www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.3.2

УДК 004:002(470+571)
ББК 32.973(2Рос)

ОСНОВНЫЕ ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ В УСЛОВИЯХ ПЕРЕХОДА К ЦИФРОВОЙ ЭКОНОМИКЕ

Рашит Мутагарович Романов

Заместитель руководителя Управления Федеральной службы по техническому и экспортному контролю России по Южному и Северо-Кавказскому федеральным округам
uzhfo@fstec.ru
ул. Рабоче-Крестьянская, 1, 400074 г. Волгоград, Российская Федерация

Аннотация. В статье анализируются требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Показано, что они должны выполняться на всех стадиях (этапах) жизненного цикла в ходе создания (модернизации), эксплуатации и вывода из эксплуатации значимого объекта.

Ключевые слова: информационная безопасность, информационная инфраструктура, информационные технологии, безопасность государства, цифровая экономика.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы. Информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

Расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы.

Ситуация значительно усложняется возникшей конфронтацией Российской Федерации со странами Запада, напрямую затрагивающей сферу национальных интересов Российской Федерации и представляющей непосредственную угрозу национальной безопасности страны, ключевым звеном которой является информационная безопасность [1; 2].

В своей речи на заседании Совета Безопасности 26 октября 2017 г. Президент Российской Федерации отметил, что устойчивая работа информационных систем, средств коммуникации и связи, их защищенность имеют для страны стратегическое значение. Это важный фактор обеспечения суверенитета, обороноспособности, безопасности государства, эффективного развития экономики, социальной сферы, государственного управления на базе передовых, в том числе цифровых технологий.

Фиксируется постоянный рост компьютерных атак на российские информационные ресурсы, за последнее время количество атак увеличилось в разы. При этом методы, средства и тактика проведения подобных атак совершенствуются, а их интенсивность прямо зависит от текущей международной обстановки.

В Глобальной сети открыто распространяются материалы террористической и экстремистской направленности. Увеличилось количество преступлений, совершённых с использованием информационных технологий, например, незаконных проникновений в корпоративные сети государственных и кредитно-финансовых учреждений

В этих условиях Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 утверждена новая Доктрина информационной безопасности Российской Федерации, представляющая собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

Другим указом Президента Российской Федерации, от 9 мая 2017 г. № 203, утверждена Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг., в которой большое внимание уделено обеспечению комплексной защиты информационной инфраструктуры Российской Федерации, в том числе инфраструктуры электронного правительства, частью которой являются региональные государственные и муниципальные информационные системы в органах исполнительной власти и органах местного самоуправления.

ФСТЭК России в своей деятельности, в пределах своих полномочий, уделяет самое пристальное внимание вопросам разработки обоснованных, технически и практически реализуемых условий и требований, обеспечивающих гарантированную нейтрализацию возможных угроз информационной безопасности Российской Федерации.

В рамках работ по совершенствованию технической защиты информации (ТЗИ) в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации и органах местного самоуправления ФСТЭК России, руководствуясь требованиями Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», продолжает практику проведения семинаров и сборов со специалистами подразделений по ТЗИ, в том числе ТЗИ ограниченного доступа, не содержащей сведения, составляющие государственную тайну [3–6].

Определяющим фактором, регламентирующим деятельность по ТЗИ ограниченного доступа, не содержащей сведения, составляющие государственную тайну, является выполнение комплекса организационных и технических мероприятий, включающих в себя разработку нормативных, методических и организационно-распорядительных документов, аттестацию объектов информатизации, в том числе государственных (муниципальных) информационных систем, контроль за соблюдением персоналом требований по защите информации, проводимых в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17.

Стоит отметить, что с учетом факторов роста рисков и угроз информационной безопасности для объектов информационной инфраструктуры Российской Федерации 26 июля 2017 г. был принят Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – Закон). Указанный Закон вступил в силу 1 января 2018 года.

Новый Закон предназначен для регулирования отношений в области обеспечения безопасности объектов информационной инфраструктуры Российской Федерации, функционирование которых критически важно для экономики и жизнедеятельности государства. Такие объекты в законе называются объектами критической информационной инфраструктуры (далее – объекты КИИ). Согласно Закону, к объектам КИИ могут быть отнесены информационные системы и сети, а также автоматизированные системы управления, функционирующие в сфере:

– здравоохранения;

– науки;

– транспорта;

– связи;

– энергетики;

– банковской и иных сферах финансового рынка;

– топливно-энергетического комплекса;

– атомной энергии;

– оборонной и ракетно-космической промышленности;

– горнодобывающей, металлургической и химической промышленности.

Объекты КИИ, а также сети электросвязи, используемые для организации взаимодействия между ними, составляют понятие критической информационной инфраструктуры.

Главной целью обеспечения безопасности КИИ является устойчивое функционирование КИИ при проведении в отношении нее компьютерных атак. Одним из главных принципов обеспечения безопасности является предотвращение компьютерных атак. До появления нового закона о КИИ в сфере информационной безопасности существовало похожее понятие ключевых систем информационной инфраструктуры (КСИИ). Однако с 1 января 2018 г. понятие КСИИ было официально заменено на понятие «значимые объекты КИИ».

В соответствии с Законом определены полномочия органов государственной власти Российской Федерации в области обеспечения безопасности КИИ.

В частности:

– определены полномочия федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности КИИ Российской Федерации. Таким федеральным органом исполнительной власти является ФСТЭК России в соответствии с изменениями, внесенными Указом Президента Российской Федерации от 25 ноября 2017 г. № 569 в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085;

– определены полномочия федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Что входит в полномочия Федеральной службы безопасности Российской Федерации.

В соответствии с Законом Правительство Российской Федерации, ФСТЭК России, ФСБ России и Минкомсвязи разрабатывают и утверждают нормативно-правовые акты, регулирующие вопросы в области обеспечения безопасности КИИ в части определенных полномочий.

ФСТЭК России, в пределах своей компетенции государственной политики в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, осуществляет самостоятельное нормативно-правовое регулирование вопросов обеспечения безопасности значимых объектов критической информационной инфраструктуры, а также осуществляет государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры. Правила осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации утверждены Постановлением Правительства Российской Федерации от 17 февраля 2018 г. № 162. Форма акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утверждена приказом ФСТЭК России от 11 декабря 2017 г. № 229.

Согласно Закону, субъекты КИИ должны:

– провести категорирование объектов КИИ;

– обеспечить интеграцию (встраивание) в Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА);

– принять организационные и технические меры по обеспечению безопасности объектов КИИ.

Стоит обратить внимание, что категорированию подлежат объекты КИИ, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ.

Категорирование объекта КИИ предполагает определение его категории значимости на основе ряда критериев и показателей. Всего устанавливается три категории – первая, вторая или третья (в порядке убывания значимости). Если объект КИИ не соответствует ни одному из установленных критериев, ему категория не присваивается. Те объек-

ты КИИ, которым была присвоена одна из категорий, называются в законе значимыми объектами КИИ.

По завершении категорирования сведения о его результатах должны направляться субъектом КИИ во ФСТЭК России для включения в реестр значимых объектов КИИ.

Важно отметить, что если в процессе категорирования было определено отсутствие категории значимости у объекта КИИ, результаты категорирования все равно должны быть представлены во ФСТЭК России. Регулятор проверяет представленные материалы и при необходимости направляет замечания, которые должен учесть субъект КИИ.

Порядок ведения реестра значимых объектов КИИ определяется приказом ФСТЭК России от 6 декабря 2017 № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации».

Показатели критериев значимости, а также порядок и сроки категорирования определены в Правилах категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденных Постановлением правительства от 8 февраля 2018 г. № 127. Правила регламентируют процедуру категорирования, а также содержат перечень критериев и их показатели для значимых объектов КИИ первой, второй и третьей категории.

Категорирование должно проводиться как для существующих, так и для создаваемых или модернизируемых объектов КИИ специальной комиссией под председательством руководителя субъекта КИИ (или уполномоченного им лица), его работников и, при необходимости, приглашенных специалистов ведомств – регуляторов в соответствующей сфере. Решение комиссии оформляется актом и после его утверждения направляется во ФСТЭК России. Форма направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий утверждена приказом ФСТЭК России от 22 декабря 2017 г. № 236.

Категория значимого объекта КИИ может быть изменена по мотивированному решению ФСТЭК России в рамках государственного контроля безопасности значимых объектов КИИ, в случае изменения самого объекта КИИ, а также в связи с реорганизацией субъекта КИИ (в том числе ликвидацией, изменением его организационно-правовой формы и т. д.).

Для объектов КИИ, не являющихся значимыми, в обязательном порядке должна быть обеспечена только интеграция в ГосСОПКА (канал обмена информацией). Остальные мероприятия по обеспечению безопасности объекта КИИ реализуются на усмотрение соответствующего субъекта КИИ.

Для значимых объектов КИИ, помимо интеграции в ГосСОПКА, субъекты КИИ должны:

– создать систему безопасности значимого объекта КИИ;

– реагировать на компьютерные инциденты (порядок реагирования на компьютерные инциденты разрабатывается ФСБ России);

– предоставлять на объект КИИ беспрепятственный доступ регуляторам и выполнять их предписания по результатам проверок. Законом предусматриваются как плановые, так и внеплановые проверки. Правила осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации утверждены Постановлением Правительства Российской Федерации от 17 февраля 2018 г. № 162.

Система безопасности значимого объекта КИИ представляет собой комплекс организационных и технических мер. Порядок создания системы и требования к принимаемым мерам безопасности определяются Требованиями к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденными приказом ФСТЭК России от 21 декабря 2017 г. № 235, и Требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденными приказом ФСТЭК России от 25 декабря 2017 г. № 239. ФСТЭК России отвечает за контроль реализации требований по обеспечению безопасности объектов КИИ.

Для обеспечения безопасности значимых объектов, являющихся информационными системами персональных данных, Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации применяются с учетом Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

Для обеспечения безопасности значимых объектов, являющихся государственными информационными системами, Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации применяются с учетом Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17.

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации должны выполняться на всех стадиях (этапах) жизненного цикла в ходе создания (модернизации), эксплуатации и вывода из эксплуатации значимого объекта.

Вместе с утверждением ФЗ «О безопасности КИИ» в Уголовный кодекс Российской Федерации 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 под состав 293-й статьи УК РФ «Халатность». Дополнительно следует ожидать внесения изменений в законодательство об административных правонарушениях в части определения штрафных санкций для юридических лиц за неисполнение Закона.

СПИСОК ЛИТЕРАТУРЫ

1. Информационная безопасность открытых систем. В 2 т. Т. 2. Средства защиты в сетях / С. В. Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков. – М. : ГЛТ, 2008. – 558 с.

2. Малюк, А. А. Информационная безопасность: концептуальные и методологические основы защиты информации / А. А. Малюк. – М. : ГЛТ, 2004. – 280 с.

3. Федеральный закон 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». – Электрон. дан. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/. – Загл. с экрана.

4. Федеральный закон от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации». – Электрон. дан. – Режим доступа: https://duma.consultant.ru/doc.asp?ID=77786. – Загл. с экрана.

5. Федеральный закон от 10 января 2003 г. № 15-ФЗ «Об участии в международном информационном обмене». – Электрон. дан. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10929/. – Загл. с экрана.

6. Федеральный закон от 4 июля 1996 г. № 85-ФЗ «Об участии в международном информационном обмене». – Электрон. дан. – Режим доступа: http://base.garant.ru/135401/. – Загл. с экрана.

REFERENCES

1. Zapechnikov S.V., Miloslavskaya N.G., Tolstoy A.I., Ushakov D.V. *Informatsionnaya bezopasnost otkrytykh system. V 2 t. T. 2. Sredstva zashchity v setyakh* [Information Security of Open Systems. In 2 vols. Vol. 2. Means of Protection in Networks]. Moscow, GLT Publ., 2008. 558 p.

2. Malyuk A.A. *Informatsionnaya bezopasnost: kontseptualnye i metodologicheskie osnovy zashchity informatsii* [Information Security: Conceptual and Methodological Basis of Information Security]. Moscow, GLT Publ., 2004. 280 p.

3. *Federalnyy zakon ot 27 iyulya 2006 g. № 149-FZ «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii»* [Federal Law of 27 July 2006 No. 149-FZ 'On Information, Information Technologies and Protection of Information']. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/.

4. *Federalnyy zakon ot 20 fevralya 1995 g. № 24-FZ «Ob informatsii, informatizatsii i zashchite informatsii»* [Federal Law of 20 February 1995 No. 24-FZ 'On Information, Informatization and Protection of Information']. URL: https://duma.consultant.ru/doc.asp?ID=77786.

5. *Federalnyy zakon ot 10 yanvarya 2003 g. № 15-FZ «Ob uchastii v mezhdunarodnom informatsionnom obmene»* [Federal Law of 10 January 2003 No. 15-FZ 'On Participation in International Information Exchange']. URL: http://www.consultant.ru/document/cons_doc_LAW_10929/.

6. *Federalnyy zakon ot 4 iyulya 1996 g. № 85-FZ «Ob uchastii v mezhdunarodnom informatsionnom obmene»* [Federal Law of 4 July 1996 No. 85-FZ 'On Participation in International Information Exchange']. URL: http://base.garant.ru/135401/.

THE BASIC PRINCIPLES OF INFORMATION PROTECTION IN THE RUSSIAN FEDERATION IN THE TRANSITION TO A DIGITAL ECONOMY

Rashit M. Romanov

Deputy Head of the Federal Service for Technical and Export Control of the Southern and North Caucasus Federal Districts
uzhfo@fstec.ru
Raboche-Krestyanskaya St., 1, 400074 Volgograd, Russian Federation

Abstract. The modern stage of development of society is characterized by the increasing role of the information sphere. The information sphere is a set of information, information infrastructure, entities engaged in the collection, formation, distribution and use of information, as well as a system of regulation of public relations arising in this process.

The expansion of the areas of application of information technologies, as a factor of economic development and improvement of the functioning of public and state institutions, at the same time generates new information threats.

The situation is significantly complicated by the confrontation between the Russian Federation and the West, which directly affects the sphere of national interests of the Russian Federation and poses a direct threat to the national security of the country, the key element of which is information security

There is a constant growth of computer attacks on Russian information resources, the number of attacks has increased significantly in recent years. At the same time, the methods, means and tactics of such attacks are being improved, and their intensity directly depends on the current international situation.

Terrorist and extremist materials are openly distributed in the global network. The number of crimes committed with the use of information technologies, for example, illegal penetrations into the corporate networks of state and credit and financial institutions, has increased.

The article analyzes the requirements for the security of important objects of critical information infrastructure of the Russian Federation. It is shown that they should be performed at all stages of the life cycle during the creation (modernization), operation and decommissioning of a significant object.

Key words: information security, information infrastructure, information technology, state security, digital economy.