УДК 349:004.056

Н.М. Курбатов

О ФОРМИРОВАНИИ ПРАВОВЫХ И НАУЧНЫХ ОСНОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Проводится анализ понятия критической информационной инфраструктуры. Рассматривается история его становления и закрепления в правовом пространстве российского законодательства. В статье изучается опыт зарубежных стран в сфере обеспечения информационной безопасности в целом и защите критической инфраструктуры в частности. Актуальность выбранной темы обусловлена курсом, взятым Российской Федерацией на развитие информационного общества в стране, а также необходимостью защиты значимых информационных систем и ресурсов органов государственной власти. Автором статьи раскрываются термины, входящие в определение критической информационной инфраструктуры, закрепленное в законодательстве Российской Федерации. В заключение выделяются основные проблемы рассмотренных нормативно-правовых актов, даются рекомендации по дальнейшему развитию системы информационной безопасности критической инфраструктуры.

Ключевые слова: критическая информационная инфраструктура, компьютерные атаки, компьютерные преступления, объекты критической информационной инфраструктуры, информационная безопасность, международная информационная безопасность.

DOI: 10.35634/2412-9593-2019-29-5-644-654

Современный мир подвергается изменениям, связанным с развитием информационных и цифровых технологий. Глобальное информационное пространство, формирующееся в настоящее время, создает все новые возможности и перспективы для развития государств, в том числе экономических, политических и культурных преобразований. Однако наряду с положительными аспектами развития информационных технологий присутствуют и негативные аспекты, создающие новые угрозы как на уровне отдельных стран, так и в мире в целом. Рост зависимости государств от информационных систем, их проникновение во все сферы человеческой жизни способствуют развитию компьютерных преступлений и компьютерных атак на объекты критической информационной инфраструктуры. Кроме того, это приводит к возникновению новых конфликтов международного уровня, в том числе к появлению таких угроз, как международные хакерские атаки, информационные войны и т. д. [1].

Развитие данных угроз стало основной причиной, по которой практически все современные государства стали рассматривать информационную безопасность как элемент национальной безопасности страны. Особое внимание в процессе обеспечения информационной безопасности уделяется объектам критической инфраструктуры – информационным системам (объектам), представляющим особую важность для экономики и безопасности государства (атомная отрасль, военно-промышленные объекты, банковская сфера и т. п.).

Целью данной работы является исследование истории формирования и развития понятия критической информационной инфраструктуры, а также изучение международного опыта в сфере построения систем национальной безопасности.

Следует отметить, что ряд объектов критической информационной инфраструктуры в настоящее время находится во владении частного сектора [2], поэтому к одной из основных задач государства также можно отнести создание координирующих органов, осуществляющих свою деятельность в основных секторах критической инфраструктуры государства, а также занимающихся разработкой и принятием нормативно-правовых актов, регулирующих взаимоотношения субъектов в указанных сферах.

Актуальность выбранной темы обусловлена курсом, взятым Российской Федерацией на развитие информационного общества в стране, а также необходимостью защиты значимых информационных систем и ресурсов органов государственной власти.

В настоящее время в международном сообществе отсутствует общепринятое определение критической информационной инфраструктуры. Самым значимым документом, целью которого является регулирование правоотношений в информационной сфере, стала Конвенция о преступности в сфере компьютерной информации 2001 г. [3]. Данная конвенция не содержит прямого упоминания крити-

ческой информационной инфраструктуры, однако термины и положения, используемые в ней (компьютерные сети, защита целостности данных, неправомерное использование компьютерных систем), косвенно относятся к регулированию, в том числе, правоотношений в сфере критической информационной инфраструктуры. Указанный документ ратифицирован 53 странами, включая государства Европейского союза, Японию и США. Однако положения, регламентирующие возможность проведения международных следственных действий на территориях других государств без получения официального согласования, стали главной причиной, по которой Российская Федерация отказалась от ратификации данной Конвенции.

Отсутствие четко выработанного понятия критической информационной инфраструктуры привело к тому, что каждое государство в настоящее время самостоятельно подходит к определению данного термина и классификации таких объектов. Перечни объектов, относимых к критически важной инфраструктуре, отличаются в зависимости от традиций, географических и исторических особенностей страны, а также по иным общественно-политическим причинам.

Например, в США под критической инфраструктурой понимают системы и ресурсы (как виртуальные, так и физические), нарушение функционирования которых (в том числе их разрушение) может оказать влияние на военно-политическую безопасность страны, общественный порядок, экономическую ситуацию, а также привести к негативному влиянию на здоровье граждан [4].

В настоящее время к основополагающим нормативно-правовым актам США в сфере обеспечения информационной безопасности можно отнести «Национальную стратегию кибернетической безопасности» (“The National Strategy to Secure Cyberspace” [5]) и «Национальную стратегию физической информационной безопасности критической инфраструктуры» (“The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets” [6]), разработанные Департаментом внутренней безопасности США и принятые в феврале 2003 г. Основной целью указанных документов является попытка обеспечить эффективное взаимодействие по вопросам защиты критической инфраструктуры государства.

Катализатором развития систем, обеспечивающих информационную безопасность страны, послужило увеличение числа компьютерных атак, совершаемых против объектов государственной информационной инфраструктуры, а также террористические атаки 11 сентября 2001 г., после которых защита критически важных инфраструктурных объектов стала приоритетным направлением в сфере безопасности государства [7].

Не меньший интерес для исследования представляет система обеспечения информационной безопасности Китая. Китайская экономика является второй по значимости в мире. Кроме того, данное государство известно закрытостью Интернета и спецификой законодательства в сфере информационных технологий.

Первоначальная редакция Уголовного кодекса Китая (1997 г.) включала 3 специфические статьи, регулирующие правоотношения в сфере компьютерных преступлений. Так, ст. 285 Уголовного кодекса Китая регламентировала уголовную ответственность за получение неправомерного доступа к информационным системам (ресурсам), имеющим особую важность в масштабах страны или связанным с деятельностью органов государственной власти и обороноспособностью страны [8]. Перечень объектов, включенных в состав данной статьи, позволяет провести аналогию с объектами критической информационной инфраструктуры в терминологии современного отечественного права.

Позже властями Китая были приняты поправки в Уголовный кодекс (2009 и 2015 гг., ст. 285, 286A, 287A, 287B) [9], которые вводили ответственность за преступления, совершаемые при помощи информационных систем, в том числе была установлена ответственность за повреждение, уничтожение или модификацию особо важной информации или систем. Кроме того, Уголовным кодексом было криминализировано виртуальное содействие совершению компьютерных атак и преступлений. Следовательно, рассмотренные выше статьи Уголовного кодекса Китая регулируют правоотношения в сфере обеспечения информационной безопасности объектов критической информационной инфраструктуры Китая.

Подводя итог, отметим, что в настоящее время в законодательстве Китая закреплена правовая мера за компьютерные преступления, в том числе совершаемые в отношении объектов критической инфраструктуры. При этом к правонарушителям могут также применяться традиционные положения уголовного законодательства в случае использования современных информационных систем (технологий) при совершении иных преступлений.

При изучении зарубежного опыта обеспечения безопасности объектов критической информационной инфраструктуры отдельное внимание следует уделить Конвенции Африканского союза о кибербезопасности и защите персональных данных. Данный документ был принят 27 июня 2014 г., однако за прошедшие годы Конвенция была подписана 11 государствами, а ратифицирована лишь 4 государствами [10]. Таким образом, данный нормативно-правовой акт является больше программным документом, включающим основополагающие принципы сотрудничества между государствами в сфере информационных технологий.

Вопросам противодействия компьютерным преступлениям и обеспечения кибербезопасности посвящена гл. 3 данной Конвенции [11]. В частности, в данной главе устанавливается необходимость принятия национальной политики по противодействию преступлениям в сфере информационных технологий, а также признания важности защиты критической информационной инфраструктуры. Страны, подписавшие данный документ, обязаны принимать все необходимые меры для противодействия киберпреступности. При этом важной частью Конвенции является специальное указание (ч. 3 ст. 25), что принимаемые в рамках реализации положений Конвенции меры не должны противоречить иным международным договорам и нарушать права человека.

Приоритетность обеспечения защищенности критической информационной инфраструктуры закреплена в ч. 4 ст.25 [11]. Согласно данному положению, защита критической инфраструктуры представляет собой наиболее важную часть политики в сфере обеспечения информационной безопасности, поскольку она обеспечивает благополучие экономики, а также стабильность национальной безопасности. Кроме того, данное положение закрепляет установление более строгих санкций за преступления, совершенные против объектов критической информационной инфраструктуры.

Одним из государств, преуспевших в сфере обеспечения информационной безопасности, считается Сингапур. В 2018 г. законодательство Сингапура об информационной безопасности было дополнено новыми положениями, а акт о кибербезопасности Сингапура, принятый в 2018 г. (Cybersecurity Act), считается законом нового поколения в сфере обеспечения кибербезопасности государства.

Формулирование понятия критической информационной инфраструктуры проходило в Сингапуре в несколько этапов, первым из которых было принятие в 2016 г. Стратегии национальной кибербезопасности (National Cyber security Strategy) [12]. В данном документе был закреплен список секторов критической инфраструктуры:

– государственные и аварийные службы;
– здравоохранение;
– средства массовой информации;
– банковский и финансовый сектор;
– коммунальные службы;
– транспорт.

Позже в 2018 г. парламентом Сингапура был принят акт о кибербезопасности (Cyber Security Act), в котором классификация объектов критической информационной инфраструктуры проводилась в рамках термина «существенных служб». В свою очередь, под этим термином понимались любые службы, использующиеся в сфере обеспечения национальной безопасности, экономики, международных отношений, общественного порядка, безопасности и здравоохранения [13].

В Стратегии национальной кибербезопасности Сингапура закреплено четкое определение объектов критический информационной инфраструктуры, под которыми понимают «компьютер или компьютерные системы, полностью или частично находящиеся на территории Сингапура и необходимые для функционирования существенных служб, в случае утери контроля над которыми (или причинение вреда которым) окажет прямое воздействие на доступность указанных служб» (Там же).

В рамках реализации Стратегии был утвержден Регламент по обеспечению кибербезопасности объектов критической инфраструктуры (Cyber security (Critical Information Infrastructure) Regulations). Данный нормативно-правовой акт содержит положения по идентификации объектов критической инфраструктуры, регламентирует права и обязанности субъектов правоотношений, степень их правовой защищенности.

Формирование понятия критической информационной инфраструктуры в Российской Федерации шло своим чередом. Одной из первых попыток защиты компьютерной информации, а также обеспечения безопасности компьютерных коммуникаций в Российской Федерации стало принятие Закона от 23 сентября 1992 г. № 3523-1 «О правовой охране программ для электронных вычисли-

тельных машин и баз данных» [14]. Однако указанный документ не рассматривал такое понятие, как объект критической инфраструктуры. Данное понятие впервые было закреплено в законодательстве Российской Федерации 1994 г., а именно, было регламентировано Федеральным законом от 21 декабря 1994 г. № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» [15], который содержал следующее определение критического объекта: «Это объект, вмешательство в функционирование которого, приведет к потере управления экономикой Российской Федерации, субъекта Российской Федерации или административно-территориальной единицы субъекта Российской Федерации, необратимому негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения...».

Следующий шаг в развитии понятия критической информационной инфраструктуры был сделан в 2006 г., когда в Государственную думу был внесен законопроект «Об особенностях обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры», который, однако, был отозван в 2008 г. в связи с отсутствием денежных средств, необходимых для его реализации, а именно, для создания единой государственной системы контроля над информационно-телекоммуникационными системами. Кроме того, в полномочия указанной структуры должно было входить ведение реестра критически важных объектов и подготовка квалифицированных сотрудников [16].

Рассматривая появление термина критической информационной инфраструктуры в российском законодательстве, не стоит забывать и об Указе Президента Российской Федерации от 3 февраля 2012 года № 803 «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» [17]. Указанный документ напрямую не регулирует правоотношения в сфере критической информационной инфраструктуры, однако он заложил основу для формирования нормативно-правовой базы в области обеспечения информационной безопасности объектов критической инфраструктуры. Именно на основе рассмотренного нормативного правового акта был разработан Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры».

Кроме того, в 2014 г. временной комиссией Совета Федерации по развитию информационного общества был представлен «Проект стратегии кибербезопасности России» [18]. Целью документа являлась необходимость в обеспечении кибербезопасности личности, организации и государства. В рамках стратегии планировалось формирование культуры информационной безопасности, а также повышение цифровой грамотности граждан страны. Кроме того, принципы стратегии базировались, в том числе, на обеспечении информационной безопасности объектов критической информационной инфраструктуры. Однако проект стратегии не принят до настоящего времени.

Бурное развитие законодательства в сфере обеспечения безопасности критической информационной инфраструктуры получило в последние годы. Это связано с принятием ряда важных нормативно правовых актов. В настоящее время к документам, регулирующим указанную сферу, можно отнести: Конституцию Российской Федерации, Доктрину информационной безопасности Российской Федерации 2016 г., Стратегию национальной безопасности Российской Федерации до 2020 г., Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и другие.

Так, существенную роль в развитии понятия критической информационной инфраструктуры сыграла Доктрина информационной безопасности Российской Федерации, утвержденная 5 декабря 2016 г. Указом Президента Российской Федерации № 646. Указанный нормативно-правовой акт заменил Доктрину информационной безопасности от 9 сентября 2000 г. В рамках этого документа раскрывается текущее состояние, а также направление развития информационной безопасности Российской Федерации. Особую важность представляет то, что данные понятия рассматриваются с учетом национальных приоритетов стратегического развития, регламентированных Стратегией национальной безопасности Российской Федерации.

Содержание новой Доктрины более последовательно и структурировано по сравнению с ее предшественником. Это, в свою очередь, позволяет выстраивать все документы, регулирующие сферу информационной безопасности, в иерархическую структуру с учетом национальных приоритетов стратегического развития страны. Кроме того, положения данного документа соответствуют современным тенденциям в сфере информационных систем и технологий, фокусируются на обеспечении

информационной безопасности критически важной инфраструктуры Российской Федерации и противодействии кибератакам на нее.

Не меньшую роль в развитии правовой основы противодействия компьютерным атакам на объекты критической информационной инфраструктуры сыграла «Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы» (утверждена Указом Президента Российской Федерации от 9 сентября 2017 года № 203) [19]. Указанный документ определяет основные цели и задачи в вопросе обеспечения информационной безопасности, а также регламентирует меры внутренней и внешней политики в сфере применения информационных технологий.

Данная Стратегия вводит такие понятия, как «Интернет вещей», «информационное пространство», «критическая информационная инфраструктура», «объекты критической информационной инфраструктуры», «туманные вычисления» и другие. Кроме того, данный документ содержит положения о приоритетности защиты объектов критической информационной инфраструктуры (пп. 15 и 29) [19], а также указывает на необходимость обеспечения комплексной защиты информационной инфраструктуры Российской Федерации, в том числе с использованием государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы и системы критической информационной инфраструктуры.

Существенный вклад в развитие нормативной базы, связанной с вопросами обеспечения безопасности критической информационной инфраструктуры, внесли документы федеральной службы по техническому и экспертному контролю Российской Федерации (далее – ФСТЭК России). Разработанные ФСТЭК России документы были направлены на регулирование ключевых систем информационной инфраструктуры. К основным документам данной категории относятся:

«Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры»;

«Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры»;

«Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры»;

«Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры»;

«Положение о реестре ключевых систем информационной инфраструктуры».

ФСТЭК России также была предпринята попытка по категорированию объектов управления органов государственной власти с целью обеспечения их безопасности («Методика категорирования объектов управления органов государственной власти, органов местного самоуправления и организаций по важности защиты от иностранных технических разведок», утверждена первым заместителем директора ФСТЭК России 25 декабря 2009 года).

К числу основополагающих документов в сфере информационной безопасности можно отнести и документ Совета Безопасности от 08 ноября 2005 года «Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий». Однако данный нормативно-правовой акт отнесен к категории документов с грифом «секретно».

Указанные нормативно-правовые акты содержат следующее определение ключевой информационной инфраструктуры: «Это системы, обеспечивающие управление потенциально опасными производствами или технологическими процессами на объектах, а также обеспечивающие функционирование информационно-опасных объектов, осуществляющих управление (или информационное обеспечение управления) чувствительными (важными) для государства процессами (за исключением процессов на потенциально опасных объектах)» [20].

Таким образом, несмотря на принятие новых нормативно-правовых актов, а также на признание некоторых из них утратившими силу, рассмотренные документы сыграли значимую роль в становлении современного законодательства в сфере информационной безопасности. При этом «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры», а также «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры», утвержденные ФСТЭК России 18 мая 2007 г., могут применяться для моделирования угроз безопасности информации на значимых объектах критической информа-

ционной инфраструктуры Российской Федерации до утверждения ФСТЭК России соответствующих методических документов [21].

Рассматривая историю становления понятия критической информационной инфраструктуры в Российской Федерации, стоит также отметить значительный вклад, внесенный научным сообществом в данную сферу. Так, В.А. Чабанян в своей работе «Анализ и синтез требований к системам безопасности объектов критической информационной инфраструктуры» проводит анализ формирования требований, предъявляемых системам безопасности объектов критической информационной инфраструктуры и выделяет следующие отличительные особенности, на которые необходимо обращать внимание [22]:

– качественное развитие критической информационной инфраструктуры вместе с повсеместным увеличением потенциальной эффективности и технического уровня данных систем приводит к повышению требований к системам безопасности объектов;

– необходимо проводить разработку сценариев (условия эксплуатации критической инфраструктуры, целей и задач систем безопасности) перед формированием требований;

– применение математических моделей к формированию требований систем безопасности ограничивается фактором неопределенности исходной информации о развитии научно-технического прогресса и поведению внешней среды.

В данной работе автором также предложена структура процесса формирования требований к системам безопасности объектов на основе систем новейших достижений научно-технического прогнозирования и проведения проблемных фундаментальных исследований [22].

А.В. Коротков и Е.С. Зиновьева в своей работе «Безопасность критических информационных инфраструктур в международном гуманитарном праве» рассматривают вопрос применимости международного гуманитарного права к информационным войнам. Авторы приходят к выводу, что положения данной области права «устарели лишь формально, но не по сути». Кроме того, в данной работе рассматривается и критическая информационная инфраструктура. Авторы делают следующие выводы [23]:

− защищенные и незащищенные объекты критической информационной инфраструктуры тесно переплетены между собой в информационном пространстве;

− гуманитарные объекты критической информационной инфраструктуры не обладают отличительными знаками, отмечающими их особый правовой статус.

На основании проведенного исследования авторы предлагают привлекать представителей бизнеса, экспертного сообщества и гражданского общества к вопросам обеспечения международной правовой защиты критической информационной инфраструктуры, а также использовать отличительные знаки для защищенных объектов в информационной сфере [23].

Г.А. Остапенко, Д.Г. Плотников, А.С. Рогозина в работе «Жизнестойкость элементов критической информационной инфраструктуры: аналитическая оценка с учетом возможных ущербов» рассматривают параметры функции риска для элементов критической информационной инфраструктуры на основе параметров рисков и их компонентов. Авторами предлагаются способы расчета риска для сложных многокомпонентных систем, учитывающих как синхронные, так и асинхронные атаки. Предложенные формулы дают возможность оценки риска совместного и несовместного воздействия дестабилизирующих факторов, а также жизнестойкости системы, что, как следствие, позволяет адекватно классифицировать степень защищенности инфраструктуры и точнее прогнозировать ущерб от потери работоспособности данных объектов [24].

А.О. Калашников, Е.А. Сакрутина также рассматривают модель оценки безопасности критической информационной инфраструктуры на основе прогнозирования рисков объектов, находящихся под воздействием компьютерных атак, в своей работе «Модель оценки безопасности критической информационной инфраструктуры на основе метода вейвлет-анализа». Они предлагают модель оценки безопасности, построенную на основе вейвлет-разложения. Дальнейшее исследование динамики коэффициентов вейвлет-разложения позволит точнее выявлять опасные события, способные нарушить безопасность критической информационной инфраструктуры в будущем [25].

Необходимо отметить и работу Д.Р. Хлестова и Ф.Т. Байрушиной «Роль критических объектов информационной инфраструктуры при защите информации», в которой рассматривается предназначение объектов критической информационной инфраструктуры при защите информации, а также проводится анализ самих объектов. Авторами сделаны следующие выводы [26]:

– внедрение новых технологий должно проводиться только по результатам положительного тестирования;

– обслуживание объектов критической информационной инфраструктуры должно проводиться только высококвалифицированными специалистами по информационной безопасности;

– внедрение новых технологий должно проводиться одновременно с оценкой риска и сопоставлением с возможной выгодой от внедрения.

Р.И. Захарченко и И.Д. Королев в своей работе «Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры, функционирующей в киберпространстве» в рамках разработки методики оценки устойчивости объектов КИИ предложили расширить свойство устойчивости за счет внедрения нового свойства – киберустойчивости. Внедрение данного свойства аргументируется новой средой функционирования ГИС Российской Федерации и применения кибероружия, что, как следствие, является причиной возникновения новых угроз и уязвимостей для объектов критической информационной инфраструктуры. Суть предлагаемой методики заключается в декомпозиции критической инфраструктуры на отдельные объекты, что в теории позволит однозначно дать оценку состоянию защищенности критической информационной инфраструктуры от компьютерных атак [27].

Наконец, В.Е. Новичков и И.Г. Пыхтин в работе «Социально-правовое обоснование введения уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» проводят исследование необходимости введения уголовной ответственности за преступления, совершенные в отношении критической информационной инфраструктуры. Свои выводы авторы подкрепляют статистикой увеличения числа компьютерных преступлений в последние годы, а также анализом ранее действовавшего законодательства Российской Федерации. Полученные результаты позволяют авторам сделать вывод об актуальности и необходимости введения уголовной ответственности за данные правонарушения [28].

Таким образом, можно сделать вывод, что проблемы становления критической информационной инфраструктуры нашли отклик у научного сообщества и анализируются во многих работах современных ученых и исследователей.

Однако перейдем к рассмотрению более важного документа, регулирующего правоотношения в вопросах защиты критической информационной инфраструктуры, – Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Данный Федеральный закон вводит новые термины: «критическая информационная инфраструктура» – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов, и «объекты критической информационной инфраструктуры» – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления объектами критической информационной инфраструктуры.

Позже Указом Президента Российской Федерации от 25 ноября 2017 г. № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 года № 1085» были внесены изменения в понятие критической информационной инфраструктуры, а именно была произведена замена термина «ключевые системы информационной инфраструктуры» на «значимые объекты критической информационной инфраструктуры» [29].

К базовым понятиям критической информационной инфраструктуры можно отнести термин «информационная инфраструктура» в целом. Определение информационной инфраструктуры Российской Федерации закреплено в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 05.12.2016 № 646. Так, под информационной инфраструктурой Российской Федерации понимается «совокупность объектов информатизации, информационных систем, сайтов в сети "Интернет" и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации» [30].

Не менее важным является определение информационной системы, закрепленное в Федеральном законе от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», согласно которому информационная система «это совокупность содержащейся в

базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств» [31]. Кроме того, в указанном Федеральном законе закреплено понятие информационно-телекоммуникационной сети (далее – ИТКС), под которым понимается «технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники» [32].

Немаловажную роль играет назначение информационных систем и ИТКС (в соответствии с перечнем критически важных сегментов информационной инфраструктуры), поскольку именно от него зависит отнесение последних к категории ключевых систем. Как было рассмотрено выше, к критически важным сегментам информационных систем и ИТКС отнесены системы, нарушение функционирования которых может привести к нарушению функционирования важных государственных процессов. Таким образом, к данным сегментам отнесены следующие системы: органов государственной власти и местного самоуправления, банковской и финансовой сферы, правоохранительных структур, навигационные и спутниковые системы, используемые в специальных целях и другие.

Следовательно, информационные системы и ИТКС, управляющие объектами из перечня критически важных сегментов, относятся к категории ключевых систем информационной инфраструктуры. Информация, обрабатываемая ключевыми системами, в свою очередь, признается критически важной, поскольку ее хищение, удаление или компрометация могут привести к деструктивному воздействию на объекты критической информационной инфраструктуры, нарушению их нормального функционирования.

Таким образом, на основании рассмотренных выше определений под ИТКС объектов критической информационной инфраструктуры Российской Федерации понимается ключевая система информационной инфраструктуры, управляющая или обеспечивающая информационное управление данным объектом, неправомерное воздействие на которую может привести к чрезвычайной ситуации или нарушению выполнения функций системы с последующими негативными последствиями.

Наконец, под автоматизированной системой управления субъектами критической инфраструктуры в соответствии с «Основными направлениями государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации», утвержденнымиУказом Президента Российской Федерации от 3 февраля 2012 г. № 803, понимают «комплекс аппаратных и программных средств, информационных систем и информационно-телекоммуникационных сетей, предназначенных для решения задач оперативного управления и контроля за различными процессами и техническими объектами в рамках организации производства или технологического процесса критически важного объекта, нарушение (или прекращение) функционирования которых может нанести вред внешнеполитическим интересам Российской Федерации, стать причиной аварий и катастроф, массовых беспорядков, длительных остановок транспорта, производственных или технологических процессов, дезорганизации работы учреждений, предприятий или организаций, нанесения материального ущерба в крупном размере, смерти или нанесения тяжкого вреда здоровью хотя бы одного человека и (или) иных тяжелых последствий» [33].

Подводя итог, отметим, что актуальность принятых в последние годы законопроектов очевидна. Практически все современные государства рассматривают вопрос обеспечения информационной безопасности критической инфраструктуры как вопрос национальной безопасности.

Дальнейшее развитие юридического противодействия компьютерным атакам в Российской Федерации требует продолжения выбранной политики в сфере обеспечения информационной безопасности и принятия новых нормативно-правовых актов. Кроме того, некоторой корректировки и совершенствования требует и уже принятое законодательство.

Так, определения, рассматриваемые в Федеральном законе от 26 июля 2017 г. № 187-ФЗ, раскрываются через другие, ранее не определенные в данном нормативно-правом акте понятия («критическая информационная инфраструктура», «объекты критической информационной инфраструктуры). Определение одних норм-дефиниций через другие не способствует адекватному правопониманию, усложняет его восприятие, а следовательно, и последующее применение нормативно-правового акта [34].

Подводя итог, можно отметить, что в текущих нормативных правовых актах присутствует дисбаланс понятийного аппарата между информационными и юридическими категориями. Данное положение характеризует попытки регулирования информационных систем с помощью права и подтверждается выводами отечественных правоведов, исследующих область информационного права.

Например, И.Л. Бачило в своих трудах отмечает усиление разрыва между информатикой и информационными правоотношениями [35].

В связи с этим со стороны государства необходимо дальнейшее усиление и совершенствование правового регулирования в области обеспечения информационной безопасности объектов критической информационной инфраструктуры, поскольку именно государство является гарантом безопасности критической инфраструктуры.

Закрепление терминологии информационных систем и критической информационной инфраструктуры в современном российском законодательстве является важным этапом в становлении эффективной системы обеспечения информационной безопасности. Однако очевидным является тот факт, что построение стабильной системы информационной безопасности должно проводиться параллельно с сотрудничеством с иностранными государствами и выработкой международно-правовых норм в сфере обеспечения безопасности критической информационной инфраструктуры.

СПИСОК ЛИТЕРАТУРЫ

1. Более 600 российских интернет-ресурсов были атакованы хакерами террористической организации ИГИЛ // Сайт компании «GroupIB». 25.03.2015. URL:http://www.group-ib.ru/media/bolee-600-rossijskih-internet-resursov-b/ (дата обращения: 21.02.2019).
2. Критическая инфраструктура // Сайт компании PandaSecurity. URL:http://www.cloudav.ru/upload/iblock/447/PAD_PAD360%20-%20Whitepaper%20-20Критические%20инфраструктуры.pdf (дата обращения: 24.02.2019).
3. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) // СПС « ГАРАНТ». URL:http://www.base.garant.ru/4089723/#ixzz5hoVgZCBJ (дата обращения: 23.02.2019).
4. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. H.R. 3162. // National Institutes of Health. URL: http://www.docviewer.yandex.ru/view/Patriot_Act_2001.pdf (дата обращения: 24.02.2019).
5. The National Strategy to secure cyberspace // Official website of the Department of Homeland Security. February 2003. URL: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (дата обращения: 22.02.2019).
6. National Strategy for the Physical Protection of Critical Infrastructures and Key Assets // Homeland Security Digital Library. February 2003. URL: https://www.hsdl.org/?abstract&did=1041 (дата обращения: 21.02.2019).
7. National Strategy to Secure Cyberspace // Wikipedia. URL: http://www.wikipedia.org/ wiki/National_Strategy_to_Secure_Cyberspace (дата обращения: 26.02.2019).
8. Уголовный кодекс Китайской Народной Республики (принят на 5-й сессии Всекитайского собрания народных представителей шестого созыва 14 марта 1997 г.) // Федеральный правовой портал «Юридическая Россия». URL: http://www.law.edu.ru/norm/norm.asp?normID= 1247252&subID=100110722,100110731,100110742,100110836,100111903#text (дата обращения: 25.02.2019).
9. Criminal Law of the People's Republic of China (Adopted by the Second Session of the Fifth National People's Congress on July 1, 1979) // Сайт Министерства иностранных дел Китайской Народной Республики. URL: http://www.fmprc.gov.cn/ce/cgvienna/eng/dbtyw/jdwt/crimelaw/t209043.htm (дата обращения: 27.02.2019)
10. List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection // Официальный сайт African Union. URL: http://www.au.int/sites/default/files/treaties/29560- sl-african_union_convention_on_cyb er_security_and_personal_data_protection_2.pdf (дата обращения: 25.02.2019).
11. African Union Convention on Cyber Security and Personal Data Protection // African Union. URL: http://www.au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (дата обращения: 25.02.2019).
12. Singapore`s Cyber security Strategy // Сайт Cyber Security Agency of Singapore. October 2016. URL:https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy (дата обращения: 26.02.2019).
13. Cybersecurity Act 2018 (No. 9 of 2018) // Government Gazette. 16.03.2018. https://sso.agc.gov.sg/Acts-Supp/9-2018/ (дата обращения: 24.02.2019).
14. Закон РФ от 23.09.1992 N 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных» (ред. от 02.02.2006) // Российская газета. 1992. 20 окт.
15. Федеральный закон от 21.12.1994 № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» (ред. от 23.06.2016) // Российская газета. 2004. 24 дек.
16. Законопроект №340741-4 «Об особенностях обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры» // Система обеспечения законодательной деятельности. URL: http://www.sozd.duma.gov.ru/bill/340741-4 (дата обращения: 26.02.2019).
17. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (утв. Президентом РФ 03.02.2012 № 803) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_150730/ (дата обращения: 27.02.2019).

18. Изотов С. Проект стратегии кибербезопасности России вынесен на общественное обсуждение // ТАСС. 2014. 10 янв. URL: https://tass.ru/politika/878279 (дата обращения: 28.02.2019).
19. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы (утверждена указом Президента Российской Федерации от 09.09.2017 № 203) // Информационно-правовой портал ГАРАНТ.РУ. URL: http:/www.garant.ru/products/ipo/prime/doc/71570570/ (дата обращения: 27.02.2019).
20. Информационное сообщение по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры в связи с изданием приказа ФСТЭК России от 14.03.2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» // Федеральная служба по техническому и экспортному контролю: Официальный сайт. URL: http://www.fstec.ru/component/attachments/download/715 (дата обращения 27.02.2019).
21. Информационное сообщение ФСТЭК от 4 мая 2018 г. № 240/22/2339 «О методических документах по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры российской федерации» // Федеральная служба по техническому и экспортному контролю: Официальный сайт. URL: https://fstec.ru/component/attachments/download/1865 (дата обращения 27.02.2019).
22. Чобанян В.А., Шахалов И.Ю. Анализ и синтез требований к системам безопасности объектов критической информационной инфраструктуры // Вопросы кибербезопасности. 2013. № 1. С. 17-27.
23. Коротков А.В., Зиновьева Е.С. Безопасность критических информационных инфраструктур в международном гуманитарном праве // Вестник МГИМО. 2011. № 4. С. 154-162.
24. Остапенко Г.А., Плотников Д.Г., Рогозина А.С. Жизнестойкость элементов критической информационной инфраструктуры: аналитическая оценка с учетом возможных ущербов» // Информационная безопасность. Воронежский гос. техн. ун-т. 2013. № 3. С. 353-364.
25. Калашников А.О., Сакрутина Е.А. Модель оценки безопасности критической информационной инфраструктуры на основе метода вейвлет-анализа // Информационная безопасность. Воронежский гос. техн. ун-т. 2017. № 4. С. 478-491.
26. Хлестова Д.Р., Байрушина Ф.Т. «Роль критических объектов информационной инфраструктуры при защите информации» // Аллея науки. 2017. № 14. С. 743-744.
27. Захарченко Р.И., Королев И.Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры функционирующей в киберпространстве // Наукоемкие технологии в космических исследованиях Земли. 2018. № 2. С. 51-60.
28. Новичков В.Е., Пыхтин И.Г. Социально-правовое обоснование введения уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // Психопедагогика в правоохранительных органах. 2018. № 2 (73). С. 25-29.
29. Указ Президента РФ от 25.11.2017 № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_283384/ (дата обращения: 27.02.2019).
30. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) Пункт 2, подпункт 3 // Российская газета. 2016. 6 дек.
31. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 18.12.2018) Статья 2, пункт 3 // Российская газета. 2006. 29 июля.
32. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 18.12.2018) Статья 2, пункт 4 // Российская газета. 2006. 29 июля.
33. Указ Президента РФ №803 от 03.02.2012 «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» Пункт 3б // Сайт Совета Безопасности Российской Федерации. URL:http://www.scrf.gov.ru/security/information/document113/ (дата обращения: 25.02.2019).
34. Головкин Р.Б. Юридическое противодействие кибератакам // Аллея науки. 2018. № 4 (20). С. 845-851.
35. Бачило И.Л. Информационное право: учебник для академического бакалавриата. М.: Юрайт, 2018. 419 с.

Поступила в редакцию 14.05.2019

Курбатов Николай Михайлович, соискатель кафедры информационного права в управлении
ФГБОУ ВО «Удмуртский государственный университет»
426034, Россия, г. Ижевск, ул. Университетская, 1 (корп. 1)
E-mail: nikolaiudgu@mail.ru

N.M. Kurbatov

ON THE FORMATION OF LEGAL AND SCIENTIFIC BASES OF ENSURING THE SAFETY OF CRITICAL INFORMATION INFRASTRUCTURE OF THE RUSSIAN FEDERATION

DOI: 10.35634/2412-9593-2019-29-5-644-654

The concept of critical information infrastructure is analyzed. The history of its formation and consolidation in the legal space of Russian legislation is considered. The article studies the experience of foreign countries in the field of ensuring information security in general and protecting critical infrastructure in particular. The relevance of the chosen topic is due to the course taken by the Russian Federation for the development of the information society in the country, as well as the need to protect significant information systems and resources of state authorities. The author of the article reveals the terms included in the definition of critical information infrastructure, enshrined in the legislation of the Russian Federation. In conclusion, the main problems of the considered regulatory legal acts are highlighted, recommendations are given on the further development of the information security system of critical infrastructure.

Keywords: critical information infrastructure, computer attacks, computer crimes, objects of critical information infrastructure, information security, international information security.

Received 14.05.2019

Kurbatov N.M., applicant at Department Information law in management
Udmurt State University
Universitetskaya st., 1/1, Izhevsk, Russia, 426034
E-mail: nikolaiudgu@mail.ru