Правоведение

УДК 34.07:004.056(045)

В.Л. Акапьев, С.Е. Савотченко

ПУБЛИЧНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Переход общественной формации в категорию информационного общества, внедрение информационных технологий и информационных систем различного назначения во все сферы человеческой деятельности беспрецедентно умножают значимость общенациональной системы информационной безопасности, усиливает необходимость защиты не только используемой информации, но и объектов критической информационной инфраструктуры (КИИ) как ключевых элементов обеспечения жизнедеятельности государства. Указанное положение актуализирует необходимость исследования публично-правового регулирования данного аспекта информационной безопасности с целью разрешения ряда противоречий между интересами субъектов информационного пространства в области информационной безопасности, объединить положения нормативных правовых актов, регламентирующих требования по обеспечению безопасности объектов критической информационной инфраструктуры с правоприменительной практикой в сложившихся условиях, в значительной степени определяемых пандемией Covid 19 и перманентной войной, объявленной Западом против Российской Федерации. С момента вступления в силу закона «О безопасности критической информационной инфраструктуры Российской Федерации» минуло почти шесть лет, но до сих пор большинство субъектов КИИ по тем или иным причинам не выполнили сформулированные в нем требования, что придает решению обозначенной задачи не только теоретико-методологическое, но и практическое значение.

Ключевые слова: информационная безопасность, компьютерный инцидент, критическая информационная инфраструктура, объекты критической информационной инфраструктуры, регулятор.

DOI: 10.35634/2412-9593-2024-34-3-494-503

Кибербезопасность относится к числу направлений деятельности, развивающихся чрезвычайно быстрыми темпами. Этому способствуют как общий прогресс развития информационных технологий, так и постоянное противоборство различных сторон в процессе сохранности и приобретения информации. Поэтому проблемы, связанные с кибербезопасностью, с каждым годом становятся все более насущными и сложными.

Возможен конфликт интересов и создание противоречий, которыми сопровождается весь жизненный цикл информационной безопасности, которую многие руководители рассматривают как груз, который всем мешает как лишний функционал. У государства задача – обеспечить безопасность объектов критической информационной инфраструктуры (далее – КИИ), а у органов власти на местах задача противоположная – как можно меньше работать. И, в случае выделения объекта КИИ, у них в дальнейшем возникает ряд проблем, которых они стремятся избежать. То есть информационной безопасностью, в соответствии с действующим законодательство, заниматься нужно, но не совсем понятно, зачем, так как значительная часть руководителей не видит от этого никакого эффекта [1].

Данный диссонанс усиливается на фоне отсутствия кадрового ресурса по той простой причине, что для обеспечения информационной безопасности необходимо выделять отдельные штатные единицы специалистов, обладающих соответствующей квалификацией.

Частично, это связано с российским менталитетом по принципу: пока что-то не случиться, ничего делать не надо. На практике же действия по ИБ необходимо рассматривать как превентивные меры, позволяющие избежать негативных воздействий на тот или иной орган госвласти, которые могут привести к еще большим нежелательным последствиям.

Помимо всего прочего, на передний план борьбы за обеспечение информационной безопасности выходят следующие мотивирующие основания:

– обостряющиеся противоречия между все возрастающими потребностями общества в свободном обмене информацией и ограничениями (чрезмерным или, наоборот, недостаточным) на её распространение и использование;

– повсеместное и динамично развивающееся использование компьютерной техники, информационных технологий и средств коммуникации;

– использование информационных систем (ИС) в критических областях деятельности (в том числе в государственных органах Российской Федерации);

– консолидация в рамках единого информационного пространства все большего числа граждан и организаций;

– концентрация огромных объёмов жизненно важной информации различного назначения и принадлежности на электронных носителях;

– превалирование доли информационных услуг в формировании валового национального продукта ведущих стран мира, создание и развитие цифровой экономики, цифровой энергетики и др.;

– рост числа квалифицированных пользователей современных информационных технологий, обладающих достаточно сформированной информационно-технологической компетентностью, позволяющей им создавать нежелательные воздействия на системы обработки информации;

Этому способствуют расширение сферы применения компьютерной техники и возросший уровень доверия к системам управления и обработки информации. Здоровье, благополучие, а зачастую и само существование человечества во многом зависит от качества ответственной работы, которая доверена компьютерным информационным системам [2].

При этом информационные ресурсы государственных органов становятся важнейшим источником информации, в том числе инсайдерской, как для коммерческих организаций, так и для иностранных разведок или преступных групп.

Несмотря на существенные изменения законодательства в последние годы в сфере информационной безопасности и защиты информации от противоправных действий, проблемы не ликвидированы полностью. Существуют противоправные действия, по которым отсутствует понятийная база, что позволяет преступникам уходить от уголовного преследования. Используются методы социальной инженерии, которые выводят преступника из-под преследования, создавая ситуации якобы добровольной передачи денег, материальных ценностей или информации. Возрастает количество противоправных действий, совершаемых преступными группами по заранее составленному плану и соответствующему алгоритму. Это – деятельность мошенников по получению доступа к банковским картам населения, принявшая в последние годы массовый характер. Шифрование информационных ресурсов, взлом сайтов и серверов с последующим вымогательством денежных средств.

Также в составе преступных групп осуществляются попытки доступа к информационным ресурсам государственных органов, промышленный шпионаж [3, с. 13]. Существенная часть противоправных действий осуществляется под кураторством или непосредственным руководством иностранных разведок. В ряде таких иностранных государств, как США, Великобритания, Украина созданы специализированные подразделения для проведения противоправных действий в информационном пространстве других стран и, в первую очередь, России [4, с. 23].

В последнее время особое внимание уделяется объектам критической информационной инфраструктуры, к которым относят такие ИС, сбой или отказ в работе которых кардинально отразится на безопасности отдельных граждан, индивидуальных предпринимателей, юридических лиц, занимающихся коммерческой и производственной деятельностью, государственных органов управления различных уровней, общества и государства в целом[1].

Закон об обеспечении критической информационной инфраструктуры (КИИ)[2], принятый сравнительно недавно, определяет объекты и субъекты КИИ, он устанавливает, что должна обеспечиваться безопасность и каким образом она будет обеспечиваться. Во исполнение данного федерального закона приняты необходимые подзаконные акты. Основным документом, где описаны правила категорирования объектов КИИ, является постановление Правительства № 127, в соответствии с которым каждому объекту комиссионно присваивается категория значимости[3].

---

[1] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Российская газета. № 167. 31.07.2017.

[2] Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ (последняя редакция) // СПС «КонсультантПлюс».

[3] Постановление Правительства РФ от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»; Постановление Правительства РФ от 08.02.2018 № 127 (ред. от 20.12.2022) «Об утверждении Правил категорирования объектов критической информационной инфраструкту-

Более низкий уровень представляют руководящие документы регулятора, в данном случае, приказы Федеральной службы по техническому и экспортному контролю (ФСТЭК России). Основными документами организационного уровня являются приказы ФСТЭК № 227 от 6 декабря 2017 года о введении реестра значимых объектов и № 229 от 11 декабря 2017 года о подтверждении форм акта проверки по итогам проведения госконтроля[4].Непосредственно более приближенными по своему содержанию к субъектам КИИ являются приказы ФСТЭК России №№ 235[5], 236[6] и 239[7].

В соответствии с указанными документами ФСТЭК утвердил шаблон, по которому субъекты КИИ должны ему направлять сведения о категорировании объектов КИИ. В части обеспечения безопасности объектов КИИ регламентируются Требования к созданию систем безопасности значимых объектов КИИ [5, с. 9].

В составе объектов КИИ выделяют значимые объекты критической информационной инфраструктуры (ОКИИ), которым присвоена одна из категорий значимости и которые включены в соответствующий реестр значимых объектов критической информационной инфраструктуры.

Защита значимых объектов критической информационной инфраструктуры находится под контролем уполномоченных государственных спецслужб (регуляторов). Основная цель законодательства заключается в выявлении критических для государства объектов и обеспечении их безопасности, для чего необходимо:

– категорирование объектов КИИ;

– создание системы обеспечения безопасности объектов КИИ;

– взаимодействие с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА).

Категорирование объектов КИИ осуществляется не зависимо от того, являются ли они значимыми или нет, и данные работы производятся всеми субъектами КИИ. Здесь можно выделить сбор исходных данных, категорирование объектов КИИ, подготовку и отправку сведений о результатах категорирования объектов КИИ в ФСТЭК России.

В состав исходных данных входят:

– перечень процессов;

– перечень объектов КИИ;

– информация по объектам КИИ;

– состав информации, обрабатываемой на объектах КИИ;

– информация по угрозам безопасности;

– информация по компьютерным инцидентам.

Алгоритм сбора данных для категорирования ОКИИ реализуется следующим образом: сначала определяется перечь процессов (управленческих, технологических, производственных). Далее из этих процессов необходимо выделить критические процессы, которые могут нанести какой-либо ущерб субъекту КИИ, и имеющиеся информационные системы и ИТКС, которые поддерживают критиче-

---

ры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» (с изм. и доп., вступ. в силу с 21.03.2023) // СПС «КонсультантПлюс».

[4] Приказ ФСТЭК России от 06.12.2017 № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»; Приказ Федеральной службы по техническому и экспортному контролю от 11.12.2017 № 229 «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»; Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 20.02.2020) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // СПС «КонсультантПлюс».

[5] Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» // СПС «КонсультантПлюс».

[6] Приказ от 22 декабря 2017 г. № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» // СПС «КонсультантПлюс».

[7] Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 20.02.2020) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // СПС «КонсультантПлюс».

ские процессы. На основании этого формируется перечень объектов КИИ, который комиссионно утверждается и отправляется в ФСТЭК России письмом по форме.

Важно отметить, что продолжительное время велся спор, а нужно ли на этапе сбора исходных данных производить полноценное моделирование угроз безопасности в отношении объектов КИИ? По итогам долгих дискуссий и устоявшейся практики, специалисты пришли к выводу, что на данном этапе детальное моделирование угроз производить нецелесообразно, так как оно проводится для значимого объекта на последующих этапах, если требуется давать заключение о создании системы обеспечения безопасности [6, с. 114].

Категорирование проводит субъект КИИ, для чего приказом создается специальная комиссия, члены которой отвечают, указанным в постановлении Правительства № 127, критериям: представители руководства, специалисты по кибербезопасности, эксплуатационники. В состав комиссии рекомендуется включать лиц, занимающихся гостайной, если она имеет отношение к рассматриваемым информационным процессам, персонал, занимающийся гражданской обороной и мобилизационной подготовкой.

Разрабатывает Положение о комиссии и Проекты «Актов категорирования объектов КИИ». Основное назначение комиссии заключается на основании собранных данных и их анализа произвести категорирование. Акт категорирования может быть как для каждого объекта в отдельности, так и один акт для всех объектов на усмотрение субъекта КИИ. На практике чаще всего на каждый объект разрабатывается свой акт.

Правила категорирования объектов КИИ РФ, а также перечень показателей критериев значимости и их значений утвержден Постановлением Правительства РФ от 08.02.2018 № 127[8].Основные показатели значимости (пять групп) ущерба от угроз КБ КИИ:

– смерть или ухудшение здоровья граждан;
– сбои и отказы объектов обеспечения жизнедеятельности;
– нарушение функционирования транспортной инфраструктуры;
– нарушение функционирования сети связи;
– невыполнение органом возложенной на него функции;
– отказ в доступе к государственной услуге;
– нарушение международных обязательств, срыв переговоров;
– недополучение средств в бюджет;
– уменьшение дохода предприятия, организации;
– вредные воздействия на окружающую среду;
– нарушение работы мониторинговых и ситуационных центров;
– невыполнение гособоронзаказа и т. п.

Далее, по результатам категорирования, определяются с тем, есть ли значимые объекты или нет. В случае, когда все выделенные объекты являются незначимыми, то есть им не присвоена ни одна из категорий значимости, дальнейшие работы можно не выполнять. Мероприятия в части обеспечения безопасности КИИ прекращаются, но по желанию субъекта КИИ они могут быть выполнены.

В случае выявления значимых объектов КИИ у субъектов возникает обязанность создать систему обеспечения их безопасности и здесь вступают в силу приказы ФСТЭК, в соответствии с которыми необходимо ряд стандартных шагов:

– разработать модели угроз безопасности информации и модели нарушителя;
– разработать техническое задание на создание системы обеспечения безопасности объектов КИИ;
– разработать организационно-распорядительную документацию;
– спроектировать и внедрить системы обеспечения безопасности значимого объекта КИИ.

Система безопасности значимого объекта критической информационной инфраструктуры (ЗОКИИ) включает в свой состав силы обеспечения безопасности ЗОКИИ (подразделения и отдельные работники),программные и программно-аппаратные средства обеспечения ЗОКИИ[9].

---

[8] Постановление Правительства РФ от 08.02.2018 № 127 «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» // Собрание законодательства РФ. 19.02.2018. № 8. Ст. 1204.

[9] Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» // СПС «КонсультантПлюс».

К указанным компонентам ЗОКИИ устанавливаются четыре группы требований:

– Требования к силам обеспечения безопасности ЗОКИИ;

– Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности ЗОКИИ;

– Требования к организационно-распорядительным документам по безопасности ЗОКИИ;

– Требования к функционированию системы безопасности в части организации работ по обеспечению безопасности ЗОКИИ.

В первой группе расписываются требования по персоналу с указанием функциональных обязанностей, требования к службе безопасности и ее руководству вплоть до наличия обязательного профильного образования или высшего образования, но при прохождении профильной профессиональной переподготовки в объеме не менее 512 часов и наличии определенного опыта работы. Сюда же включаются требования об обязательном повышении квалификации персонала. Данные требования обосновывают необходимость наличия отдела безопасности, укомплектованного грамотными специалистами, которые должны периодически обучаться.

Во второй группе устанавливаются требования к средствам защиты информации, которые могут быть сертифицированными, либо прошедшими приемку или испытания. Сертификация в КИИ не является обязательным компонентом, если нет дополнительных требований.

В третьей группе фиксируются в явном виде условия наличия комплекта документации, расписывающей направления деятельности по безопасности: политики, положения и т. д.

Четвертая группа требований направлена на организацию в рамках обеспечения безопасности ЗОКИИ стандартного цикла обязательных работ. Должны проводиться работы по планированию, по реализации контроля и его совершенствованию. Указанные виды работ должны носить циклический характер на постоянной основе, а не выполняться в виде одноразовой акции.

Этапность выполнения работ[10] включает в себя:

– моделирование угроз безопасности;

– установление требований к обеспечению безопасности ЗОКИИ;

– проектирование системы обеспечения безопасности ЗОКИИ;

– внедрение системы обеспечения безопасности ЗОКИИ.

Идеология построения системы безопасности ЗОКИИ базируется на разделении жизненного цикла на отдельные подэтапы: формирование требований, создание системы обеспечения безопасности, внедрение этой системы, ее эксплуатация и вывод из эксплуатации. На сегодняшний день большинство субъектов КИИ прошли этап категорирования, часть субъектов КИИ приступают к созданию системы обеспечения безопасности и считанные единицы занимаются полноценным внедрением средств защиты информации [7, с. 56].

Моделирование угроз безопасности усилиями ФСТЭК в значительной степени унифицировано и при реализации различных направлений обеспечения ИБ (персональные данные, государственные информационные системы, КИИ и др.) используется единообразный подход[11], в рамках которого разработан банк данных угроз безопасности информации[12]. По направлениям работы ФСБ России также принят ряд документов в части модели нарушителя, если используются не сертифицированные средства криптографической защиты информации (СКЗИ)[13].

---

[10]Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 20.02.2020) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // СПС «КонсультантПлюс».

[11] Методический документ «Методика оценки угроз безопасности информации (утвержден ФСТЭК России 5 февраля 2021 г.) // СПС «КонсультантПлюс».

[12] Информационное сообщение ФСТЭК России от 6 марта 2015 г. № 240/22/879 «О банке данных угроз безопасности информации» (https://bdu.fstec.ru).

[13] Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»; «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» (утв. ФСБ России 31.03.2015 № 149/7/2/6-432) // СПС «КонсультантПлюс».

Но с учетом новой методики оценки угроз банк данных угроз практически не используется, так как существующие угрозы под данную методичку не подходят [8, с. 54]. По этой причине ФСТЭК России банк данных перерабатывает и уже опубликован пилотный вариант нового банка данных угроз.

В настоящее время государство, исходя из анализа действующих нормативных правовых актов, стало подходить к решению проблемы информационной безопасности КИИ с точки зрения резко ориентированного подхода, при котором необходимо отталкиваться от непосредственных угроз и негативных последствий, которые они могут повлечь. На первом шаге определяются негативные последствия, затем определяется объект воздействия, на котором в результате воздействия могут возникать негативные последствия, далее определяются источники угроз, способы реализации угроз нарушителем и на завершающем этапе производится оценка актуальности угроз [9, с. 1440].

В действующей методике заложена двухфазная система, когда в начале определяется возможная угроза, но не актуальность. Угроза признается возможной в случае, если для нее определены четыре критерия: есть нарушитель (источник угрозы), который может реализовать некоторую угрозу в отношении конкретного объекта воздействия, имеется конкретный способ реализации угроз, который приведет к негативным последствиям. Как пример, утечка защищаемой информации:

Угроза безопасности информации	**Нарушитель (источник угрозы)**	**Объекты воздействия**	**Способы реализации угроз**	**Негативные последствия**
Угроза утечки защищаемой информации	Авторизованные пользователи систем и сетей	Сетевое оборудование. Серверы. Конфигурационные файлы сетевого оборудования. Конфигурационные файлы операционной системы.	Использование уязвимостей архитектуры и конфигурации ИС, а также организационных и многофакторных уязвимостей	Утечка информации ограниченного доступа

Авторизованный пользователь системы, используя уязвимости архитектуры и конфигурации, в отношении сетевого оборудования может совершить какие-то мероприятия, которые приведут к утечке информации ограниченного доступа, то такая угроза признается вероятной. То есть наличие всех этих факторов является основанием признания угрозы вероятной.

Но это еще не актуальная угроза. Чтобы угроза превратилась в актуальную, необходимо рассмотреть сценарий реализации этих угроз. Если для угрозы безопасности существует сценарий ее реализации (тактика, техника), то угроза признается актуальной. Существует несколько способов описания сценариев, из которых субъект ИБ может выбирать оптимальный для себя [10].

Методика выделения сначала возможных угроз, а затем определение актуальных угроз имеет некоторую странность: при наличии всех четырех факторов, определяющих возможную угрозу, всегда можно описать сценарий ее реализации. То есть, фактически, любая вероятная угроза может считаться актуальной.

Третий блок работ – это взаимодействие с ГосСОПКА[14], в которую стекаются данные об инцидентах, происходящих на большом количестве объектов, преимущественно объектов КИИ, при чем не зависимо от того, значимые это объекты или нет. Также немалое количество госорганов передают данные в эту систему, независимо от того, являются они или нет объектами КИИ, и, с вступлением в силу указа Президента № 250[15], ещё немалая доля компании попала под уведомления в сторону ГосСОПКА и, наконец, с 1 сентября 2022 года все операторы персональных данных (ПДн) обязаны передавать сведения об инцидентах с персональными данными в ГосСОПКА.

Важная особенность информирования о компьютерных инцидентах заключается в том, что информирование производится не зависимо от наличия или отсутствия значимых объектов. Различие сводится к регламентации времени сообщения об инцидентах в регулирующий орган. Если в случае

[14] Указ Президента РФ от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (с изменениями и дополнениями) // СПС «КонсультантПлюс».

[15] Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» // СПС «КонсультантПлюс».

значимых объектов выделяется три часа для уведомления о компьютерных инцидентах, то в случае незначимых – 24 часа. Это обязательный блок для всех субъектов КИИ вне зависимости от типа объекта. При этом форма взаимодействия может быть разной, как с условием использования специальных средств, так и, буквально, по почте.

В части ГосСОПКА регулятором является ФСБ России, которая создает специальный орган по реагированию на компьютерные инциденты – Национальный координационный центр по компьютерным инцидентам[16], являющийся, по факту, большим государственным SOC[17]. Соответственно, действующие приказы ФСБ непосредственно связаны с организацией работы данного Центра[18]. Помимо указанных приказов, в ФСБ разработан ряд рекомендаций в части взаимодействия с ГосСОПКА (ДСП).

Таким образом, основными регуляторами являются ФСТЭК и ФСБ. Если обратить внимание на разделение полномочий между органами власти, то складывается следующая картина:

– Правительство РФ определяет порядок: категорирования КИИ, госконтроля за безопасностью КИИ, подготовки сетей для функционирования КИИ;

– ФСТЭК отвечает за ведение реестра значимых ОКИИ, формирование требований по ИБ и контроль исполнения этих требований. Контролирует выполнение требований по категорированию объектов КИИ;

– ФСБ отвечает за создание ГосСОПКА, подключение к ней объектов КИИ управление инцидентами объектов КИИ, оценка безопасности объектов КИИ.

И, в заключение, несколько слов о киберинцидентах. Компьютерный инцидент, или киберинцидент, – факт нарушения безопасности КИИ. Кибератаки на объекты КИИ – это сложные многоходовые процессы, приводящие к несанкционированному воздействию на объекты КИИ в целях нарушения их функциональности и/или создания угрозы безопасности данных:

Категория	Типы киберинцидентов на объектах КИИ
Внедрение и распространение ВПО	– заражение вредоносным ПО (ВПО); – использование для распространения ВПО; – внедрение модулей ВПО.
Нарушение или замедление работы	– компьютерная атака типа DDoS; – несанкционированный вывод из строя; – непреднамеренное отключение.

[16] 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»)// СПС «КонсультантПлюс».

[17] Security Operations Center.

[18] Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»; Приказ Федеральной службы безопасности Российской Федерации от 19.06.2019 № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации»; Приказ Федеральной службы безопасности Российской Федерации от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации»; Приказ Федеральной службы безопасности Российской Федерации от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» // СПС «КонсультантПлюс».

Категория	Типы киберинцидентов на объектах КИИ
Несанкционированный доступ к ИР и ПТС	– эксплуатация уязвимостей; – компрометация учетной записи; – подбор паролей.
Сбор сведений об АИС	– попытки авторизации в АИС; – сканирование ресурсов АИС; – сканирование ИР; – перехват сетевого трафика; – социальная инженерия.
Нарушение конфиденциальности и целостности ИР	– разглашение информации; – несанкционированное изменение информации.
Распространение запрещенной информации	– рассылка спам-сообщений; – публикация запрещённого контента.
Мошенничество с ИР	– подделка личности/организации; – публикация мошеннических данных.

Довольно часто кибератаки на объекты КИИ начинаются со взлома или заражения SCADA (SupervisoryControlAndDataAcquisition) – программно-аппаратных комплексов управления киберфизическими системами с человеко-машинным интерфейсом (HMI, HumaneMachineInterface).

Наиболее известной атакой на КИИ считается вывод из строя центрифуг на заводе по обогащению урана в иранском городе Нетензе в 2009-2010 годах. Атака произведена с помощью червя Win32/Stuxnet, внедренного в заводскую сеть при помощи USB-flash накопителей.

По мнению ряда экспертов, Stuxnet представляет собой специализированную разработку спецслужб Израиля и США, направленную против ядерной программы Ирана.

Другой пример связан с атакой государственной информационной инфраструктуры Эстонии в 2007 году. Нападение на сайты правительства Эстонии, эстонских СМИ, банков и других организаций было связано с решением эстонских властей перенести памятник советским солдатам из центра Таллина на воинское кладбище. Против официальных сайтов Эстонии использовалась DDoS-атаки типа Ping of Death и SYN-флуд, Министр иностранных дел Эстонии публично обвинил российские власти в причастности к данным атакам, но не смог предоставить каких-либо доказательств.

12 мая 2017 года начал свое распространение по миру червь WannaCry. Атаке подвергалась информационная инфраструктура различных организаций на Украине, в Индии, Тайване и других странах. Код WannaCry эксплуатировал уязвимость Windows, которая была ранее выявлена Агентством национальной безопасности (АНБ) США.

В 2015 году была проведена многоходовая атака на энергосеть Украины. Сначала сотрудникам трех энергетических компаний были направлены фишинговые письма с вложенным документом формата MS Word. Для просмотра документа требовалось включить выполнение макросов, после чего на атакуемый компьютер устанавливалась программа под названием BlackEnergy3 с бэкдором для удалённого доступа [1].

Анализ киберинцидентов, связанных с КИИ, обостряет противоречие классического интернета вещей (IoT) между простотой управления по сети Интернет и защищенностью от кибератак.

Можно сформулировать ряд мер, повышающих уровень защиты объектов КИИ от кибератак:

1. Гибридная архитектура, разделяющая коммуникационные ИТ-сети и производственные ОТ-сети, которые непосредственно управляют элементами киберфизических систем, взаимодействующих с физическими объектами.

2. Сегментация сети и максимальная изоляция киберфизических систем от Интернета.

3. Непрерывный мониторинг функционирования объектов КИИ, в том числе с помощью комплексов SCADA.

4. Контроль изменения конфигурации АИС и подключения новых устройств, в том числе съемных носителей.

5. Регулярное обновление ПО.

6. Периодическое тестирование АИС на проникновение и на уязвимости ПТС.

7. Проверка лояльности авторизованных пользователей и обслуживающего персонала АС, в том числе методами OSINT (Open Source INTelligence – разведка по открытым источникам) и социальной инженерии.

Под безопасностью КИИ следует понимать такую степень защищенности, которая обеспечивает устойчивое функционирование объектов КИИ. С точки зрения закона, основное направление деятельности заключается в выявлении критических для государства объектов и обеспечении их безопасности.

Вполне очевидно, что для обнаружения угроз и реагирования на инциденты киберзопасности в режиме реального времени необходимо наличие специального подразделения, оснащенного специализированными средствами автоматизации выявления, реагирования и расследования инцидентов кибербезопасности.

Полноценная реализация информационной безопасности объектов КИИ в современных реалиях не возможна без импортозамещения. Сотрудничество с передовыми российскими разработчиками и практический опыт перехода с импортных информационных технологий и ИБ решений на отечественные позволяют учесть все потребности и ограничения заказчиков при выполнении поставленных задач. Однако такой переход будет связан со значительными финансовыми затратами, которые лягут на субъект КИИ, несмотря на государственную программу целевого субсидирования, осуществляемого на конкурсной основе. Тем более, что конкурс в 2021 году был отменен в связи с перераспределением бюджетных средств [10].

Основное содержание работы по обеспечению информационной безопасности объектов КИИ заключается в обеспечении их защиты от компьютерных атак, от целенаправленного воздействия аппаратных и программных средств, основной целью которых является прекращение или нарушение функционирования данных объектов и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

Исходя из того, что основной чертой Закона о защите КИИ является защита не только инфраструктуры самого субъекта КИИ, подвергшегося компьютерной атаке, но и недопущение негативных последствий для государства в целом, вызывает недоумение тот факт, что в нем не отражен госсектор. Закон призван на защиту КИИ, но большая часть госорганов, которые играют важную роль в обеспечении жизнедеятельности государства, не попадают в перечень тринадцати отраслей, зафиксированных в законе как субъекты КИИ.

Также на практике возникают проблемы с выделением объектов: на сколько их можно масштабировать или детализировать? По данной проблематике отсутствуют четкие критерии, поэтому вопрос решается на усмотрение субъекта КИИ. Возможно информационные системы делать отдельными объектами КИИ, так и «схлопывать» ИС в один объект КИИ, то есть в один объект может входить несколько информационных систем.

Существует уголовная ответственность за нарушение правил эксплуатации объектов КИИ при нанесении ущерба таким объектам, за утечки информации, за нарушения финансовой, налоговой, банковской и иных видов тайн. Имеет место дисциплинарная ответственность, но это уже внутренняя дело каждой организации. Законодательством предусмотрена гражданская ответственность, которая не так часто применяется в области кибербезопасности.

При этом надо понимать, что существует законодательство, а есть правоприменительная практика, которая имеет свою специфику. Поэтому *необходимо учитывать все факторы для построения сбалансированной, как с точки зрения законодательства, так и с точки зрения фактической результативной действенности, системы информационной безопасности объектов критической информационной инфраструктуры*.

Можно констатировать, что защита объектов КИИ является нетривиальной задачей, на выполнение которой оказывают влияние различные внутренние и внешние мешающие факторы. Пандемия вносит свои коррективы, так как в условиях удаленной работы многих сотрудников субъектов КИИ сложно выполнить условие нормативно-правового регулирования в части недопущения удаленного доступа.

СПИСОК ЛИТЕРАТУРЫ

1. Хонин А. Обеспечение безопасности объектов критической информационной инфраструктуры//URL: https://www.youtube.com/watch?v=MMu7wnIbqKE&t=158s (дата обращения: 11.03.2023).
2. Категорирование объектов критической информационной инфраструктуры. URL: https://www.youtube.com/watch?v=i1s3Q5c4yqA (дата обращения: 08.04.2023).
3. Андресс Дж. Защита данных. От авторизации до аудита. СПб.: Питер, 2021. 275 с.

4. Ашманов И., Касперская Н. Цифровая гигиена. СПб.: Питер, 2022. 340 с.
5. Белоус А.И., Солодуха В.А. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения. М.: Техносфера, 2021. 482 с.
6. Грей Дж. Социальная инженерия и этичный хакинг на практике. М.: ДМК, 2023. 228 с.
7. Келдыш Н.В. Системная защита информации компьютерных сетей. М.: Мир науки, 2022. 100 с.
8. Страхов А.А. Информационные технологии и информационная безопасность в ОВД. Основные термины и определения: словарь. М.: МУ МВД России, 2015. 143 с.
9. Горелик В.Ю., Безус М.Ю. О безопасности критической информационной инфраструктуры Российской Федерации // StudNet. 2020. № 9. С. 1438 - 1448.
10. Защита критической информационной инфраструктуры 2021-2022. Тренды и прогнозы. URL: https://www.youtube.com/watch?v=Ms-w_5wJGzM (дата обращения: 02.05.2023).

Поступила в редакцию 29.01.2024

Акапьев Виктор Львович, кандидат педагогических наук, доцент кафедры ИКТД ОВД
Белгородский юридический институт МВД России имени И.Д. Путилина
308024, Россия, г. Белгород, ул. Горького, 71
E-mail: akapevv@yandex.ru

Савотченко Сергей Евгеньевич, доктор физико-математических наук, доцент,
профессор кафедры математики
Российский государственный геологоразведочный университет имени Серго Орджоникидзе
117997, Россия, г. Москва, ГСП-7, ул. Миклухо-Маклая, 23
E-mail: savotchenkose@yandex.ru

V.L. Akap'ev, S.E. Savotchenko

PUBLIC LEGAL REGULATION OF THE SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE FACILITIES

DOI: 10.35634/2412-9593-2024-34-3-494-503

Transition of a public formation into the category of an information society, the introduction of information technologies and information systems for various purposes in all spheres of human activity unprecedentedly multiplies the importance of a nationwide information security system, reinforces the need to protect not only the information used, but also the objects of critical information infrastructure (CII) as key elements of ensuring the vital activity of the state. The above situation actualizes the need to study the public law regulation of this aspect of information security in order to resolve a number of contradictions between the interests of the subjects of the information space in the field of information security, to combine the provisions of normative legal acts regulating the requirements for ensuring the security of critical information infrastructure facilities with law enforcement practice in the current conditions, largely determined by the Covid 19 pandemic and permanent war, declared by the West against the Russian Federation. Almost six years have passed since the law "On the Security of the Critical Information Infrastructure of the Russian Federation" came into force, but so far most of the subjects of the CII, for one reason or another, have not fulfilled the requirements formulated in it, which gives the solution of the designated task not only theoretical and methodological, but also practical significance.

Keywords: information security, computer incident, critical information infrastructure, critical information infrastructure facilities, regulator.

Received 29.01.2024

Akapev V.L., Candidate of Pedagogy, Associate Professor
Putilin Belgorod Law Institute of Ministry of the Interior of Russia
Gorkogo st., 71, Belgorod, Russia, 308024
E-mail: akapevv@yandex.ru

Savotchenko S.E., Doctor of Physical and Mathematical Sciences, Associate Professor
Sergo Ordzhonikidze Russian Geological Prospecting State University,
Mikluho-Maklaya st., 23, Moscow, Russia, 117997
E-mail: savotchenkose@yandex.ru