СБОРНИК **НАУЧНЫХ ТРУДОВ НГТУ. – 2019. – № 1 (94).** – 123–131

СООБЩЕНИЯ

УДК 004.01 DOI: 10.17212/2307-6879-2019-1-123-131

РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ЗНАЧИМОГО ОБЪЕКТА КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ*

Л.Д. ЗАВОРИНА[1], В.В. СЕЛИФАНОВ[2]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, студент кафедры защиты информации. E-mail: ljubasik-1234@mail.ru*

[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель кафедры защиты информации. E-mail: sfo1@mail.ru.*

Еще два года назад к безопасности критически важных объектов относили только защиту промышленных объектов, однако сейчас ситуация изменилась. С 1 января 2018 года вступил в силу ФЗ № 187 от 26.07.2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации», где было обозначено понятие критической информационной инфраструктуры, для которой важна разработка системы защиты информации.В нашем регионе вопрос защиты КИИ стоит крайне остро, поскольку в Сибирском федеральном округе сосредоточено значительное количество ведущих предприятий и организаций, попадающих под действие закона. Можно выделить основные цели защиты системы безопасности значимого объекта критической информационной инфраструктуры: предотвращение неправомерного доступа к информации, недопущение воздействия на технические средства обработки информации, восстановление функционирования значимых объектов КИИ, непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Перед созданием системы безопасности предприятию необходимо грамотно составить перечень объектов КИИ и провести их категорирование. Для создания системы защиты необходимо обследовать ИТ-инфраструктуру, сформировать перечень организационных и технических мероприятий. На первом этапе руководителю организации нужно разработать и утвердить приказ о создании системы безопасности значимых объектов КИИ. На втором этапе возникает потребность в разработке технического задания. Третий этап подразумевает формирование организационных и технических мер по обеспечению безопасности значимого объекта КИИ: модели угроз, документация технического проекта, комплект эксплуатационной документации. В завершение лицензиатом ФСТЭК проводится аттестация значимого объекта КИИ (обязательное условие для государственных информационных систем).

* Статья получена 30 октября 2018 г.

Ключевые слова: критическая информационная инфраструктура (КИИ), объект КИИ, Федеральная служба по техническому и экспортному контролю России (ФСТЭК), государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГОССОПКА), система безопасности значимого объекта КИИ (СБЗОКИИ), информационная безопасность

ВВЕДЕНИЕ

Еще в 2017 году к безопасности критически важных объектов относили только защиту промышленных объектов, требования к их обеспечению защиты изложены в Приказе № 31 ФСТЭК России. С 2018 года ситуация изменилась на государственном уровне. Пришли к выводу, что если, например, кибератака притормозит работу крупного банка, то ущерб будет значительным для многих людей. С 1 января 2018 года вступил в силу Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической инфраструктуры Российской Федерации», закрепляющий понятие критической информационной инфраструктуры, которой важна разработка системы защиты информации.

РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ

Система защиты значимого объекта КИИ разрабатывается для субъектов, работающих в сфере ракетно-космической, атомной, металлургической, горно-добывающей, химической и оборонной промышленности, науки, здравоохранения, транспорта, энергетики, связи, топливно-энергетического комплекса, финансовой и банковской [1].

Прежде чем приступить с созданию системы безопасности значимого объекта КИИ, субъектам необходимо сформировать перечень объектов КИИ и провести их категорирование. И уже на этом этапе у предприятий возникают трудности. На данный момент уже более 1100 организаций, которые точно будут попадать под действие 187-ФЗ, отправили информацию об объектах КИИ во ФСТЭК и продолжают это делать с возрастающей интенсивностью. В конце февраля 2019 года заместитель начальника Управления ФСТЭК России Е.Б. Торбенко уточнила, что ФСТЭК уже известно об 29 000 объектов КИИ. На данный момент их скорее всего уже 30 000, из них категорировано уже более 1400 объектов, а информация о результатах категорирования 600 объектов была возвращена владельцам. Следовательно, зачастую субъекты отправляют во ФСТЭК неполную информацию, пропуская важные моменты, и присылают ненужную информацию, серьезно загружая регулятор.

В нашем регионе вопрос защиты КИИ стоит крайне остро, поскольку в Сибирском федеральном округе сосредоточено значительное количество ведущих предприятий и организаций, попадающих под действие закона № 187-ФЗ.

12 декабря 2018 года в Новосибирске прошла конференция «Будни информационной безопасности», посвященная значимым проблемам российской отрасли информационной безопасности и ключевым направлениям ее развития. Организатором мероприятия выступал ведущий российский разработчик и производитель высокотехнологичных программных и программно-аппаратных средств зашиты информации – компания ИнфорТеКС. Специалисты по ИБ получили ответы на интересующие вопросы, относящиеся к требованиям, подходам к защите, подключению к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации(ГОССОПКА). Такого рода конференции прошли во многих областных центрах страны. Следовательно, существует проблема в создании системы защиты значимого объекта КИИ, и мы подробно разберем, какие меры необходимо предпринять в соответствии с новыми требованиями.

В соответствии с Приказом ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований в созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования» можно выделить следующие цели защиты системы:

– предотвращение неправомерного доступа к информации, обрабатываемой значимыми объектами КИИ (т. е. не всеми), 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 КИИ (наличие СКУД и видеонаблюдения обязательно);

– восстановление функционирования значимых объектов КИИ, 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 в соответствии со ст. 5 187-ФЗ (ГОССОПКА) [3].

На первом этапе руководителю организации необходимо разработать и утвердить приказ о создании системы безопасности значимых объектов КИИ. Должны быть описаны цели и сроки создания СБЗОКИИ, субъекты, ответственные за безопасность и их полномочия по обеспечению безопасности КИИ, ответственные за создание лица и лицо, осуществляющее за этим контроль [1, 3].

На втором этапе возникает потребность в установлении требований к обеспечению безопасности значимых объектов КИИ, т. е. в разработке технического задания на создание СБЗОКИИ. Подразделение ИБ организации, лицензиат ФСТЭК России должны выполнить следующие задачи:

– на основании установленной категории значимости установить базовый набор мер по обеспечению безопасности значимого объекта;

– адаптировать вышеупомянутый набор мер в соответствии с угрозами безопасности информации, которые могут быть применены информационными технологиями и особенностями функционирования значимого объекта;

– разработать меры компенсации, которые будут обеспечивать нейтрализацию угроз безопасности информации с надлежащим уровнем защищенности значимого объекта [2].

На выходе разрабатывается техническое задание на создание СБЗОКИИ, в котором должны быть описаны:

– цели и задачи обеспечения безопасности значимого объекта или СБЗОКИИ;

– категория значимости значимого объекта;

– перечень нормативно-правовых актов и иных документов и стандартов, соответствующих значимому объекту;

– перечень типов объектов защиты значимого объекта;

– технические и организационные меры, применяемые для безопасности значимого объекта;

– этапы работ создания системы безопасности значимого объекта;

– требования к используемым программным и программно-аппаратным средствам, в том числе средствам защиты информации;

– требования к защите средств и систем, которые обеспечивают функционирование значимого объекта;

– требования к информационному взаимодействию значимого объекта с иными объектами КИИ (в том числе ИС, АСУ, ИТС) [Там же].

Третий этап подразумевает разработку организационных и технических мер по обеспечению безопасности значимого объекта КИИ, в результате которого составляются модель угроз безопасности информации значимого объекта КИИ, документация технического проекта, комплект эксплуатационной документации [2, 3].

В процессе анализа угроз безопасности и разработки модели угроз безопасности информации подразделение ИБ организации должно выполнить следующие задачи:

– выявить источники угроз и оценить потенциал внешних и внутренних нарушителей;

– сделать анализ уязвимостей значимого объекта и его программно-аппаратных средств;

– определить возможные сценарии реализации угроз;

– оценить вероятные последствия от возникновения угроз.

Модель угроз должна содержать следующую информацию о значимом объекте:

– описание архитектуры;

– характеристика источников угроз безопасности, модель нарушителя;

– описание всех актуальных угроз (с указанием источников, уязвимостей, способов реализации и возможных последствий) [2, 3].

Затем подразделению ИБ необходимо разработать документацию технического проекта, включающую следующее:

– ведомость;

– пояснительную записку;

– схему структуры комплекса технических средств с описанием комплекса;

– описание программного обеспечения;

– схему функциональной структуры;

– схему и описание организационной структуры;

– план расположения;

– сметы на создание системы [Там же].

Состав и содержание документации технического проекта определяются в соответствии с ГОСТ 34.201, РД 50-34.698-90.

Затем разрабатывается эксплуатационная документация на значимый объект, которая включает:

– описание архитектуры системы безопасности;

– описание параметров и порядка настройки средств защиты, программно-аппаратных средств;

– правила безопасной эксплуатации [2].

На четвертом этапе подразделение ИБ выполняет внедрение организационных и технических мер по обеспечению безопасности значимого объекта КИИ и ввод СБЗОКИИ в действие.

Первым делом программные и технические средства для СБЗОКИИ закупают, устанавливают на объекты и настраивают. Составляются товарные накладные, акты передачи прав на ПО, акты установки-настройки средств защиты.

Далее разрабатываются организационно-распорядительные документы о правилах и процедурах обеспечения безопасности значимого объекта КИИ.

Комплект документов включает:

– политику идентификации и аутентификации;
– политику управления доступом;
– матрицу доступа;
– политику ограничения программной среды;
– политику защиты машинных носителей и журнал учета;
– политику аудита безопасности;
– политику антивирусной защиты;
– политику компьютерных атак;
– политику обеспечения целостности;
– политику обеспечения доступности;
– политику защиты технических средств и систем;
– план контролируемой зоны;
– политику защиты информационной системы и ее компонентов;
– политику реагирования на компьютерные инциденты;
– политику управления конфигурацией информационной системы;
– технический паспорт ОКИИ;
– перечень разрешенного к использованию программного обеспечения;
– политику управления обновлениями программного обеспечения;
– политику планирования мероприятий по обеспечению защиты информации;
– план мероприятий по обеспечению безопасности значимых объектов;
– политику обеспечения действий в нештатных ситуациях;
– политику информирования и обучения персонала [2, 3].

Затем подразделение ИБ внедряет организационные и технические меры по обеспечению безопасности значимого объекта КИИ в организации, составляет приказ.

На этапе предварительных испытаний значимого объекта КИИ и его системы безопасности разрабатываются программа и методика, приказ о проведении, протокол проведения и акт приемки СБЗОКИИ в опытную эксплуатацию [2].

Далее подразделение ИБ предприятия проверяет функционирование системы безопасности, знания и умения пользователей и администраторов, которые необходимы для эксплуатации значимого объекта и его системы безопасности. В результате проверок составляются программа, методика и журнал опытной эксплуатации.

На основе оформленного анализа уязвимостей значимого объекта подразделение ИБ создает протокол, в котором должно быть подтверждение того,

что в значимом объекте отсутствуют, по крайней мере, уязвимости, содержащиеся в банке данных угроз безопасности информации ФСТЭК России.

Затем проводятся приемочные испытания значимого объекта КИИ и его системы безопасности, разрабатываются программа и методика, приказ о проведении испытаний, протокол проведения и акт приемки СБЗОКИИ в эксплуатацию [2].

Завершающий этап – аттестация значимого объекта КИИ, которую проводит лицензиат ФСТЭК России с аттестатом аккредитации, только в том случае, если значимый объект является государственной информационной системой и обрабатывает информацию, содержащую государственную тайну. На основании разработанной им программы и методики проводятся комплексные испытания значимого объекта КИИ в реальных условиях.

По усмотрению руководителя организации оценка соответствия объекта КИИ требованиям по ЗИ проводится в форме аттестации [Там же].

ЗАКЛЮЧЕНИЕ

Защита важной для жизнедеятельности людей и безопасности страны информационной инфраструктуры больше не является личным делом ее владельцев. У субъектов КИИ должны быть подготовлены и переданы во ФСТЭК перечни объектов и их категорирование, а практика показывает, что далеко не все предприятия успели это сделать. Для приведения системы защиты необходимо провести обследование ИТ-инфраструктуры, сформировать перечень организационных и технических мероприятий. Время пока еще есть, но специалистам по ИБ стоит поспешить.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.

2. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

3. Приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования».

4. Анализ требований законодательства по защите критической информационной инфраструктуры [Электронный ресурс]. – URL: https://www.security-code.ru/company/events/analiz-trebovaniy-zakonodatelstva-po-zashchite-kriticheskoy-informatsionnoy-infrastruktury-kii/ (дата обращения: 07.06.2019).

Заворина Любовь Денисовна, студентка кафедры защиты информации Новосибирского государственного технического университета. E-mail: ljubasik-1234@mail.ru

Селифанов Валентин Валерьевич, старший преподаватель кафедры защиты информации. E-mail: sfo1@mail.ru

DOI: 10.17212/2307-6879-2019-1-123-131

Development of the system of protection of information of a significant object of critical infrastructure of the Russian Federation*

L.D. Zavorina[1], V.V. Selifanov[2]

[1] *Novosibirsk State Technical University, 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation, student of the information security department, AB-528 group. E-mail: ljubasik-1234@mail.ru*

[2] *Novosibirsk State Technical University, 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation, Senior lecturer, department of information protection. E-mail: sfo1@mail.ru*

Two years ago, the safety of critical facilities was attributed only to the protection of industrial facilities, but now the situation has changed. From 1 January 2018, Federal law No. 187 of 26.07.2017 "On the safety of the critical information infrastructure of the Russian Federation" came into force, which established the concept of critical information infrastructure, which is important for the development of the information protection system. In our region, the issue of CII protection is extremely acute, as a significant number of leading enterprises and organizations falling under the law are concentrated in the Siberian Federal district. It is possible to identify the main objectives of the security system protection of a significant object of critical information infrastructure: prevention of unauthorized access to information, failure to influence the technical means of information processing, restoration of the functioning of significant objects of CII, continuous interaction with the state system of detection, prevention and elimination of the consequences of computer attacks on information resources of the Russian Federation. Before creating a security system, an enterprise should correctly compile a list of KII facilities and categorize them. To create a security system, it is necessary to examine the IT infrastructure, create a list of organizational and technical measures. At the first stage, the head of the organization needs to develop and approve an order to create a security system for significant facilities of the KII. At the second stage there is a need for the development of technical specifications. The third stage involves the formation of organizational and technical measures to ensure the safety of a significant CII facility: threat models, technical project documentation, a set of operational documentation. At the end, the licensee of the FSTEC conducts certification of a significant object of the CII (a prerequisite for state-impact information systems).

Keywords: critical information infrastructure (CII), object CUES, the Federal service for technical and export control of Russia (FSTEC), the state system of detection, prevention and elimination of consequences of computer attacks (GOSSIPY), security system significant object CUES (SBTCI), information security

* *Received 30 October 2018.*

REFERENCES

1. Federal law "On security of critical information infrastructure of the Russian Federation" dated 26.07.2017 N 187-FZ. (In Russian).

2. Order of FSTEC of Russia of December 25, 2017 N 239 "About the approval of requirements for safety of significant objects of critical information infrastructure of the Russian Federation». (In Russian).

3. Order of FSTEC of Russia of December 21, 2017 N 235 "About the approval of Requirements to creation of security systems of significant objects of KII of the Russian Federation and ensuring their functioning». (In Russian).

4. *Analiz trebovanii zakonodatel'stva po zashchite kriticheskoi informatsionnoi infrastruktury* [Analysis of the requirements of legislation for the protection of critical infrastructure]. Available at: https://www.securitycode.ru/company/events/analiz-trebovaniy-zakonodatelstva-po-zashchite-kriticheskoy-informatsionnoy-infrastruktury-kii/ (accessed 07.06.2019).

Для цитирования:

Заворина Л.Д., Селифанов В.В. Разработка системы защиты информации значимого объекта критической инфраструктуры Российской Федерации // Сборник научных трудов НГТУ. – 2019. – № 1 (94). – С. 123–131. – DOI: 10.17212/2307-6879-2019-1-123-131.

For citation:

Zavorina L.D., Selifanov V.V. Razrabotka sistemy zashchity informatsii znachimogo ob"ekta kriticheskoi infrastruktury Rossiiskoi Federatsii [Development of the system of protection of information of a significant object of critical infrastructure of the Russian Federation]. *Sbornik nauchnykh trudov Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta – Transaction of scientific papers of the Novosibirsk state technical university*, 2019, no. 1 (94), pp. 123–131. DOI: 10.17212/2307-6879-2019-1-123-131.