Доверие и безопасность в информационном обществе

ЗАЩИТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ КАК НОВЫЙ ИНСТИТУТ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Статья рекомендована к публикации членом редакционного совета А.Н. Райковым 16.01.2020.

Ельчанинова Наталья Борисовна

Кандидат технических наук, доцент
Южный федеральный университет, Институт компьютерных технологий и информационной безопасности, Кафедра безопасности информационных технологий, доцент
Ростов-на-Дону, Российская Федерация
inf_2012@mail.ru

Аннотация

Статья посвящена исследованию правовых проблем обеспечения безопасности критической информационной инфраструктуры (КИИ). Рассмотрены примеры крупных общемировых кибератак и их последствий, существенно отразившихся на политической, экономической и международной обстановке в разных странах мира. Проведён анализ федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» и системы взаимосвязанных с ним ведомственных подзаконных актов. Рассмотрены понятие объектов КИИ, правила их категорирования и применяемые для этого критерии, а также порядок ведения Реестра значимых объектов КИИ. Исследованы основные этапы, организационные, правовые и технические особенности разработки и ввода в эксплуатацию системы обеспечения безопасности объекта КИИ в соответствии с требованиями ФСТЭК России. Рассмотрены функциональное назначение, задачи, структура Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). Исследованы процедуры обмена информацией о компьютерных инцидентах между субъектами КИИ и государственными органами. Выявлены правовые проблемы привлечения к уголовной ответственности за неправомерное воздействие на объекты КИИ. Сделан вывод о необходимости совершенствования законодательства в сфере обеспечения безопасности критической информационной инфраструктуры.

Ключевые слова

кибертерроризм, критическая информационная инфраструктура, категорирование объектов КИИ, информационная безопасность, защита информации, законодательство, компьютерная атака, ГосСОПКА, компьютерное преступление, уголовная ответственность.

Введение

Кибертерроризм становится общемировой проблемой. Целями кибератак могут выступать органы государственного управления, социальные учреждения, особо опасные производства, жилищно-коммунальная инфраструктура, объекты связи и транспорта, что может привести к катастрофическим последствиям для населения. Кибероружие используется как в недобросовестной внутриполитической борьбе, так и для получения преимущества в межгосударственном противостоянии.

История знает множество примеров крупных атак, существенно отразившихся на состоянии мировой экономики и политической обстановки.

Например, 1 мая 2000 г. на территории Азии в сеть был запущен компьютерный вирус «Iloveyou», который мгновенно распространился по всему миру, поразил более трёх миллионов компьютеров и практически парализовал деятельность государственных учреждений и коммерческих компаний разных государств. Федеральному бюро расследований США удалось установить, что кибератака была осуществлена с территории Филиппин, где на тот момент времени

отсутствовало законодательство, направленное против киберпреступности. Ущерб от воздействия данного вируса, нанесенный мировой экономике, оценивается примерно в 10–15 млрд долл. США [1, с. 191].

В июне 2010 г. был запущен вирус «Stuxnet», нацеленный против иранского завода по переработке ядерного топлива путём вывода из строя газовых центрифуг, в результате чего была заражена атомная электростанция в Бушере [2, с. 48]. Примечательно, что первичное заражение происходило не через сеть, а посредством использования так называемого «человеческого фактора». Далее вирус распространился на промышленные системы Китая и других стран, но техногенной катастрофы тогда, к счастью, не произошло. Позднее Хилари Клинтон косвенно признала, что вирус был разработан в США и направлен против ядерной программы Ирана.

В 2017 г. произошла массовая кибератака двух вирусных программ-шифровальщиков «WannaCry» и «Petya», которые требовали уплаты денежного выкупа за расшифровку данных на компьютере. Нападению были подвергнуты государственные организации, больницы, банки, транспортная инфраструктура по всему миру. Наиболее пострадали Россия, Украина, Индия, Тайвань, в Великобритании была парализована работа системы здравоохранения.

В марте 2019 г. появился новый вирус, который был использован для оказания политического давления на законное правительство Венесуэлы в целях совершения государственного переворота. Нападению подверглась автоматическая система контроля гидроэлектростанции «Гури», в результате чего вся страна осталась без электричества на несколько дней: без света оказались аэропорты, школы, больницы, начались волнения среди населения. Венесуэльские власти возложили ответственность за случившееся на США, которые тогда активно поддерживали оппозиционные силы. Президент Николас Мадуро отметил: «Вашингтон любыми способами провоцирует кризис, чтобы устроить в стране государственный переворот».

Государства всех стран мира осознали надвигающуюся угрозу и предпринимают активные попытки совершенствования законодательства в целях противостояния кибертерроризму. В России органы государственной власти уделяют вопросам обеспечения информационной безопасности значительное внимание, четко осознавая, что дальнейшее противостояние на межгосударственном уровне будет происходить в основном в информационной плоскости, и победу в нем сможет одержать страна, обладающая достаточными техническими средствами, кадровым потенциалом и законодательной базой для применения кибероружия и защиты от его воздействия. В 2016 г. Указом Президента РФ была принята «Доктрина информационной безопасности РФ», которая в качестве одного из главных стратегических направлений выделила пресечение использования иностранными государствами информационных технологий для нанесения ущерба национальной безопасности РФ [3].

В рамках реализации указанной Доктрины в июле 2017 г. был принят федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации», который впервые законодательно закрепил такие юридически значимые понятия, как «компьютерная атака», «компьютерный инцидент», «объекты критической информационной инфраструктуры» (далее — КИИ), а также установил основные требования в сфере обеспечения их безопасности [4]. Процесс принятия данного закона был достаточно долгим, поскольку теперь владельцы КИИ должны привести систему защиты указанных объектов в соответствие с требованиями закона, что требует от них значительных финансовых затрат [5, с. 73].

К объектам критической информационной инфраструктуры закон относит информационные системы, функционирующие в сфере здравоохранения, науки, транспорта, связи и энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, то есть фактически это больницы, аэропорты, вокзалы, банки, электростанции, опасные химические производства, кибератаки на которые могут вызвать глобальную гуманитарную катастрофу.

В целях определения уровня значимости объектов КИИ и соответствующих им мер защиты производится их категорирование в порядке, регламентированном постановлением Правительства РФ [6]. Правила категорирования основываются на оценке степени неблагоприятных последствий, которые могут наступить в результате атаки на объекты КИИ. Оценка осуществляется комиссией экспертов по соответствующим показателям в пяти различных сферах деятельности:

- в социальной сфере (причинение ущерба жизни и здоровью людей, нарушение функционирования объектов ЖКХ, транспорта, связи);

- в политической сфере (блокирование деятельности государственного органа, срыв подписания или нарушение условий международного договора);

- в экономической сфере (причинение ущерба бюджету РФ, государственным корпорациям и организациям с государственным участием, блокирование деятельности банков);

- в экологической сфере (неблагоприятное воздействие загрязняющих веществ на окружающую среду в зависимости от масштабов пораженной территории и количества пострадавших людей);

- в сфере обороны и безопасности государства (нарушение деятельности органов государственного управления различных уровней, прекращение работы информационных систем в области обороны страны или охраны правопорядка, снижение показателей гособоронзаказа).

По результатам оценки объекту КИИ присваивается одна из трёх категорий значимости (первая — самая высокая). Если значения ни по одному из критериев не превышают установленных показателей либо ни один из показателей неприменим к объекту КИИ, то категория значимости такому объекту не присваивается и повышенные требования к его защите не устанавливаются. Результаты категорирования оформляются актом комиссии, который должен быть направлен в Федеральную службу по техническому и экспортному контролю РФ (ФСТЭК) в течение 10 дней для включения в Реестр значимых объектов КИИ, порядок ведения которого регулируется приказом ФСТЭК РФ от 6.12.2017 г. № 227 [7].

Содержание и форма направляемых в Реестр сведений закреплены приказом ФСТЭК РФ от 22.12.2017 г. № 236 [8]. В состав указанных сведений наряду с выбранной категорией значимости входят также полное описание объекта КИИ, данные о субъекте КИИ и его должностных лицах, отвечающих за безопасность, информация об операторе связи и способах его взаимодействия с объектом КИИ, сведения об используемых сертифицированных средствах программно-аппаратной защиты информации, модель нарушителя, модель угроз, типы возможных компьютерных инцидентов и их последствий.

Субъекты КИИ несут полную ответственность за достоверность предоставляемых ими сведений, а также обязаны в случае их изменения направлять в ФСТЭК РФ соответствующие обновления и дополнения. Каждому объекту КИИ в Реестре присваивается индивидуальный регистрационный номер, включающий в том числе код федерального округа, где он территориально расположен, сферу его деятельности и тип объекта (информационная система, АСУ ТП или информационно-телекоммуникационная сеть). Сведения из Реестра ежемесячно направляются в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак. В целях обеспечения сохранности содержащейся в Реестре информации каждый месяц должно осуществляться резервное копирование данных на внешние машинные носители, которые потом хранятся не менее 5 лет.

Правильное определение категории значимости объекта КИИ играет важную роль в процессе дальнейшей разработки и ввода в эксплуатацию системы обеспечения его безопасности, требования к порядку создания которой содержатся в приказе ФСТЭК РФ от 21.12.2017 г. № 235 [9]. Руководствуясь этим приказом, можно выделить в процедуре создания системы безопасности объекта КИИ следующие основные этапы: описание объекта КИИ и его структурно-функциональных характеристик; построение модели угроз безопасности; формирование базового набора организационных и технических мер по обеспечению безопасности в соответствии с выбранной категорией значимости объекта КИИ с учетом их адаптации и дополнения; подбор средств защиты информации и разработка архитектуры подсистемы безопасности; разработка эксплуатационной документации; установка и настройка средств защиты информации; реализация организационных мер защиты.

Требования к организационным и техническим мерам защиты в отношении значимых объектов КИИ установлены приказом ФСТЭК РФ от 25.12.2017 г. № 239 [10]. Базовые меры защиты перечислены в п. 22 данного приказа. Там же содержится ссылка на необходимость использования методических рекомендаций ФСТЭК РФ, которые в настоящий момент пока еще не разработаны. Поэтому для данной цели можно предложить руководствоваться лишь действующей методичкой ФСТЭК РФ «Меры защиты информации в государственных информационных системах» [11] и пытаться применять ее «по аналогии».

Формирование набора мер защиты является основой для подготовки в дальнейшем частного технического задания на разработку системы обеспечения безопасности значимого объекта КИИ и включает три основных этапа: определение базового набора мер в соответствии с выбранной категорией значимости согласно таблице, содержащейся в приложении к приказу; адаптация

набора мер с точки зрения особенностей структурно-функциональных характеристик объекта КИИ; дополнение набора мер в случае если объект КИИ одновременно является государственной информационной системой, информационной системой обработки персональных данных или в нем используются средства криптографической защиты информации, поскольку в указанных областях приказами ФСТЭК РФ и ФСБ России установлены дополнительные требованиям к мерам защиты. Так как многие объекты КИИ являются государственными и обрабатывают персональные данные с применение криптографических средств защиты, выполнение последнего этапа всегда присутствует.

В процессе реализации системы обеспечения безопасности объекта КИИ необходимо использовать сертифицированные средства защиты информации, соответствующие его категории значимости (табл. 1). При этом для объектов первой и второй категорий значимости должны применяться средства защиты не ниже 4 уровня контроля отсутствия недекларированных возможностей.

Таблица 1. Соответствие сертификации средств защиты информации категориям значимости

Категория значимости объекта КИИ	Средства защиты информации	Средства вычислительной техники
1	4 класс защиты	5 класс
2	5 класс защиты	5 класс
3	6 класс защиты	5 класс

Функции государственного контроля соблюдения установленных требований в сфере обеспечения безопасности КИИ возложены на ФСТЭК России и осуществляются на основании постановления Правительства РФ [12]. Проверки могут быть плановыми (проводятся комиссией один раз в три года) и внеплановыми (могут осуществляться одним должностным лицом). Внеплановая проверка проводится в случае возникновения компьютерного инцидента, на основании поручения Президента РФ, Правительства РФ или требования прокурора, а также в случае истечения срока устранения выявленных ранее нарушений. По итогам проверки составляется акт и субъекту КИИ выдается предписание об устранении выявленных нарушений с указанием срока их устранения. Неисполнение выданного предписания в установленный срок влечет назначение административного штрафа для юридических лиц в размере от двухсот до пятисот тысяч рублей [13]. Неоднократное неисполнение выданных предписаний может привести к лишению субъекта КИИ лицензии на право осуществления соответствующего вида деятельности.

Во исполнение требований статьи 5 ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» была создана Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), в задачи которой входит: прогнозирование компьютерных атак; обеспечение взаимодействия владельцев информационных ресурсов, операторов связи и субъектов защиты информации; государственный контроль защищённости информационных ресурсов; выявление причин компьютерных инцидентов [14]. Координирует деятельность ГосСОПКи специально созданный для этого орган — Национальный координационный центр по компьютерным инцидентам (НКЦКИ), находящийся в ведении ФСБ России. Основное функциональное назначение НКЦКИ заключается в своевременном реагировании на компьютерные инциденты, а также обеспечении обмена информацией между субъектами КИИ о компьютерных атаках, способах их обнаружения и предупреждения [15].

Порядок обмена указанными видами информации, перечень и формы её предоставления в ГосСОПКу регулируются приказами ФСБ России от 24.07.2018 г. № 367 и № 368. Для обмена информацией используется специальный технический сервис, к которому могут быть подключены любые субъекты КИИ. Для тех, кто не имеет возможности подключения к данному сервису, был создан официальный сайт в сети интернет — http://cert.gov.ru, на котором любой желающий с помощью формы обратной формы связи может сообщить об обнаруженной им уязвимости или компьютерном инциденте.

Несмотря на активные действия со стороны государства, компьютерная преступность в России демонстрирует неуклонный рост на протяжении последних трёх лет, о котором свидетельствует официальная статистика МВД РФ [16] (табл. 2).

Таблица 2. Статистика МВД РФ о компьютерной преступности

Временной период	Количество зарегистрированных компьютерных преступлений	Рост по сравнению с предыдущим периодом
2017 год	1883	+ 7,7 %
2018 год	2500	+ 32,8 %
2019 год	2883	+ 15,3 %

В целях обеспечения безопасности критической информационной инфраструктуры Уголовный кодекс РФ был дополнен ст. 274.1, установившей повышенные меры ответственности за преступные посягательства в указанной сфере [17]. Фактически новая статья дублирует существующие составы, предусмотренные ст. 272–273 УК РФ, с той лишь разницей, что она содержит специальный объект — критическую информационную инфраструктуру РФ [18, с. 100]. Вероятно, именно этим и вызвана необходимость введения отдельной статьи, иначе можно было бы просто ограничиться дополнением указанных статей 28-й главы уголовного закона новыми частями. При этом специалисты отмечают ряд недостатков вновь принятой нормы. В частности, ч. 3 ст. 274.1 УК РФ предусматривает лишение свободы сроком до шести лет при отсутствии указания нижнего предела наказания, что позволяет назначить срок менее двух лет, то есть меньше, чем за аналогичное деяние по ч. 1 ст. 274 УК РФ [19, с. 240].

На основе проведенного анализа российского законодательства в сфере обеспечения безопасности критической информационной инфраструктуры можно видеть, что государство в последние годы ведет активную работу, направленную на совершенствование механизмов защиты объектов КИИ и государственного контроля в данной области. Указанные правоотношения регулируются не только федеральным законом, но еще и целой системой взаимосвязанных между собой ведомственных подзаконных актов. Четко разграничены полномочия между контролирующими органами. В частности, ФСТЭК РФ ведёт реестр объектов КИИ, устанавливает требования к созданию систем безопасности значимых объектов КИИ, осуществляет государственный контроль в данной сфере. К полномочиям ФСБ России отнесена деятельность Национального координационного центра по компьютерным инцидентам, утверждение переченя информации, предоставляемой в ГосСОПКу, обеспечение взаимодействия субъектов КИИ с государственными органами. Также законодатель учел необходимость ужесточения уголовной ответственности за киберпреступления, совершенные в отношении объектов КИИ.

Вместе с этим нельзя не отметить существующие проблемы действующего законодательства, к которым можно отнести следующие: слишком размытое определение понятия объекта КИИ в законе; недостаточно чётко регламентирована процедура определения категории значимости объектов КИИ; недостаточно эффективно налажен обмен информацией между субъектами КИИ и государственными органами; наличие пробелов в законодательстве об ответственности.

Возможно, в ближайшем будущем потребуется принять ряд изменений и дополнений, а также ряд ведомственных руководящих и методических документов, которые помогут субъектам КИИ в полном объёме выполнить новые возложенные на них государством обязанности.

Литература

1. Логинова Е.М. Кибертерроризм на заре новой эпохи // Уголовный закон: современное состояние и перспективы развития: материалы II Международной научно-практической конференции, приуроченной ко дню принятия Уголовного Кодекса РФ. Воронеж, 2018. С. 189–202.
2. Kushner D. The Real Story of Stuxnet // IEEE Spectrum. 2013. Vol. 50. Issue 3. Pp. 48–53. https://doi.org/10.1109/MSPEC.2013.6471059.
3. Доктрина информационной безопасности Российской Федерации, утв. Указом Президента РФ от 5 декабря 2016 г. № 646 // Собрание законодательства РФ. 2016. № 50. Ст. 7074.
4. О безопасности критической информационной инфраструктуры Российской Федера-ции: федеральный закон от 26 июля 2017 г. № 187-ФЗ // Собрание законодательства РФ. 2017. № 31 (ч. 1). Ст. 4736.

5. Ванцева И.О., Зырянова Т.Ю., Медведева О.О. Влияние федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» на владельцев критических информационных инфраструктур // Вестник УрФО. 2018. № 1(27). С. 71–76.
6. Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, утв. постановлением Правительства РФ от 8 февраля 2018 г. № 127 // Собрание законодательства РФ. 2018. № 8. Ст. 1204.
7. Приказ ФСТЭК РФ от 6 декабря 2017 г. № 227 «Об утверждении порядка ведения реестра значимых объектов критической информационной инфраструктуры Россий-ской Федерации» // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru (дата обращения: 09.02.2018).
8. Приказ ФСТЭК РФ от 22 декабря 2017 г. № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной ин-фраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» // Официальный интернет-портал право-вой информации. URL: http://www.pravo.gov.ru (дата обращения: 16.04.2018).
9. Приказ ФСТЭК РФ от 21 декабря 2017 г. № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной ин-фраструктуры Российской Федерации и обеспечению их функционирования» // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru (дата обращения: 22.02.2018).
10. Приказ ФСТЭК РФ от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной ин-фраструктуры Российской Федерации» // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru (дата обращения: 27.03.2018).
11. Меры защиты информации в государственных информационных системах: методиче-ский документ, утв. ФСТЭК РФ 11 февраля 2014 г. // Официальный сайт ФСТЭК России. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (дата обра-щения: 21.10.2019).
12. Правила осуществления государственного контроля в области обеспечения безопас-ности значимых объектов критической информационной инфраструктуры Россий-ской Федерации, утв. постановлением Правительства РФ от 17 февраля 2018 г. № 162 // Собрание законодательства РФ. 2018. № 9. Ст. 1393.
13. Кодекс РФ об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (часть 2 статьи 19.5) // Собрание законодательства РФ. 2002. № 1 (ч. 1). Ст. 1.
14. Указ Президента РФ от 22 декабря 2017 г. № 620 «О совершенствовании Государ-ственной системы обнаружения, предупреждения и ликвидации последствий компь-ютерных атак на информационные ресурсы Российской Федерации» // Собрание за-конодательства РФ. 2017. № 52 (ч. 1). Ст. 8112.
15. Положение о Национальном координационном центре по компьютерным инциден-там, утв. приказом ФСБ России от 24 июля 2018 г. № 366 // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru (дата обращения: 10.09.2018).
16. Состояние преступности в Российской Федерации // Официальный сайт МВД Рос-сии. URL: https://мвд.рф/reports/item/18556721 (дата обращения: 14.10.2019).
17. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (статья 274.1) // Собрание законодательства РФ. 1996. № 25. Ст. 2954.
18. Пыхтин И.Г. Уголовно-правовая охрана объектов критической информационной ин-фраструктуры как одно из ключевых направлений современной борьбы с киберпре-ступностью в Российской Федерации // Известия Юго-Западного государственного университета. Серия: История и право. 2018. Т. 8. № 1(26). С. 98–103.
19. Шульга А.В., Галиакбаров Р.Р. Уголовная ответственность за неправомерное воздей-ствие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1. УК РФ) // Гуманитарные, социально-экономические и общественные науки. 2018. № 5. С. 238–242.

PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE AS A NEW INSTITUTE OF LEGALLY ENFORCING INFORMATION SECURITY

Elchaninova Natalia Borisovna

Candidate of technical sciences, associate professor
Southern Federal University, Institute of Computer Technologies and Information Security, IT security department, associate professor
Rostov-on-Don, Russian Federation
inf_2012@mail.ru

Abstract

The article is dedicated to a research of law problems of security provision for critical information infrastructure (CII). There are described examples of great cyberattacks and their consequences which significantly affected on the political, economic and international situation in different countries. Analysis of the federal law "About the security of critical information infrastructure in Russian Federation" and system of related departmental by-laws is carried out. The concept of CII objects, rules of their categorization, criteria applied for this purpose and order of maintaining Register of significant CII objects are described. Milestones, organizational, legal and technical features of development and commissioning of the security provision system for CII objects in accordance with requirements of Federal Service for Technical and Export Control of Russia are investigated. Functional purpose, tasks, structure of the State system for detection, prevention and elimination of the consequences of computer attacks are described. Procedures of information exchange about computer incidents between CII entities and public authorities are investigated. Law problems of criminal prosecution for illegal impact on CII objects are manifested. It is concluded that improvement of legislation in the sphere of security provision for critical information infrastructure is necessary.

Keywords

cyberterrorism, critical information infrastructure, CII, categorization of CII objects, information security, information protection, legislation, computer attack, GosSOPKA, cybercrime, criminal responsibility

References

1. Loginova Ye.M. Kiberterrorizm na zare novoy epokhi // Ugolovnyy zakon: sovremennoye sostoyaniye i perspektivy razvitiya: materialy II Mezhdunarodnoy nauchno-prakticheskoy konferentsii, priurochennoy ko dnyu prinyatiya Ugolovnogo Kodeksa RF. Voronezh, 2018. S. 189–202.
2. Kushner D. The Real Story of Stuxnet // IEEE Spectrum. 2013. Vol. 50. Issue 3. Pp. 48–53. https://doi.org/10.1109/MSPEC.2013.6471059.
3. Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii, utv. Ukazom Prezidenta RF ot 5 dekabrya 2016 g. № 646 // Sobraniye zakonodatel'stva RF. 2016. № 50. St. 7074.
4. O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federa-tsii: federal'nyy zakon ot 26 iyulya 2017 g. № 187-FZ // Sobraniye zakonodatel'stva RF. 2017. № 31 (ch. 1). St. 4736.
5. Vantseva I.O., Zyryanova T.YU., Medvedeva O.O. Vliyaniye federal'nogo zakona «O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii» na vladel'tsev kriticheskikh informatsionnykh infrastruktur // Vestnik UrFO. 2018. № 1(27). S. 71–76.
6. Pravila kategorirovaniya ob"yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii, utv. postanovleniyem Pravitel'stva RF ot 8 fevralya 2018 g. № 127 // Sobraniye zakonodatel'stva RF. 2018. № 8. St. 1204.
7. Prikaz FSTEK RF ot 6 dekabrya 2017 g. № 227 «Ob utverzhdenii poryadka vedeniya reyestra znachimykh ob"yektov kriticheskoy informatsionnoy infrastruktury Rossiy-skoy Federatsii» // Ofitsial'nyy internet-portal pravovoy informatsii. URL: http://www.pravo.gov.ru (data obrashcheniya: 09.02.2018).
8. Prikaz FSTEK RF ot 22 dekabrya 2017 g. № 236 «Ob utverzhdenii formy napravleniya svedeniy o rezul'tatakh prisvoyeniya ob"yektu kriticheskoy informatsionnoy in-frastruktury odnoy iz kategoriy znachimosti libo ob otsutstvii neobkhodimosti prisvoyeniya yemu odnoy iz takikh kategoriy» //

Ofitsial'nyy internet-portal pravo-voy informatsii. URL: http://www.pravo.gov.ru (data obrashcheniya: 16.04.2018).

9. Prikaz FSTEK RF ot 21 dekabrya 2017 g. № 235 «Ob utverzhdenii trebovaniy k sozdaniyu sistem bezopasnosti znachimykh ob"yektov kriticheskoy informatsionnoy in-frastruktury Rossiyskoy Federatsii i obespecheniyu ikh funktsionirovaniya» // Ofitsial'nyy internet-portal pravovoy informatsii. URL: http://www.pravo.gov.ru (data obrashcheniya: 22.02.2018).
10. Prikaz FSTEK RF ot 25 dekabrya 2017 g. № 239 «Ob utverzhdenii trebovaniy po obespecheniyu bezopasnosti znachimykh ob"yektov kriticheskoy informatsionnoy in-frastruktury Rossiyskoy Federatsii» // Ofitsial'nyy internet-portal pravovoy informatsii. URL: http://www.pravo.gov.ru (data obrashcheniya: 27.03.2018).
11. Mery zashchity informatsii v gosudarstvennykh informatsionnykh sistemakh: metodiche-skiy dokument, utv. FSTEK RF 11 fevralya 2014 g. // Ofitsial'nyy sayt FSTEK Rossii. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (data obra-shcheniya: 21.10.2019).
12. Pravila osushchestvleniya gosudarstvennogo kontrolya v oblasti obespecheniya bezopas-nosti znachimykh ob"yektov kriticheskoy informatsionnoy infrastruktury Rossiy-skoy Federatsii, utv. postanovleniyem Pravitel'stva RF ot 17 fevralya 2018 g. № 162 // Sobraniye zakonodatel'stva RF. 2018. № 9. St. 1393.
13. Kodeks RF ob administrativnykh pravonarusheniyakh ot 30 dekabrya 2001 g. № 195-FZ (chast' 2 stat'i 19.5) // Sobraniye zakonodatel'stva RF. 2002. № 1 (ch. 1). St. 1.
14. Ukaz Prezidenta RF ot 22 dekabrya 2017 g. № 620 «O sovershenstvovanii Gosudar-stvennoy sistemy obnaruzheniya, preduprezhdeniya i likvidatsii posledstviy komp'-yuternykh atak na informatsionnyye resursy Rossiyskoy Federatsii» // Sobraniye za-konodatel'stva RF. 2017. № 52 (ch. 1). St. 8112.
15. Polozheniye o Natsional'nom koordinatsionnom tsentre po komp'yuternym intsiden-tam, utv. prikazom FSB Rossii ot 24 iyulya 2018 g. № 366 // Ofitsial'nyy internet-portal pravovoy informatsii. URL: http://www.pravo.gov.ru (data obrashcheniya: 10.09.2018).
16. Sostoyaniye prestupnosti v Rossiyskoy Federatsii // Ofitsial'nyy sayt MVD Ros-sii. URL: https://mvd.rf/reports/item/18556721 (data obrashcheniya: 14.10.2019).
17. Ugolovnyy kodeks Rossiyskoy Federatsii ot 13 iyunya 1996 g. № 63-FZ (stat'ya 274.1) // Sobraniye zakonodatel'stva RF. 1996. № 25. St. 2954.
18. Pykhtin I.G. Ugolovno-pravovaya okhrana ob"yektov kriticheskoy informatsionnoy in-frastruktury kak odno iz klyuchevykh napravleniy sovremennoy bor'by s kiberpre-stupnost'yu v Rossiyskoy Federatsii // Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo. 2018. T. 8. № 1(26). S. 98–103.
19. Shul'ga A.V., Galiakbarov R.R. Ugolovnaya otvetstvennost' za nepravomernoye vozdey-stviye na kriticheskuyu informatsionnuyu infrastrukturu Rossiyskoy Federatsii (st. 274.1. UK RF) // Gumanitarnyye, sotsial'no-ekonomicheskiye i obshchestvennyye nauki. 2018. № 5. S. 238–242.