пользования этой глобальной сетью не существует, действуют, однако, общепризнанные нормы работы в ней, направленные на то, чтобы деятельность каждого пользователя сети не мешала работе других пользователей. Фундаментальное положение этих норм таково: правила использования любых ресурсов сети Интернет (от почтового ящика до канала связи) определяют владельцы этих ресурсов, и только они [2].

В рассматриваемой статье УК РФ наряду с прочими объектами защиты появилось и понятие оконечного оборудования (обработки) данных (ООД), которое, как известно, предназначено для преобразования пользовательской информации в

[1] Российская газета. 2012. 15 февраля.

данные для передачи по линиям связи и осуществления обратного преобразования. Оно может являться источником информации, её получателем или тем и другим одновременно. Передача и (или) приём данных посредством использования ООД предполагает наличие линий связи и каналов связи (в рассматриваемом нами случае таковыми являются ИТКС).

Когда речь заходит о компьютерных преступлениях, в качестве ООД, как правило, рассматривается персональный компьютер (ЭВМ), являющийся одновременно средством хранения и обработки компьютерной информации. Поэтому как самостоятельный объект защиты в диспозиции ст. 274 УК РФ оконечное оборудование можно было бы и не указывать.

Следует выделить как минимум два вида правил эксплуатации средств хранения, обработки или передачи компьютерной информации, ИТКС и оконечного оборудования (в дальнейшем они могут именоваться «средства электронно-вычислительной техники» – «средства ЭВТ»), которыми должен руководствоваться в своей деятельности работающий с ними персонал. Первый вид правил – инструкции по работе с ЭВМ, машинными носителями информации и информационно-телекоммуникационными сетями, разрабатываемые их проектировщиками и изготовителями. Они поставляются пользователям вместе с электронно-вычислительной техникой. Эти правила обязательны для соблюдения последними, а их нарушение грозит, по меньшей мере, потерей прав на гарантийный ремонт и техническое обслуживание средств ЭВТ.

Второй вид правил – правила, устанавливаемые обладателем или законным пользователем информационных ресурсов, информационных систем, технологий и средств их обеспечения. Они же определяют и порядок доступа к ИТКС. (следует напомнить, что под неправомерным доступом к последней понимается самовольное подсоединение к ней без разрешения её обладателя, с нарушением установленного порядка для получения доступа к циркулирующей в ней информации).

В целом нарушения правил эксплуатации средств ЭВТ могут быть подразделены на физические (неправильное подключение периферийного оборудования, отсутствие устройств для бесперебойного питания, нарушение теплового режима в помещении, неправильное подключение компьютера к источникам питания, нерегулярное техническое обслуживание, использование несертифицированных средств защиты и самодельных узлов и приборов и пр.) и интеллектуальные (невыполнение процедуры резервного копирования, несанкционированная замена программного обеспечения, параметров настройки компьютера или компьютерной сети и пр.).

Именно нарушение всех этих правил, повлекшее причинение предусмотренного уголовным законом крупного вреда обладателю информационного ресурса, является уголовно наказуемым деянием, предусмотренным ст. 274 УК РФ. Квалифицирующими признаками данного преступления является наступление тяжких последствий или создание угрозы их наступления.

Редакция ст. 274.1 УК РФ (Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации) представляет собой объединение трёх форм преступного посягательства на безопасность компьютерных данных и систем: 1) неправомерный доступ; 2) создание и распространение вредоносного контента и 3) нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации. По смыслу ст. 274.1 УК РФ все эти деяния должны быть направлены против объектов критической информационной инфраструктуры (КИИ). Таким образом, анализируемая уголовно-правовая норма конкурирует сразу с тремя статьями УК РФ – 272, 273 и 274 и является специальной по отношению к ним. В некотором смысле конструирование

ст. 274.1 УК РФ противоречит сложившимся отечественным традициям криминализации и использования приёмов юридической техники при описании уголовно-правовых норм. Следуя им, установление более строгой уголовной ответственности за посягательства на объекты КИИ предпочтительнее было бы реализовать путём выделения соответствующих квалифицирующих и особо квалифицирующих признаков в ст. ст. 272, 273 и 274 УК РФ.

Анализируемая уголовно-правовая норма имеет бланкетный характер, что предполагает обязательное обращение к Федеральному закону от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[1]. Объектом преступлений, предусмотренных ст. 274.1 УК РФ, выступает безопасность КИИ Российской Федерации, т.е. состояние защищенности последней от любого воздействия программными или программно-техническими средствами, которое способно привести к нарушению её функционирования и (или) нарушению безопасности обрабатываемой ею информации. Предметом преступления, предусмотренного ч. 1 ст. 274.1 УК РФ, является компьютерная информация или компьютерные программы, заведомо предназначенные для совершения компьютерных атак на объекты КИИ. Следует отметить, что установление данного признака на практике может вызвать значительные затруднения. Функциональная направленность вредоносной программы, т.е. её предназначение именно для посягательств на соответствующие объекты, может быть установлена только в случае уникальности средств и технологий программной защиты объектов критической информационной инфраструктуры, что представляется маловероятным. Специфическим предметом преступлений, предусмотренных частями 2 и 3 ст. 274.1 УК РФ, выступают объекты КИИ – информационные системы, ИТКС государственных органов, а также информационные системы, ИТКС и автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, области здравоохранения, транспорта, связи, кредитно-финансовой сфере, энергетике, а также в топливной, атомной, ракетно-космической, горнодобывающей, металлургической и химической промышленности. Относимость того или иного информационного ресурса к критическому определяется посредством его включения в Реестр значимых объектов критической информационной инфраструктуры (ст. 8 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»).

Объективная сторона преступления, предусмотренного ч. 1 ст. 274.1 УК РФ, предполагает совершение любого из трёх альтернативных действий: 1) создание; 2) использование или 3) распространение компьютерных программ или информации, заведомо предназначенных для совершения атак на объекты КИИ. Состав по конструкции (по моменту описания в законе момента окончания преступления) является формальным. Состав данного преступления образуется, если лицо разработало, использовало и (или) распространило вредоносную компьютерную программу, заведомо предназначенную для совершения компьютерных атак на объекты КИИ. В завершение рассмотрения данного состава следует отметить, что объективная сторона преступления, предусмотренного ч. 2 ст. 274.1 УК РФ, заключается в неправомерном доступе к компьютерной информации, содержащейся в КИИ.

В Федеральном законе «Об информации, информационных технологиях и о защите информации» содержится ряд правовых норм, нацеленных на защиту безопасности ИТКС. Это – ст. 15.1. (Единый реестр доменных имён, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих

[1] Российская газета. 2017. 31 июля.

идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено); ст. 15.2. (Порядок ограничения доступа к информации, распространяемой с нарушением исключительных прав на фильмы, в том числе кинофильмы, телефильмы); ст. 15.3. (Порядок ограничения доступа к информации, распространяемой с нарушением закона); ст. 15.4. (Порядок ограничения доступа к информационному ресурсу организатора распространения информации в сети «Интернет»); и др.

В ходе контроля за соблюдением операторами связи, оказывающими услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет» требований, установленных указанными выше статьями, им предоставляются соответствующие технические средства для осуществления контроля за соблюдением указанных требований[1].

В развитие рассматриваемой темы следует упомянуть также положения п. 18 Доктрины информационной безопасности Российской Федерации, утверждённой Указом Президента РФ от 5 декабря 2016 г. № 646[2], где вполне обоснованно отмечается, что мероприятия по обеспечению безопасности информационной инфраструктуры, включая её целостность, доступность и устойчивое функционирование, с использованием отечественных информационных технологий и отечественной продукции зачастую не имеют комплексной основы. Кроме того, в пп. «в», «г» п. 23 Доктрины говорится, что к основным направлениям обеспечебия информационной безопасности в области государственной и общественной безопасности относятся:

– повышение защищённости КИИ и устойчивости её функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищённости граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты КИИ;

– повышение безопасности функционирования объектов КИИ, в том числе в целях обеспечения устойчивого взаимодействия государственных органов, недопущения иностранного контроля за функционированием таких объектов, обеспечение целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации, а также обеспечение безопасности информации, передаваемой по ней и обрабатываемой в информационных системах на территории Российской Федерации.

Существенное значение на современном этапе приобретает защита федеральных государственных информационных систем, создаваемых или используемых в целях реализации полномочий федеральных органов исполнительной власти и содержащих сведения, указанные в Перечне информации о деятельности Правительства Российской Федерации, размещаемой в сети Интернет, и Перечне информации о деятельности федеральных органов исполнительной власти, руководство деятельностью которых осуществляет Правительство Российской Федерации, и подведомственных им органов исполнительной власти, размещаемой в сети Интернет, утверждённых постановлением Правительства РФ от 24 ноября 2009 г. № 953 (с изм. и доп.)[3]. Это так называемые информационные

[1] Порядок предоставления операторам связи технических средств контроля за соблюдением оператором связи требований, установленных статьями 15.1–15.4 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: утв. приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 17 июля 2014 г. № 103 // Российская газета. 2014. 3 декабря.

[2] Российская газета. 2016. 5 декабря.

[3] Российская газета. 2009. 2 декабря.

системы общего пользования, доступ к которым не ограничивается определённым кругом лиц.

Для создания таких систем в своё время был разработан План перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения на 2011–2015 годы, утверждённый распоряжением Правительства РФ от 17 декабря 2010 г. № 2299-р[1], который предусматривал их переход на использование обновлённых пакетов базового свободного программного обеспечения и пакетов (обновлённых пакетов) дополнительных прикладных программ.

Защита указанных информационных систем регламентировалась также Постановлением Правительства РФ от 18 мая 2009 г. № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям»[2], изданными в развитие его положений «Требованиями по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования», утверждёнными приказом Министерства связи и массовых коммуникаций Российской Федерации от 25 августа 2009 г. № 104[3], и «Требованиями о защите информации, содержащейся в информационных системах общего пользования», утверждёнными приказом Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю от 31 августа 2010 г. № 416/489[4].

Кстати, именно п. 3 последнего из перечисленных нормативных правовых раскрывает содержание информационной системы общего пользования, которая включают в свой состав средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приёма и обработки информации, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации, программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

С целью обеспечения предоставления из федерального бюджета субсидий организациям связи и организациям, осуществляющим деятельность в области информационных технологий, приказом Министерства связи и массовых коммуникаций РФ от 30 июня 2017 г. № 340 были утверждены «Правила предоставления субсидии организации, осуществляющей ведение федеральных информационных фондов, баз и банков данных[5]»

С 1 июля 2015 г. в соответствии с ч. 2.1 ст. 13 Федерального закона «Об информации, информационных технологиях и о защите информации» технические средства информационных систем, используемых государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями или государственными и муниципальными учреждениями, должны размещаться исключительно на территории Российской Федерации. В соответствии с ч. 7 указанной статьи, порядок осуществления контроля за соблюдением данных требований устанавливается Правительством Российской Федерации. Часть 6 ст. 14 указанного Закона предусматривает также, что Правительство Российской Федерации должно утверждать требования к порядку

[1] Интернет-портал Правительства РФ // URL: http://правительство.рф/gov/results/?page=8 (дата обращения: 05.10.2022).
[2] Российская газета. 2009. 22 мая.
[3] Российская газета. 2009. 7 октября.
[4] Российская газета. 2010. 22 октября.
[5] Официальный портал правовой информации. 2017. 22 сентября.

создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем, дальнейшего хранения содержащейся в их базах данных информации, включающие в себя перечень, содержание и сроки реализации этапов мероприятий по созданию, развитию, вводу в эксплуатацию, эксплуатации и выводу из эксплуатации государственных информационных систем, дальнейшему хранению содержащейся в их базах данных информации.

Статья 13.27 (Нарушение требований к организации доступа к информации о деятельности государственных органов и органов местного самоуправления и ее размещению в сети «Интернет»), содержащаяся в Кодексе Российской Федерации об административных правонарушениях, за нарушение требований к технологическим, программным и лингвистическим средствам обеспечения пользования официальными сайтами государственных органов и органов местного самоуправления предусматривает наложение административного штрафа на должностных лиц в размере от 3 до 5 тыс. руб.

Вместе с тем, как отмечают специалисты, в интересах формирования и развития Единого информационного пространства (ЕИП) России необходимо определить приоритетные направления развития законодательной основы этой деятельности. В частности, следует рассмотреть федеральные законопроекты «О телевизионном вещании и радиовещании», «Об обеспечении участия Российской Федерации в структуре международной электросвязи», «Об информационном обеспечении органов государственной власти», «Об обеспечении информационного взаимодействия Российской Федерации и субъектов Российской Федерации», «О защите русского языка»; «Об информационной безопасности», а также о внесении изменений в законодательство о СМИ, в том числе электронных, с целью ограничения регионального сепаратизма и негативного воздействия, оказываемого на российское общественное мнение нашими зарубежными оппонентами. Необходимо объединить усилия широкой общественности, профессионалов, представителей органов власти, делового мира для решения исключительно важной в настоящее время для национальной безопасности России задачи – эффективного и безопасного построения ЕИП страны. Теоретическое осмысление этих проблем и правовое обоснование их решения является важнейшей задачей юридической науки и информационного права [3].

В рассматриваемом плане следует обозначить и ряд других важнейших проблем, связанных с обеспечением безопасности отечественной виртуальной среды. Практически все важнейшие хозяйствующие субъекты в России, не говоря уже о рядовых пользователях компьютерной техники, – до сих пор работают на иностранном программном обеспечении и оборудовании. На закупку всего этого «добра» за последние десятилетия истрачены сотни миллиардов долларов. В результате вероятный противник с помощью всевозможных «спящих» вредоносных программ и созданных в этом оборудовании преднамеренных уязвимостей получает возможность контролировать нас изнутри и при случае делать с нами всё что угодно [4, с. 1, 8, 9]. Поэтому весьма серьезную проблему в данном контексте представляет отсутствие на сегодняшний день отечественных предприятий, которые на отечественной элементной базе выпускали бы отечественные процессоры, контроллеры и прочие компоненты [5, с. 8–9].

По словам известного IT-эксперта, одного из разработчиков отечественной операционной системы А. Смирнова, если мы хотим избавиться от технологической зависимости в рассматриваемой сфере, необходимы значительные вложения для того, чтобы создать новую отрасль промышленности, целую новую индустрию [6].

В связи с этим одним из главных направлений усиления безопасности компьютерных сетей является активное импортозамещение. Специалисты

заговорили об этом уже давно[1]. Ещё в 2013 г. был издан Указ Президента РФ от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (ГосСОПКА)[2]. Из опубликованных в открытом доступе материалов видно, что полномочия по созданию системы, которая должна обеспечивать безопасность информационной инфраструктуры как в самой России, так и в диппредставительствах Российской Федерации за рубежом, этим указом были возложены на ФСБ России. Впоследствии её специалистами была создана и в настоящее время успешно развивается новейшая информационная система, предназначенная для «обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы страны». Органами федеральной службы безопасности разработана также методика обнаружения компьютерных атак и определён порядок обмена информацией между федеральными органами власти в случае их возникновения. В рамках решения поставленных задач в Вооружённых Силах РФ появились войска информационных технологий, о чем 22 февраля 2017 г. официально заявил министр обороны России С.К. Шойгу[3].

Следует напомнить, что задачи по переходу на отечественный софт и защите информационной инфраструктуры закреплены в двух федеральных проектах национальной программы – «Цифровая экономика» – «Информационная инфраструктура» и «Информационная безопасность». В утверждённом перечне поручений по итогам «Прямой линии» с главой государства, состоявшейся 20 июня 2019 г., Президент России В.В. Путин поручил Правительству представить предложения по обеспечению технологической независимости и безопасности КИИ России за счёт использования преимущественно отечественного программного обеспечения. Исполнить поручение главы государства Правительство должно было к 1 октября 2019 г.[4], и многое в этом направлении было сделано. Продолжением этого процесса явилась подготовка проекта Указа Президента РФ «О мерах экономического характера по обеспечению технологической независимости и безопасности объектов критической информационной инфраструктуры»[5], где отмечается, что к 2025 г. объекты КИИ РФ переведут преимущественно на отечественное оборудование. Согласно этому документу, Правительству необходимо утвердить требования к программному обеспечению и оборудованию, используемому на объектах КИИ, а также порядок перехода в рамках активного импортозамещения на российский софт и оборудование. Под «преимущественным» понимается приоритетное использование российского ПО и (или) оборудования при наличии соответствующих российских аналогов[6]. Однако, по мнению руководителей некоторых хозяйствующих субъектов, такой переход в материальном плане является

---

[1] В российской армии официально созданы кибервойска // Вести.RU. URL: http://www.vesti.ru/doc.html?id=2858596 (дата обращения: 24.10.2022).

Критическую информационную инфраструктуру защитят отечественным ПО // Концорциум Кодекс. 2019. 4 июля // URL: https://kodeks.ru/news/read/kriticheskuu-informacionnuu-infrastrukturu-zaschityat-otechestvennym-po (дата обращения: 18.03.2021).

Объекты критической информинфраструктуры переведут на российское оборудование к 2025 году // ТАСС. 2020. 29 октября // URL: https://tass.ru/ekonomika/9851951 (дата обращения: 18.03.2021).

[2] Российская газета. 2013. 18 января.

[3] В российской армии официально созданы кибервойска // Вести.RU. URL: http://www.vesti.ru/doc.html?id=2858596 (дата обращения: 24.10.2022).

[4] Критическую информационную инфраструктуру защитят отечественным ПО // Концорциум Кодекс. 2019. 4 июля // URL: https://kodeks.ru/news/read/kriticheskuu-informacionnuu-infrastrukturu-zaschityat-otechestvennym-po (дата обращения: 18.03.2021).

[5] URL: https://storage.consultant.ru/ondb/attachments/ 202011/02/Proekt_ukaza_Prezidenta_RF_fAT.pdf.

[6] Объекты критической информинфраструктуры переведут на российское оборудование к 2025 году // ТАСС. 2020. 29 октября // URL: https://tass.ru/ekonomika/9851951 (дата обращения: 18.03.2021).

весьма затратным и по своим темпам не может быть осуществлён в установленные сроки [7].

В этом случае, как отмечают некоторые специалисты, на переходный период для защиты российской КИИ можно обойтись относительно дешёвым, но весьма эффективным способом – за счёт широкого применения технологий, разработанных, испытанных и внедрённых ещё в конце 1990-х – начале нулевых годов в Санкт-Петербургском Государственном научном центре РФ «Центральный научно-исследовательский и опытно-конструкторский институт робототехники и технической кибернетики». Они связаны с созданием защитных программ-невидимок, реализованных в микропроцессорах (так называемый «компьютерный стелс»). В основе этой системы – защита не отдельных приложений или сервисов, например электронной почты или веб-приложений, а инфраструктуры обмена информацией в целом. Сами средства защиты должны быть неуязвимы для нападения, как, например, известные «межсетевые экраны» (невидимые «сетевые агенты»). Они не имеют ни физических, ни логических (IP) адресов и надёжно защищают от любых проникновений. Самое главное, что для их успешной работы не надо менять «железо» и даже придумывать свою операционную систему. «Сетевые агенты» – по сути, микропрограммы, не видимые никому. Они сами управляют потоками команд и информацией, оставаясь невидимыми и недоступными противнику.

Данные технологии могут и должны быть положены в основу российской глубокоэшелонированной системы защиты объектов КИИ, включая частные приложения, операционные системы, облачные структуры и телекоммуникационные каналы связи. В этом плане можно наладить кооперацию с другими заинтересованными странами, например Китаем или Индией [8, с. 1, 8, 9].

Таким образом, для успешного создания эффективного и безопасного единого информационного пространства России, которое находится сейчас в стадии формирования, следует стремиться к закреплению тех положительных тенденций в данной сфере, которые наметились в последнее время. В этой связи необходимо объединить усилия широкой общественности, профессионалов, представителей органов государственной власти и делового мира.

Библиографический список.

1. Старостин В.И. Правовые проблемы информационной войны. – М.: Военный университет, 2000 // URL: http://www.refstar.ru/data/r/print.file/id.15121_1.html (дата обращения: 19.10.2022).
2. Ягудин А. Проблемы привлечения к уголовной ответственности по ст. 274 УК РФ // URL: http://adel-yagudin.livejournal.com/4185.html (дата обращения: 02.10.2022).
3. Лопатин В.Н. Теоретико-правовые проблемы защиты единого информационного пространства и их отражение в системах российского права и законодательства. // URL: http://www.for-expert.ru/problemy_inform_prava/15.shtml (дата обращения: 09.10.2022).
4. Угланов А. Кто парализовал Москву 10 марта? // Аргументы недели. 2021. № 10.
5. Чуйков А. Россия: отстать навсегда? // Аргументы недели. № 27(671). 2019. 17 июля.
6. Васильченко С. Россия проигрывает Третью мировую войну: технологическое от-ставание стало критическим. Почему страна стала аутсайдером в IT-конкуренции // MKRU. 2019. 19 августа // URL: https://www.mk.ru/politics/2019/08/19/rossiya-proigryvaet-tretyu-mirovuyu-voynu-tekhnologicheskoe-otstavanie-stalo-kriticheskim.html (дата обращения: 23.10.2022).

7. Подобедова Л., Сидоркова И., Галимова Н. Глава «Газпрома» оценил в ₽180 млрд переход компании на российское ПО // РБК. 2021. 23 марта // URL: https://www.rbc.ru/business/23/03/2021/605887c89a79476b5398b6ab?utm_source=yxnews&utm_medium=desktop (дата обращения: 23.10.2022).
8. Угланов А. Кто парализовал Москву 10 марта? // Аргументы недели. 2021. № 10.

SOME ASPECTS OF ORGANIZATIONAL AND LEGAL PROTECTION OF INFORMATION AND TELECOMMUNICATION SYSTEMS

E.N. Yakovets
Russian Customs Academy, Lyubertsy
email: koshka997@mail.ru

Annotation. This article analyzes the content of the regulatory framework for the protection of information and telecommunications systems in the Russian Federation. Particular attention in terms of the formation of a unified information space in Russia is paid to the protection of state virtual networks, primarily critical information infrastructure. It is concluded that it is necessary to identify priority areas for the development of the legislative framework of this activity. Another unsolved problem is import substitution in the field of computer equipment production and software development.

Keywords: information and telecommunication systems, closed non-governmental (corporate) systems, critical information infrastructure, import substitution.