DOI 10.37882/2223-2966.2024.03.09

ОБ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ МЕТОДАМИ УГОЛОВНОГО ПРАВА[1]

ON ENSURING THE SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE BY METHODS OF CRIMINAL LAW

V. Elin
A. Tsaregorodtsev

Summary. The article reveals the features of ensuring the security of the critical information infrastructure of the Russian Federation and the need to improve the current Russian criminal legislation in this area, taking into account the requirements of the law in the interests of implementing public-private partnerships and ensuring interaction between the subject of the critical information infrastructure, the State system for detecting, preventing and eliminating the consequences of computer attacks (GosSOPKA) and the National Coordination Center for Computer Incidents (NKTsKI).

Keywords: information security, incident, critical infrastructure security, public-private partnership.

Елин Владимир Михайлович
Кандидат педагогических наук, доцент, Финансовый университет при Правительстве Российской Федерации, Москва;
Доцент, Московский университет МВД России имени В.Я. Кикотя, Москва
elin_vm@mail.ru
Царегородцев Анатолий Валерьевич
Доктор технических наук, профессор, главный научный сотрудник, Финансовый университет при Правительстве Российской Федерации, Москва
academic_tsar@mail.ru

Аннотация. В статье раскрываются особенности обеспечения безопасности критической информационной инфраструктуры Российской Федерации и необходимость совершенствования действующего российского уголовного законодательства в данной сфере с учетом требований законодательства в интересах осуществления государственно-частного партнерства и обеспечении взаимодействия между субъектом критической информационной инфраструктуры, Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и Национальным координационным центром по компьютерным инцидентам (НКЦКИ).

Ключевые слова: информационная безопасность, инцидент, безопасность критической инфраструктуры, государственно-частное партнерство.

Введение

С момента вступления в силу Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»[1] встал вопрос о возможности практического обеспечения комплекса организационных и технических мер, направленных на практическое воплощение нормативных требований [1,2]. Ряд аспектов государственно-частного партнерства в сфере обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на киберинциденты со стороны государства раскрывается особенностями функционирования ГосСОПКИ[2] в качестве SIEM-системы и Национального координационного центра по компьютерным инцидента (далее: НКЦКИ) в качестве SOC-центра. Другим участником данного правоотношения выступают субъекты критической информационной инфраструктуры, к признакам которых относятся как владение информационными системами и сетями, так и принадлежность к установленным Законом сферам (например: здравоохранение, топливно-энергетический комплекс, связь), в отношении которых субъектам критической информационной инфраструктуры следует осуществить комплекс мероприятий (например: категорирование, информирование, содействие и др).

[1] Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ// СЗ РФ , 31.07.2017, № 31 (Часть I), ст. 4736

[2] Указ Президента РФ от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // СПС Консультатнт плюс

[1] Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финуниверситета.

Вышеизложенный закон затрагивает госорганы и госучреждения, юридические лица и индивидуальных предпринимателей, которым на праве собственности или аренды принадлежат объекты критической информационной инфраструктуры. В случае нарушения законодательства начинает работать правовая норма, предусмотренная ст. 274.1 УК РФ и предусматривающая уголовную ответственность за неправомерное воздействие на критическую информационную инфраструктуру (Далее: «КИИ») Российской Федерации[3].

Общая характеристика запретительных требований

По своей сути содержание ст. 274-1 УК РФ представляет собой переработанные диспозиции ст. 272-274 УК РФ, предполагая в качестве материальных последствий преступления наступление вредоносного воздействия и причинения вреда критической информационной инфраструктуре Российской Федерации.

Применяемые инструменты уголовного правового реагирования определяют, что уголовная ответственность наступает за деяния, связанные за противоправные действия в отношении объектов КИИ Российской Федерации. При этом следует иметь в виду, что уголовно-правовой охране подлежат не только информационные системы и автоматизированные системы управления технологическими процессами, но также информационно-телекоммуникационные сети и сети электросвязи.

Уголовная ответственность наступает вследствие неправомерного доступа к содержащейся в КИИ Российской Федерации охраняемой компьютерной информации; либо причинения вреда КИИ Российской Федерации путем создания, распространения или использования заведомо вредоносных компьютерных программ. В части защиты информационных систем уголовная ответственность наступает вследствие нарушения правил, касающихся доступа и эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, либо КИИ Российской Федерации в целом. В результате применения указанного подхода ряд авторов выдвигает требования о необходимости учета характеристик информации при установлении отраслевой, структурной либо политической значимости [4].

Квалифицирующими признаками выступает совершение преступлений группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения, либо наступление в результате совершения преступления особо тяжких последствий.

Подход законодателя к построению указанной правовой нормы представляется не совсем оправданным поскольку вступает в противоречие с требованиями Закона «О безопасности критической информационной инфраструктуры Российской Федерации» (далее: Закон «О безопасности КИИ»), направленного на обеспечение правового регулирование общественных отношений в области обеспечения безопасности КИИ. Безопасность КИИ Российской Федерации, по мнению законодателя, должна находиться в состоянии защищенности, что предполагает устойчивое функционирование КИИ Российской Федерации при проведении в отношении ее компьютерных атак.

Компьютерная атака как ключевой элемент воздействия на критическую информационную инфраструктуру

Обращает на себя внимание то обстоятельство, что в диспозиции уголовно-правовой нормы отсутствуют такие ключевые понятия как: «компьютерная атака» в качестве результата инцидента.

Между тем, понятие «компьютерной атаки» предполагает, с одной стороны, использование программного или программно-аппаратного инструментария при целенаправленном воздействии на КИИ РФ, с другой стороны, целью представленного воздействия наступает как нарушение или прекращение функционирования КИИ, так и возникновение угрозы безопасности информации, обработка которой производится на объектах КИИ Российской Федерации. При этом факт наступления указанных материальных последствий, в том числе произошедший в результате компьютерной атаки, законодатель определяет в качестве «компьютерного инцидента».

Таким образом, Закон «О безопасности КИИ» в качестве объекта вредоносного воздействия рассматривает объекты КИИ Российской Федерации и используемые для организации взаимодействия объектов КИИ сети электросвязи[4]. При этом информационные системы, информационно-телекоммуникационные сети, а также автоматизированные системы управления субъектов КИИ, представляют собой объекты КИИ Российской Федерации.

[3] Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 194-ФЗ (последняя редакция)// СПС «Консультант плюс»

[4] Постановление Правительства РФ от 08.06.2019 № 743 «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры»//СПС Консультант плюс

Раскрывая понятие субъектов КИИ законодатель выделяет 2 категории субъектов, первая из которых должна отвечать ряду признаков:

- организационно-правовая форма: государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели;
- имущественные отношения: право собственности, аренды или наличие иного законного основания принадлежности объектов КИИ Российской Федерации;
- сфера народного хозяйства, в котором осуществляют свою деятельность субъекты КИИ: здравоохранение, наука, транспорт, связь, энергетика, банковская сфера и иные сферы финансового рынка, топливно-энергетический комплекс, атомная энергетика, оборонная, ракетно-космическая, горнодобывающая, металлургическая и химическая промышленности.

Вторая категория субъектов включает российских юридических лиц или индивидуальных предпринимателей, обеспечивающих взаимодействие объектов КИИ Российской Федерации.

Как следует из раскрываемых определений, Закон «О безопасности КИИ» содержит исчерпывающий перечень противоправных деяний, определяемых в качестве компьютерных атак, и возможных наступлений материальных последствий, определяемых в качестве компьютерных инцидентов. Представляется, что нормы уголовного законодательства, представленные в ч.1 и ч.2 ст. 274.1 УК РФ, достаточно слабо коррелируют с положениями Закона «О безопасности КИИ» и направлены в первую очередь на обеспечение безопасности информации, но не на обеспечение безопасности объектов КИИ.

В том, что касается возможности наступления сформулированной в ч.3 ст. 274.1 УК РФ уголовной ответственности за нарушение комплекса организационных мероприятий и норм технического регулирования, следует учитывать следующие обстоятельства: сформулированные в Законе «О безопасности КИИ» принципы обеспечения безопасности критической информационной инфраструктуры включают законность, приоритет предотвращения компьютерных атак, а также непрерывность и комплексность обеспечения безопасности КИИ, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти (далее: ФОИВ) и субъектов КИИ.

Особенности государственно-частного партнерства при обеспечении безопасности критической информационной инфраструктуры РФ

В основе взаимодействия ФОИВ положены основные направления государственной политики в области обеспечения безопасности КИИ, установленные полномочиями Президента Российской Федерации в указанной сфере правового регулирования.

Правительство Российской Федерации устанавливает правила, связанные с процессом категорирования объектов КИИ и осуществления государственного контроля в области безопасности значимых объектов КИИ; подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов КИИ. Правительство Российской Федерации также устанавливает показатели критериев значимости объектов КИИ и их значения, порядок и сроки их категорирования[5].

Взаимодействие ФОИВ связано, прежде всего, с деятельностью двух категорий уполномоченных: в области обеспечения безопасности КИИ Российской Федерации (осуществляет ФСТЭК РФ) и в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (осуществляет ФСБ РФ).

Таким образом, в настоящее время практическая деятельность по обеспечению безопасности критической информационной инфраструктуры осуществляется совместно Федеральной службой безопасности (ФСБ РФ), Федеральной службой по техническому и экспертному контролю (ФСТЭК РФ) и Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Именно указанные ФОИВ осуществляют комплекс организационно-техническим и правовых мер, направленных на обеспечение безопасности КИИ РФ.

Инструментом взаимодействия уполномоченных ФОИВ и субъектов КИИ выступает Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее: ГосСОПКА) и национальный координационный центр по компьютерным инцидентам (далее: НКЦКИ). Следует также отметить, что наряду с осуществлением взаимодействия в рамках государственно-частного партнерства, ФОИВ осуществляют значительный объем дополнительных функций, связанных с установлением требований, порядков, перечней, осуществлением контроля и т.д.

ГосСОПКА, находящаяся в подчинении ФСБ России в рамках осуществления государственно-частного пар-

[5] Постановление Правительства РФ от 08.02.2018 № 127 (ред. от 20.12.2022) «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»

тнерства, выступает в качестве структуры SIEM в сфере обеспечения безопасности КИИ.

Деятельность в сфере SIEM (Security Information and Event Management) связана с необходимостью осуществления двух категорий операций: управления информационной безопасностью (Security Information Management (SIM) и управление событиями безопасности (Security Event Management (SEM). По мнению авторов концепции, деятельность SIEM-систем включает инструменты управления идентификацией и доступом, уязвимостями и базами данных и приложений. Функционирование системы направлено на сбор, анализ и представление информации из сетевых устройств и устройств безопасности [5].

Национальный координационный центр по компьютерным инцидентам (НКЦКИ)[6], который координирует деятельность субъектов КИИ и чья техническая инфраструктура используется для функционирования системы НКЦКИ представляет собой Центр SOC (Security Operation Center) в государственном масштабе.

SOC (Security Operations Center), что в буквальном переводе с английского означает «Центр операций по безопасности», в русскоязычной литературе часто переводится как Ситуационный центр информационной безопасности, либо Центр мониторинга кибербезопасности, либо Центр обеспечения компьютерной безопасности. В англоязычной литературе также встречается термин CSOC — CyberSecurity Operations Center. Отечественные специалисты по информационной безопасности также используют в качестве акронима «СОК». В любом случае, SOC представляет собой структурное подразделение, осуществляющее мониторинг работы систем защиты информации и реагирующее на инциденты информационной безопасности, включающее группу специалистов по защите информации, которые непрерывно осуществляют контроль за сообщениями, поступающими от технических средств, для того чтобы как можно оперативнее устранить угрозу информационной безопасности.

Основная задача SOC-Центра — это обеспечение реагирования на инциденты информационной безопасности в рамках соглашения о качестве оказываемых услуг SLA (Service Level Agreement). Предварительно также обговариваются задаваемые критерии, ключевые показатели эффективности KPI (Key Performance Indicators) для команд реагирования SOC-Центров и определенные типы шагов по реагированию на кибератаки, их сдерживанию, локализации и нейтрализации угроз информационной безопасности, которые будут предприниматься командой SOC в рамках обработки инцидентов.

Субъектов ГосСОПКА можно разделить на несколько видов, у каждого из которых свои основания участия в ГосСОПКА, участие органов власти представляется обязательным на основании распоряжения Правительства. Государственные корпорации создают центры ГосСОПКА по решению своего основного акционера — государства. Прочие организации, относящиеся к критической информационной инфраструктуре, имеют право с согласия ФСБ России создавать центры ГосСОПКА и становиться участниками системы. Это решение принимается добровольно: централизация мер защиты целесообразна экономически и позволяет использовать ограниченное количество специалистов для обеспечения защиты большого количества информационных систем. Юридические лица и индивидуальные предприниматели, имеющие лицензии ФСТЭК России и ФСБ России, также имеют право создавать центры ГосСОПКА, подключаться к ГосСОПКА и оказывать услуги по противодействию компьютерным атакам в рамках этой системы. Указанный подход позволяет распространить деятельность ГосСОПКА на субъекты КИИ, неспособные самостоятельно обеспечить противодействие компьютерным атакам в объеме, предусмотренном нормативными документами ФСБ РФ.

Центры ГосСОПКА могут быть как ведомственными, так и корпоративными: ведомственные защищают информацию органов государственной власти, а корпоративные — расследуют инциденты в своих системах и могут предоставлять такие услуги на коммерческой основе. Центры ГосСОПКА — это, упрощенно говоря, еще один пример государственного Центра SOC, по аналогии с НКЦКИ. Сразу отметим, что создание своего корпоративного Центра ГосСОПКА потребует не только закупки средств защиты (например, систем SIEM и IRP) и найма специалистов-аналитиков ИБ, но и получения лицензии ФСТЭК России на осуществление деятельности по мониторингу информационной безопасности, а также налаживания взаимодействия с НКЦКИ для обмена информацией об инцидентах КИИ.

Определение угроз безопасности в объектах КИИ можно осуществлять в соответствии с методическим документом ФСТЭК России в рамках деятельности по выполнению работ и разработки моделей угроз безопасности[7].

Заключение

Таким образом, в настоящее время возникает потребность более тщательного подхода к формирова-

[6] Приказ ФСБ России от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам» (вместе с «Положением о Национальном координационном центре по компьютерным инцидентам») (Зарегистрировано в Минюсте России 06.09.2018 N 52109) // СПС Консультатнт плюс

[7] Методический документ "Методика оценки угроз безопасности информации". Утвержден ФСТЭК России 5 февраля 2021 г. // СПС Консультатнт плюс

нию системы уголовного-правового инструментария, направленного на обеспечение безопасности КИИ Российской Федерации, прежде всего, на противодействие компьютерным атакам или компьютерным инцидентам. В основу подхода следует положить необходимость предупреждения и наказания за совершение компьютерных атак на объекты КИИ с учетом разработок ФОИВ осуществляющих деятельность в данной сфере.

ЛИТЕРАТУРА

1. Лобач Д.В., Смирнова Е.А. Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам // Территория новых возможностей. Вестник ВГУЭС. 2019. № 4. С. 24–32.
2. Баянова Ю.А. Критическая информационная инфраструктура как объект обеспечения бе зопасности // Инновационная наука. 2021. № 10-2. С. 62–65.
3. Горелик В.Ю., Безус М.Ю. О безопасности критической информационной инфраструктуры Российской Федерации// «StudNet»: 2020. № 9. С 1435–1448.
4. Дремлюга Р.И., Зотов С.С., Павлинская В.Ю. Критическая информационная инфраструктура как предмет преступного посягательства // Азиатско-тихоокеанский регион: экономика, политика, право. 2019. № 2. С. 130–139.
5. Построение центра ГосСОПКА. Комплексное решение для создания центра ГосСОПКА и взаимодействия с НКЦКИ. // https://www.ptsecurity.com/ru-ru/solutions/center-gossopka/
6. Ахметов, Р., SOC (Security Operation Center): что это такое и зачем используется? Центры мониторинга информационной безопасности// https://www.securityvision.ru/blog/soc-chto-eto/

Журнал «Современная наука: актуальные проблемы теории и практики»