Критически важный объект в контексте национальной безопасности

С.И. Луценко[1]

Эксперт НИИ Корпоративного и проектного управления (г. Москва). Аналитик Института экономический стратегий Отделения общественных наук Российской академии наук.

Соавтор документа «Стратегия развития электросетевого комплекса Российской Федерации».
Автор проекта «Контуры Концепции развития финансового кластера Российской Федерации на долгосрочную перспективу»
E-mail: scorp_ante@rambler.ru

Автор рассматривает особенности критически важных объектов (критической информационной инфраструктуры) в контексте национальной безопасности. Государство обязуется создать структуру, которая позволит обеспечить защиту от хакерских атак и информационную безопасность систем. Автор обращается к примерам других государств в отношении регулирования критически важных объектов.

Ключевые слова: критически важный объект, национальная безопасность, критическая информационная инфраструктура, компьютерная система, компьютерная атака

Начнем с определения критически важного объекта (далее – КВО).

КВО – это объект, нарушение или прекращение функционирования которого приведет к потере управления экономикой Российской Федерации, субъекта Российской Федерации или административно-территориальной единицы субъекта Российской Федерации, ее необратимому негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения [2].

Более комплексное определение КВО можно определить как совокупность объектов социальной, производственной, инженерно-транспортной, энергетической, информационно-коммуникационной и иной инфраструктуры, нарушение функционирования которых в результате акта терроризма может способствовать дестабилизации общественного порядка и достижению иных целей терроризма и (или) повлечь за собой человеческие жертвы, причинение вреда здоровью людей или окружающей среде, значительный материальный ущерб и нарушение условий жизнедеятельности людей; предусматриваются обязанности государственных органов и иных организаций в отношении таких объектов (включая организацию и (или) осуществление охранной деятельности и соблюдение требований безопасности, а также выполнение профилактических, режимных, организационных и иных мер по предупреждению террористической деятельности и минимизации ее последствий), направленные на недопущение совершения актов терроризма на указанных объектах.

Причем законодательное регулирование действий государственных органов и иных организаций, эксплуатирующих критически важные объекты, связано с недопущением совершения актов терроризма на данных объектах и защищает независимость и территориальную целостность, конституционный строй, обеспечивая законность и правопорядок [6].

Приведем небольшой пример.

В целях достижения киберустойчивости в рамках КВО в Республике Беларусь реализуется особый комплекс правовых, организационных и технических мероприятий, основанный на выработке критериев отнесения объектов к такой категории и принятии в их

[1] Автор благодарит Чеснокова А.Н. за идею и ценные замечания.

отношении соответствующих целенаправленных и всесторонних защитных мер. Данный подход позволяет создавать индивидуальную модель безопасности каждого КВО с учетом систематизированных общих требований по безопасности, эффективно выявлять и оценивать риски, поддерживать высокую готовность к предупреждению и локализации последствий кибератак, а также проводить внешнюю оценку созданных систем безопасности [3].

Кроме того, принято Положение об обеспечении безопасности критически важных объектов.

В частности, в Положении устанавливается порядок организации мероприятий по обеспечению безопасности критически важных объектов информатизации (далее - КВОИ), включая мероприятия по созданию системы безопасности КВОИ правового, организационного и технического характера, мониторингу угроз безопасности КВОИ и реагированию на такие угрозы.

В свою очередь, в ходе создания системы безопасности КВОИ осуществляются, в числе прочих, определение физических и логических границ области применения системы безопасности (формуляр, паспорт) с использованием структурной и логической схем КВОИ. Структурная схема отражает расположение физических устройств с номерами портов, а также физических линий связи, соединяющих физические интерфейсы технических, программно-аппаратных средств обработки информации. В логической схеме отражаются информационные системы, направления потоков данных, а также спецификация используемых технологий и протоколов, списки VLAN, IP-адреса устройств [4].

В свою очередь, в соответствии со Стратегией национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации [7], к одним из основных угроз государственной и общественной безопасности относятся: деятельность террористических и экстремистских организаций, направленная на насильственное изменение конституционного строя Российской Федерации, дестабилизацию работы органов государственной власти, уничтожение или нарушение функционирования военных и промышленных объектов, объектов жизнеобеспечения населения, транспортной инфраструктуры, устрашение населения, в том числе путем завладения оружием массового уничтожения, радиоактивными, отравляющими, токсичными, химически и биологически опасными веществами, совершения актов ядерного терроризма, нарушения безопасности и устойчивости функционирования критической информационной инфраструктуры Российской Федерации.

Федеральным законом «О безопасности критической информационной инфраструктуры» (вступил в силу 01.01.2018) [8] предусматривается создание государственной структуры, обеспечивающей защиту от хакерских атак и информационную безопасность информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления.

Федеральным законом определяются основы и принципы обеспечения безопасности критической информационной инфраструктуры Российской Федерации, в том числе основы функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, которая представляет собой единый территориально распределенный комплекс, включающий в себя силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Нормативный акт устанавливает механизм предупреждения компьютерных инцидентов на объектах критической информационной инфраструктуры Российской Федерации, который позволит существенно уменьшить негативные последствия для Российской Федерации в случае проведения против нее компьютерных атак.

Федеральным законом даны определения таких понятий, как «критическая информационная инфраструктура Российской Федерации», «объекты критической информационной инфраструктуры Российской Федерации», «субъекты критической информационной

инфраструктуры Российской Федерации», «компьютерная атака», «компьютерный инцидент».

В частности, критическая информационная инфраструктура (далее – КИИ) определяется как объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов". Объекты КИИ определяются как информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры, а субъектами КИИ выступают государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Кроме того, Федеральный закон «О безопасности критической информационной инфраструктуры» устанавливает критерии категорирования КИИ: это социальная, политическая, экономическая, экологическая значимость, а также значимость для обеспечения обороны страны, безопасности государства и правопорядка.

Кроме того, в законе устанавливаются полномочия органов государственной власти Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, права и обязанности субъектов критической информационной инфраструктуры Российской Федерации, а также вводится институт категорирования объектов критической информационной инфраструктуры Российской Федерации.

Так, к полномочиям органов государственной власти Российской Федерации отнесены в числе прочих: утверждение показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и значений таких показателей; ведение реестра значимых объектов критической информационной инфраструктуры Российской Федерации; утверждение порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации; установление требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации; оценка безопасности критической информационной инфраструктуры Российской Федерации; государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

К обязанностям субъектов критической информационной инфраструктуры Российской Федерации Федеральным законом отнесены, в частности: присвоение принадлежащим им на законном основании объектам критической информационной инфраструктуры Российской Федерации одной из категорий значимости; информирование о компьютерных инцидентах федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации; соблюдение требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

В статье 5 Закона [8] перечислены организации и структуры, входящие в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

После вступления в силу данного федерального закона российские регионы начали формировать направления информационной безопасности в отношении критической информационной инфраструктуры.

Рассмотрим пример Сингапура.

В законодательстве государства Сингапура дается определение КИИ как компьютера или компьютерной системы, которые полностью или частично находятся в Сингапуре, необходимы для непрерывного функционирования существенных служб, а утеря контроля над ними или причинение им вреда окажет негативное влияние на доступность существенной службы [9].

Кроме того, законодательство устанавливает процедуру идентификации информационных сетей как КИИ: уполномоченный орган издает предписание (notice), содержащее юридически обязательное требование конкретному субъекту об отнесении его компьютера или компьютерной системы к КИИ. Основаниями для идентификации КИИ выступают следующие: компьютер или компьютерная система являются необходимыми для постоянного обслуживания существенной службы, а утеря контроля над ними или причинение им вреда окажет негативное влияние на доступность существенной службы; (компьютер или компьютерная система полностью или частично расположены на территории Сингапура.

Изданное предписание (notice) должно содержать следующую информацию: описание компьютера или компьютерной системы, которые идентифицируются как КИИ; данные о субъекте компьютера или компьютерной системы, которые идентифицируются как КИИ; права и обязанности субъекта КИИ; данные о должностном лице уполномоченного органа, ответственном за КИИ; уведомление субъекта КИИ о сроках предоставления возражений против этого предписания в уполномоченный орган; информация о порядке обжалования данного предписания в Министерстве коммуникации и информации Сингапура.

В Стратегии кибербезопасности Сингапура от 2016 года выделены четыре основных направления обеспечения безопасности КИИ: построение устойчивой инфраструктуры для усиления КИИ путем тесного сотрудничества частного сектора и представителей публичного сектора, уполномоченных на обеспечение кибербезопасности; создание безопасного киберпространства путем привлечения не только правительственных субъектов, но и гражданского общества и предпринимателей; развитие динамичной экосистемы кибербезопасности за счет увеличения количества специалистов в результате сотрудничества частного сектора и образовательных заведений; усиление международного сотрудничества, особенно в рамках АСЕАН.

В Сингапуре институциональный механизм обеспечения безопасности КИИ представлен органом специальной компетенции - Агентством кибербезопасности Сингапура, обладающим широкими полномочиями.

В Сингапуре государственный контроль в сфере КИИ реализуется опосредованно - через аудиторов, и отчет в Агентство кибербезопасности направляется не самим аудитором, а субъектом КИИ. Интересен и опыт проведения учений для субъектов КИИ - эти учения носят не всеохватывающий характер, а избирательный - для определенных объектов и субъектов КИИ, готовых/неготовых к кибератакам разного уровня и интенсивности. Так, достигается эффективность применения мер безопасности по отношению к разным секторам КИИ.

Недостатком российского законодательства является отсутствие правового регулирования процедуры идентификации информационных сетей как объектов и организаций как субъектов КИИ. Особенностью российского механизма является множественность субъектов, обеспечивающих безопасность КИИ, в отличие от сингапурского, представленного одним ведомством. Преимуществом российского механизма является участие службы, располагающей специальными силами и средствами, а также наделенной процессуальными полномочиями по оперативному реагированию на кибератаки [1].

В заключение, приведем интересный пример муниципалитета Курской области в сфере КИИ.

Муниципалитет, прежде всего, руководствовался общим положением Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» [8] о том, что должна быть обеспечена безопасность критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении нее компьютерных атак.

В соответствии с Распоряжением администрации г. Курчатова Курской области «Об утверждении основных направлений политики информационной безопасности администрации города Курчатова» [5], в муниципалитете должны быть определены и прокатегорированы объекты критической информационной инфраструктуры. Категорирование объекта критическое информационной инфраструктуры представляет собой установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.

В соответствии с критериями значимости и показателями их значений, а также порядком осуществления категорирования присваивается одна из категорий значимости объектам критической информационной инфраструктуры. Если объект критической информационной инфраструктуры не соответствует критериям значимости, показателям этих критериев и их значениям, ему не присваивается ни одна из таких категорий.

В целях обеспечения безопасности значимого объекта критической информационной инфраструктуры в соответствии с требованиями к созданию систем безопасности таких объектов и обеспечению их функционирования, утвержденными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, создается система безопасности такого объекта и обеспечивается ее функционирование.

Основными задачами системы безопасности значимого объекта критической информационной инфраструктуры являются: предотвращение неправомерного доступа к информации, обрабатываемой значимым объектом критической информационной инфраструктуры, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации; недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта критической информационной инфраструктуры; восстановление функционирования значимого объекта критической информационной инфраструктуры, обеспечиваемого в том числе за счет создания и хранения резервных копий необходимой для этого информации; непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, устанавливаемые федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, дифференцируются в зависимости от категории значимости объектов критической информационной инфраструктуры.

В администрации города Курчатова должны быть назначены сотрудники, ответственные за ведение реестра объектов критической информационной инфраструктуры и обеспечение на них безопасности информации.

В целях противодействия угрозам информационной безопасности Российской Федерации при использовании информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации администрация города Курчатова должна осуществить подключение находящихся в их ведении государственных ИС и информационно-телекоммуникационных сетей к российскому государственному сегменту сети «Интер-

нет» (далее - RSNet) и обеспечить размещение (публикацию) информации в сети «Интернет» в соответствии с порядком, утвержденным Указом Президента Российской Федерации от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации».

Подключение ИС и информационно-телекоммуникационных сетей к сети «Интернет» через сегмент RSNet осуществляется по каналам передачи данных, защищенным с использованием шифровальных (криптографических) средств. Защита информации в ИС и информационно-телекоммуникационных сетях, подключаемых к сети "Интернет" через российский сегмент RSNet, обеспечивается в соответствии с законодательством Российской Федерации.

Поддержание, эксплуатацию и развитие российского государственного сегмента RSNet обеспечивает Федеральная служба охраны Российской Федерации.

Технические условия подключения к сети «Интернет» и размещения (публикации) в ней информации через сеть RSNet определяются Соглашением о подключении к информационно-телекоммуникационной сети «Интернет» и размещении (публикации) в ней информации через российский государственный сегмент сети "Интернет" (сеть RSNet) и включают в себя следующие технические параметры подключения: технологическая площадка, через которую осуществляется подключение; тип канала связи; скорость передачи данных; логические характеристики подключения; требования по обеспечению информационной безопасности.

Процедура подключения ИС и информационно-телекоммуникационных сетей к сети RSNet включает в себя следующие этапы: обращение муниципалитета в адрес оператора сети RSNet; заключение Соглашения; организация подключения ИС и информационно-телекоммуникационных сетей к сети «Интернет» через сеть RSNet в соответствии с Техническими условиями.

В данном случае, на уровне муниципалитета формулируются основные направления политики информационной безопасности администрации города, определяется система приоритетов, принципов и методов достижения информационной безопасности конфиденциальной информации и электронных информационных ресурсов. В свою очередь, меры защиты информации, направлены на нейтрализацию актуальных угроз информационной безопасности, потенциально опасных для конфиденциальной информации, обрабатываемой в администрации города.

Результаты анализа опыта правового регулирования безопасности критической информационной инфраструктуры стран с развитой информационной инфраструктурой, таких как Германия, США, Великобритания, Япония и Южная Корея, а также международных правовых актов в данной области, показывают, что обеспечение безопасности критической информационной инфраструктуры Российской Федерации исключительно силами и средствами государства невозможно. Существенная часть объектов критической информационной инфраструктуры в этих странах, как и в Российской Федерации, не находится в собственности государства.

Тем не менее, создание правовой и организационной основы для эффективного функционирования системы безопасности критической информационной инфраструктуры Российской Федерации, позволит предупредить возникновения компьютерных инцидентов на ее объектах, а также существенно снизит политические, финансовые и иные негативные последствия для Российской Федерации в случае проведения против нее компьютерных атак.

Литература

1. Горян Э.В. Институциональные механизмы обеспечения безопасности критической информационной инфраструктуры Российской Федерации и Сингапура: сравнительно-правовой аспект // Административное и муниципальное право. 2018. N 9. С. 49 – 60

2. ГОСТ Р 22.2.06-2016. Национальный стандарт Российской Федерации. Безопасность в чрезвычайных ситуациях. Менеджмент риска чрезвычайной ситуации. Оценка риска чрез-

вычайных ситуаций при разработке паспорта безопасности критически важного объекта и потенциально опасного объекта (утв. и введен в действие Приказом Росстандарта от 29.06.2016 № 726-ст) // М.: Стандартинформ. 2016.
3. Постановление Совета Безопасности Республики Беларусь от 18.03.2019 № 1 «О Концепции информационной безопасности Республики Беларусь» // Доступ из СПС «Консультант Плюс».
4. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 12.10.2018 № 151 «Об утверждении Положения об обеспечении безопасности критически важных объектов информатизации» // Доступ из СПС «Консультант Плюс».
5. Распоряжение администрации г. Курчатова Курской области от 07.11.2018 № 428р «Об утверждении основных направлений политики информационной безопасности администрации города Курчатова» Доступ из СПС «Консультант Плюс».
6. Решение Конституционного Суда Республики Беларусь от 28.12.2017 № Р-1113/2017 // Доступ из СПС «Консультант Плюс».
7. Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. 2016. № 1 (часть II).
8. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры» // // Собрание законодательства РФ. 2017. № 31 (1 ч.).
9. Singapore's Cybersecurity Strategy 2016 // Cyber Security Agency of Singapore. https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy