УДК 004.056.57
ББК Х404.06 + 79(2)-983

Вестник УрФО № 1(27) / 2018, с. 71–76

Ванцева И. О., Зырянова Т. Ю., Медведева О. О.

ВЛИЯНИЕ ФЕДЕРАЛЬНОГО ЗАКОНА «О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ» НА ВЛАДЕЛЬЦЕВ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР

В статье рассмотрены актуальные вопросы, связанные с выходом федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», а также отражены основные аспекты категорирования объектов критической информационной инфраструктуры, о котором говорится в Постановлении Правительства от 08.02.2018 г. № 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», также в статье указано, что такое ГосСОПКА, для чего создана и какие функции должна выполнять.

Ключевые слова: *критическая информационная инфраструктура, информационная безопасность, категорирование объектов.*

INFLUENCE OF THE FEDERAL LAW «ON THE SECURITY OF THE CRITICAL INFORMATION INFRASTRUCTURE OF THE RUSSIAN FEDERATION» ON OWNERS OF CRITICAL INFORMATION INFRASTRUCTURES

The article deals with topical issues related to the issue of the federal law of July 26, 2017 No 187-FL «On the Security of the Critical Information Infrastructure of the Russian Federation», and also reflects the main aspects of categorizing critical information infrastructure facilities, which is mentioned in the Government Decree of 08.02.2018 No 127 «On approval of the Rules for the categorization of critical information infrastructure of the Russian Federation, as well as a list of indicators of criticality criteria for critical information objects information infrastructure of the Russian Federation and their values», as the article states that such SSDPECA, for what is created and what features should perform.

Keywords: *critical information infrastructure, information security, categorization of objects.*

На сегодняшний день хакерские атаки грозят неприятностями не только владельцам компьютеров, но и промышленным технологическим системам, и информационным системам жизнеобеспечения городов, и других объектов, входящих в критическую информационную инфраструктуру. Последствия этих сбоев могут быть катастрофичны, поэтому в России принят Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», направленный на защиту такой инфраструктуры.

Весь мир сосредоточен на проблеме обеспечения безопасности инфраструктуры и информационных систем. Компании и госструктуры подсчитывают потенциальные убытки, которые могут понести в ситуации, если не будут готовы к внезапному нападению на свои системы. Поэтому тема безопасности в нынешнее время наиболее актуальна, особенно если речь идет об объектах инфраструктуры, от которых напрямую зависит жизнедеятельность целых городов, отдельных регионов, а то и всей страны.

В конце 2016 года в Госдуму был внесен законопроект «О безопасности критической информационной инфраструктуры Российской Федерации». Тема вызвала у специалистов интерес, но оставила массу сомнений относительно возможности реализации законопроекта на практике.

Критическая информационная инфраструктура Российской Федерации – совокупность объектов критической информационной инфраструктуры (КИИ), а также сетей электросвязи, используемых для организации взаимодействия объектов КИИ между собой.

К объектам КИИ можно отнести информационные системы, информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, области здравоохранения, транспорта, связи, кредитно-финансовой сфере, энергетике, топливной промышленности, атомной промышленности, ракетно-космической промышленности, горнодобывающей промышленности, металлургической промышленности и химической промышленности[1].

Процесс принятия законопроекта тянулся очень долго не случайно. Сейчас, после принятия закона, владельцы КИИ обязаны провести ряд технических и информационных мероприятий по защите объектов. Разумеется, это потребует финансовых вложений, причем внушительных (речь идет о критической инфраструктуре). Взламывают КИИ не так уж часто. Однако если инцидент происходит, то последствия бывают весьма плачевными. Последняя крупная кибератака произошла в мае 2017 года.

WannaCry (также известна как WannaCrypt, WCry, WanaCrypt0r2.0 и Wanna Decryptor) — вредоносная программа, сетевой червь и программа-вымогатель денежных средств, поражающая только компьютеры под управлением операционной системы Microsoft Windows. Программа шифрует почти все хранящиеся на компьютере файлы и требует денежный выкуп за их расшифровку. Её массовое распространение началось 12 мая 2017 года — одними из первых были атакованы компьютеры в Испании, а затем и в других странах. Среди них по количеству заражений лидировали Россия, Украина и Индия. В общей сложности, от червя пострадало более 500 тысяч компьютеров, принадлежащих частным лицам, коммерческим организациям и правительственным учреждениям, в более чем 150 странах мира

Приоритет предупреждения компьютерной атаки перед устранением ее последствий – один из основополагающих принципов обеспечения информационной безопасности вообще и безопасности критической инфраструктуры в частности.

Появление новой Доктрины информационной безопасности России было обусловлено тем, что предыдущая версия, утвержденная в 2000 году, утратила силу. За последние 17 лет в стране произошли существенные изменения в части технологического развития в мире в целом и на различных предприятиях в частности. Вместе с тем возросло и число потенциальных угроз. Утверждение подобного документа стало важнейшим этапом для всей отрасли информационной безопасности. Теперь государство рассматривает информационную безопасность как составляющую национальной безопасности. Кроме того, в Доктрине существенно расширен круг сфер, в которых должна обеспечиваться информационная безопасность: здравоохранение, транспорт, связь, энергетика и промышленность. Также особенный акцент сделан на обеспечение информационной безопасности в кредитно-финансовой сфере[2].

Законопроект «О безопасности КИИ», подготовленный в рамках Доктрины, в первую очередь был направлен на регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры РФ в целях ее устойчивого функционирования при проведении компьютерных атак. Он вводит четкое разделение обязанностей по обеспечению безопасности, а также устанавливает полномочия государственных органов в этом вопросе. В проекте оговариваются процедуры государственного контроля КИИ и порядок подготовки и контроля единой сети электросвязи, обеспечивающей функционирование сетей и групп КИИ. Зафиксирована возможность дифференцированных наказаний за нарушение закона – от административной до уголовной ответственности.

К объектам подобной инфраструктуры отнесены информация, информационные системы, телекоммуникационные сети и автоматизированные системы управления технологическими процессами.

Такие системы должны обеспечивать:

- предотвращение неправомерного доступа к информации, обрабатываемой значимыми объектами, 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 значимых объектов;

- восстановление функционирования значимых объектов, 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 России.

Согласно приказу ФСТЭК России № 235 от 21.12.2017 г. «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования» субъекты КИИ должны создавать системы безопасности, включающие в себя правовые, организационные и технические меры защиты информации субъектов КИИ.

Данные системы должны обеспечивать устойчивую работоспособность значимых объектов КИИ.

Системы безопасности включают силы обеспечения безопасности значимых объектов КИИ, к которым относятся подразделения субъекта КИИ, обеспечивающие безопасность КИИ, эксплуатацию объектов КИИ и их функционирование.

Системы безопасности должны функционировать согласно организационно-распорядительным документам, разработанным согласно Требованиям, прописанным в федеральном законе «О безопасности критической информационной инфраструктуры Российской Федерации».

Категорирование объектов критической информационной инфраструктуры (КИИ) осуществляется субъектами КИИ в отношении принадлежащих им объектов КИИ. Для присвоения категории создается специальная комиссия. Об этом говорится в Постановлении Правительства от 08.02.2018 г. № 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».

Так же в нем регламентируются порядок и сроки категорирования объектов КИИ, перечень критериев значимости объектов КИИ, и показателей для количественной оценки значения критерия.

Для проведения категорирования решением руководителя субъекта критической информационной инфраструктуры создается комиссия по категорированию, в состав которой включаются: руководитель подразделения, работники по ГТ и работники по ГО и ЧС.

Комиссия по категорированию в ходе своей работы:

а) определяет процессы, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры;

б) выявляет наличие критических процессов у субъекта критической информационной инфраструктуры;

в) выявляет объекты критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов, а также готовит предложения для включения в перечень объектов;

г) рассматривает возможные действия нарушителей в отношении объектов критической информационной инфраструктуры, а также иные источники угроз безопасности информации;

д) анализирует угрозы безопасности информации и уязвимости, которые могут привести к возникновению компьютерных инцидентов на объектах критической информационной инфраструктуры;

е) оценивает в соответствии с перечнем показателей критериев значимости масштаб возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры;

ж) устанавливает каждому из объектов критической информационной инфраструктуры одну из категорий значимости либо принимает решение об отсутствии необходимости присвоения им категорий значимости[3].

Исходя из результата работы комиссии объекту КИИ присваивается категория значимости согласно перечню показателей критериев значимости.

Значимость определяется размером ущерба, который будет причинен государству, обществу и владельцу КИИ в случае выхода из строя объекта.

Показатели сгруппированы по пяти типам значимости: социальная, политическая, экономическая, экологическая и значимость для обеспечения обороны страны, безопасности государства и правопорядка. Например, к социальной значимости относится критерий

«Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов)»; к политической – «Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации» и т. д.

Постановлением ограничен срок категорирования после утверждения субъектом КИИ до одного года. Далее в течение пяти рабочих дней необходимо направить перечень объектов в федеральные органы исполнительной власти, уполномоченные в области обеспечения безопасности КИИ.

Комиссия оформляет свое решение по категорированию актом и подписывает его. Руководитель субъекта КИИ утверждает акт и направляет в течение 10 дней данные в органы исполнительной власти, уполномоченные в области обеспечения безопасности КИИ (см. рис.).

Субъект КИИ обязан не реже раза в 5 лет осуществлять пересмотр присвоенной категории значимости в соответствии с Правилами, утвержденными постановлением Правительства № 127 от 08.02.2017 г. Ведь вместе с утверждением ФЗ «О безопасности КИИ» в УК РФ была добавлена новая статья 274.1, которая устанавливает уголовную ответственность должностных лиц субъекта КИИ за несоблюдение установленных правил эксплуатации технических средств объекта КИИ или нарушение порядка доступа к ним вплоть до лишения свободы сроком на 6 лет. Пока данная статья не предусматривает ответственности за невыполнение необходимых мероприятий по обеспечению безопасности объекта КИИ, однако в случае наступления последствий (аварий и чрезвычайных ситуаций, повлекших за собой крупный ущерб) непринятие таких мер подпадает по состав 293 статьи УК РФ «Халатность». Дополнительно следует ожидать внесения изменений в административное законодательство в части определения штрафных санкций для юридических лиц за неисполнение Закона. С большой долей уверенности можно говорить о том, что именно введение существенных денежных штрафов будет стимулировать субъекты КИИ к выполнению требований Закона.

В соответствии с федеральным законом от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» органы государственной власти, государственные корпорации и другие организации, относящиеся к КИИ, должны создать у себя ведомственные или корпоративные центры ГосСОПКА (государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации). Для этого организациям необходимы соответствующие технические решения и высокая экспертиза аналитиков, которая позволит осуществлять мониторинг, анализ и расследование инцидентов, а также выполнять ряд других функций.

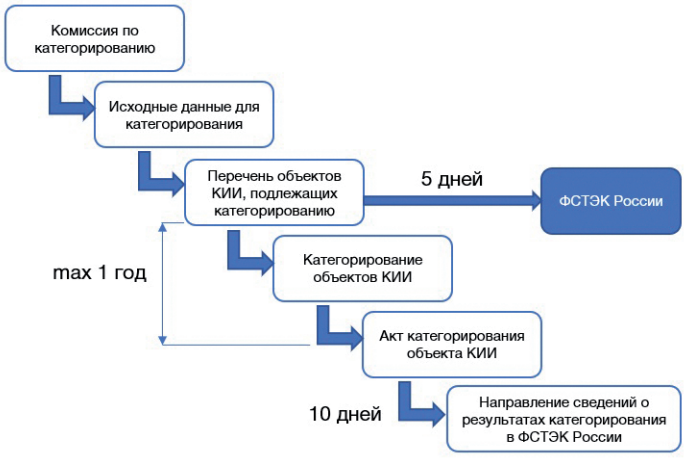

Схема категорирования объектов КИИ

Литература

1. О безопасности критической информационной инфраструктуры Российской Федерации: от 26.07.2017 № 187-ФЗ (последняя редакция) // Консультант Плюс. Законодательство. ВерсияПроф [Электронный ресурс] / АО «Консультант Плюс». – М., 2018.

2. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) // Консультант Плюс. Законодательство. ВерсияПроф [Электронный ресурс] / АО «Консультант Плюс». – М., 2018.

3. 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 от 08.02.2018 г. № 127: Постановление Правительства // Консультант Плюс. Законодательство. ВерсияПроф [Электронный ресурс] / АО «Консультант Плюс». – М., 2018.

References

1. On the Security of the Critical Information Infrastructure of the Russian Federation: dated July 26, 2017 No. 187-FL (last version) // Consultant Plus. Legislation. VersionProf [Electronic resource] / JSC Consultant Plus. - M., 2018.

2. The Doctrine of Information Security of the Russian Federation (approved by the Decree of the President of the Russian Federation of December 5, 2016 No. 646) // Consultant Plus. Legislation. VersionProf [Electronic resource] / JSC Consultant Plus. - M., 2018.

3. On the approval of the rules for categorizing the objects of the critical information infrastructure of the Russian Federation, as well as the list of indicators of criteria for the significance of critical information infrastructure facilities of the Russian Federation and their values dated 08.02.2018 No. 127 - Government Decision // Consultant Plus. Legislation. VersionProf [Electronic resource] / JSC Consultant Plus. - M., 2018.

ВАНЦЕВА Ирина Олеговна, магистрант кафедры «Информационные технологии и защита информации» Уральского государственного университета путей сообщения, 620034, г. Екатеринбург, ул. Колмогорова, д. 66. E-mail: east_94@mail.ru

VANTSEVA Irina, Graduate student of Department «Information Technology and Information Security» of the Ural State University of Railway Transport. Bld. 66, Kolmogorova str., Yekaterinburg, 620034. E-mail: east_94@mail.ru

ЗЫРЯНОВА Татьяна Юрьевна, заведующий кафедрой «Информационные технологии и защита информации» Уральского государственного университета путей сообщения, канд. тех. наук. 620034, г. Екатеринбург, ул. Колмогорова, д. 66. E-mail: tzyryanova@usurt.ru

ZYRYANOVA Tatiana, Chief of Department «Information Technology and Information Security» of the Ural State University of Railway Transport. Bld. 66, Kolmogorova str., Yekaterinburg, 620034. E-mail: tzyryanova@usurt.ru

МЕДВЕДЕВА Оксана Олеговна, магистрант кафедры «Информационные технологии и защита информации» Уральского государственного университета путей сообщения, 620034, г. Екатеринбург, ул. Колмогорова, д. 66. E-mail: oks__@mail.ru

MEDVEDEVA Oksana, Graduate student of Department «Information Technology and Information Security» of the Ural State University of Railway Transport. Bld. 66, Kolmogorova str., Yekaterinburg, 620034. E-mail: oks__@mail.ru