ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

25 декабря 2017 г. Москва № 239

Об утверждении Требований
по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации
(в ред. приказов ФСТЭК России от 9 августа 2018 г. № 138, от 26 марта 2019 г. № 60, от 20 февраля 2020 г. № 35)

В соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) **П Р И К А З Ы В А Ю**:

Утвердить прилагаемые Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

УТВЕРЖДЕНЫ
приказом ФСТЭК России
от 25 декабря 2017 г. № 239

Требования
по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

I. Общие положения

1. Настоящие Требования разработаны в соответствии с Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и направлены на обеспечение устойчивого функционирования значимых объектов критической информационной инфраструктуры Российской Федерации (далее – значимые объекты, критическая информационная инфраструктура) при проведении в отношении них компьютерных атак.

2. Действие настоящих Требований распространяется на информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети, которые отнесены к значимым объектам критической информационной инфраструктуры в соответствии со статьей 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

3. По решению субъекта критической информационной инфраструктуры настоящие Требования могут применяться для обеспечения безопасности объектов критической информационной инфраструктуры, не отнесенных к значимым объектам.

4. Обеспечение безопасности значимых объектов, в которых обрабатывается информация, составляющая государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

5. Для обеспечения безопасности значимых объектов, являющихся информационными системами персональных данных, настоящие Требования 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 (Собрание законодательства Российской Федерации, 2012, № 45, ст. 6257).

Для обеспечения безопасности значимых объектов, являющихся государственными информационными системами, настоящие Требования

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 (зарегистрирован Минюстом России 31 мая 2013 г., регистрационный № 28608) (с изменениями, внесенными приказом ФСТЭК России от 15 февраля 2017 г. № 27 «О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17» (зарегистрирован Минюстом России 14 марта 2017 г., регистрационный № 45933).

6. Безопасность значимых объектов обеспечивается субъектами критической информационной инфраструктуры в рамках функционирования систем безопасности значимых объектов, создаваемых субъектами критической информационной инфраструктуры в соответствии со статьей 10 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

II. Требования к обеспечению безопасности в ходе создания, эксплуатации и вывода из эксплуатации значимых объектов

7. Обеспечение безопасности значимых объектов является составной частью работ по созданию (модернизации, при которой изменяется архитектура значимого объекта, в том числе подсистема его безопасности, в соответствии с отдельным техническим заданием на модернизацию значимого объекта и (или) техническим заданием (частным техническим заданием) на модернизацию подсистемы безопасности значимого объекта (далее - модернизация), эксплуатации и вывода из эксплуатации значимых объектов. Меры по обеспечению безопасности значимых объектов принимаются на всех стадиях (этапах) их жизненного цикла.

8. На стадиях (этапах) жизненного цикла в ходе создания (модернизации), эксплуатации и вывода из эксплуатации значимого объекта проводятся:

а) установление требований к обеспечению безопасности значимого объекта;

б) разработка организационных и технических мер по обеспечению безопасности значимого объекта;

в) внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие;

г) обеспечение безопасности значимого объекта в ходе его эксплуатации;

д) обеспечение безопасности значимого объекта при выводе его из эксплуатации.

Результаты реализации мероприятий, проводимых для обеспечения

безопасности значимого объекта на стадиях (этапах) его жизненного цикла, подлежат документированию. Состав и формы документов определяются субъектом критической информационной инфраструктуры.

9. Для значимых объектов, находящихся в эксплуатации, настоящие Требования подлежат реализации в рамках модернизации или дооснащения подсистем безопасности эксплуатируемых значимых объектов. Модернизация или дооснащение подсистем безопасности значимых объектов осуществляется в порядке, установленном настоящими Требованиями для создания значимых объектов и их подсистем безопасности, с учетом имеющихся у субъектов критической информационной инфраструктуры программ (планов) по модернизации или дооснащению значимых объектов.

Установление требований к обеспечению безопасности значимого объекта

10. Задание требований к обеспечению безопасности значимого объекта осуществляется субъектом критической информационной инфраструктуры и (или) лицом, устанавливающим требования к обеспечению безопасности значимых объектов, в соответствии с категорией значимости значимого объекта, определенной в порядке, установленном Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 8 февраля 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» (Собрание законодательства Российской Федерации, 2018, № 8, ст. 1204).

Требования к обеспечению безопасности включаются в техническое задание на создание значимого объекта и (или) техническое задание (частное техническое задание) на создание подсистемы безопасности значимого объекта, которые должны содержать:

а) цель и задачи обеспечения безопасности значимого объекта или подсистемы безопасности значимого объекта;

б) категорию значимости значимого объекта;

в) перечень нормативных правовых актов, методических документов и национальных стандартов, которым должен соответствовать значимый объект;

г) перечень типов объектов защиты значимого объекта;

д) требования к организационным и техническим мерам, применяемым для обеспечения безопасности значимого объекта;

е) стадии (этапы работ) создания подсистемы безопасности значимого объекта;

ж) требования к применяемым программным и программно-аппаратным средствам, в том числе средствам защиты информации;

з) требования к защите средств и систем, обеспечивающих функционирование значимого объекта (обеспечивающей инфраструктуре);

и) требования к информационному взаимодействию значимого объекта с иными объектами критической информационной инфраструктуры, а также иными информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями,

к) требования к составу и содержанию документации, разрабатываемой в ходе создания значимого объекта.

В случае если значимый объект создается в рамках объекта капитального строительства, требования к обеспечению безопасности значимого объекта задаются застройщиком и оформляются в виде приложения к заданию на проектирование (реконструкцию) объекта капитального строительства.

При определении требований к обеспечению безопасности значимого объекта учитываются положения организационно-распорядительных документов по обеспечению безопасности значимых объектов, разрабатываемых субъектами критической информационной инфраструктуры в соответствии с требованиями к созданию систем безопасности значимых объектов и обеспечению их функционирования, утвержденными в соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – организационно-распорядительные документы по безопасности значимых объектов).

Разработка организационных и технических мер по обеспечению безопасности значимого объекта

11. Разработка организационных и технических мер по обеспечению безопасности значимого объекта осуществляется субъектом критической информационной инфраструктуры и (или) лицом, привлекаемым в соответствии с законодательством Российской Федерации к проведению работ по созданию (модернизации) значимого объекта и (или) обеспечению его безопасности, в соответствии с техническим заданием на создание значимого объекта и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимого объекта и должна включать:

а) анализ угроз безопасности информации и разработку модели угроз безопасности информации или ее уточнение (при ее наличии);

б) проектирование подсистемы безопасности значимого объекта;

в) разработку рабочей (эксплуатационной) документации на значимый объект (в части обеспечения его безопасности).

Разрабатываемые организационные и технические меры по обеспечению безопасности значимого объекта не должны оказывать негативного влияния на создание и функционирование значимого объекта.

При разработке организационных и технических мер по обеспечению безопасности значимого объекта учитывается его информационное взаимодействие с иными объектами критической информационной инфраструктуры, информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями.

11.1. Целью анализа угроз безопасности информации является определение возможных способов реализации (возникновения) угроз безопасности информации и последствий их реализации (возникновения) с учетом состава пользователей и их полномочий, программных и программно-аппаратных средств, взаимосвязей компонентов значимого объекта, взаимодействия с иными объектами критической информационной инфраструктуры, информационными системами, автоматизированными системами управления, информационно-телекоммуникационными сетями (далее – архитектура значимого объекта), а также особенностей функционирования значимого объекта.

Анализ угроз безопасности информации должен включать:

а) выявление источников угроз безопасности информации и оценку возможностей (потенциала) внешних и внутренних нарушителей;

б) анализ возможных уязвимостей значимого объекта и его программных, программно-аппаратных средств;

в) определение возможных способов (сценариев) реализации (возникновения) угроз безопасности информации;

г) оценку возможных последствий от реализации (возникновения) угроз безопасности информации.

В качестве исходных данных для анализа угроз безопасности информации используется банк данных угроз безопасности информации, ведение которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2006, № 49, ст. 5192; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818; 2013, № 26, ст. 3314; № 53, ст. 7137; 2014, № 36, ст. 4833; № 44, ст. 6041; 2015, № 4, ст. 641; 2016, № 1, ст. 211; 2017, № 48, ст. 7198) (далее – банк данных угроз безопасности информации ФСТЭК России), а также источники, содержащие иные сведения об уязвимостях и угрозах безопасности информации.

По результатам анализа угроз безопасности информации могут быть разработаны рекомендации по корректировке архитектуры значимого объекта и

организационно-распорядительных документов по безопасности значимых объектов, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Модель угроз безопасности информации должна содержать краткое описание архитектуры значимого объекта, характеристику источников угроз безопасности информации, в том числе модель нарушителя, и описание всех угроз безопасности информации, актуальных для значимого объекта.

Описание каждой угрозы безопасности информации должно включать:

а) источник угрозы безопасности информации;

б) уязвимости (ошибки), которые могут быть использованы для реализации (способствовать возникновению) угрозы безопасности информации;

в) возможные способы (сценарии) реализации угрозы безопасности информации;

г) возможные последствия от реализации (возникновения) угрозы безопасности информации.

Модель угроз безопасности информации может разрабатываться для нескольких значимых объектов, имеющих одинаковые цели создания и архитектуру, а также типовые угрозы безопасности информации.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации должны применяться методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

11.2. Проектирование подсистемы безопасности значимого объекта должно осуществляться в соответствии с техническим заданием на создание значимого объекта и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимого объекта с учетом модели угроз безопасности информации и категории значимости значимого объекта.

При проектировании подсистемы безопасности значимого объекта:

а) определяются субъекты доступа (пользователи, процессы и иные субъекты доступа) и объекты доступа;

б) определяются политики управления доступом (дискреционная, мандатная, ролевая, комбинированная);

в) определяются и обосновываются организационные и технические меры, подлежащие реализации в рамках подсистемы безопасности значимого объекта;

г) определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер по обеспечению безопасности значимого объекта;

д) осуществляется выбор средств защиты информации и (или) их разработка с учетом категории значимости значимого объекта, совместимости с программными и программно-аппаратными средствами, выполняемых функций безопасности и ограничений на эксплуатацию;

е) разрабатывается архитектура подсистемы безопасности значимого объекта, включающая состав, места установки, взаимосвязи средств защиты информации;

ж) определяются требования к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, блокирование (нейтрализацию) угроз безопасности информации и устранение уязвимостей значимого объекта;

з) определяются меры по обеспечению безопасности при взаимодействии значимого объекта с иными объектами критической информационной инфраструктуры, информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями.

В случае если в ходе проектирования подсистемы безопасности значимого объекта предусмотрена разработка программного обеспечения, в том числе программного обеспечения средств защиты информации, такая разработка проводится в соответствии со стандартами безопасной разработки программного обеспечения.

Результаты проектирования подсистемы безопасности значимого объекта отражаются в проектной документации на значимый объект (подсистему безопасности значимого объекта), разрабатываемой в соответствии с техническим заданием на создание значимого объекта и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимого объекта.

В процессе проектирования значимого объекта его категория значимости может быть уточнена.

В целях тестирования подсистемы безопасности значимого объекта в ходе проектирования может осуществляться ее макетирование или создание тестовой среды. Тестирование должно быть направлено на:

обеспечение работоспособности и совместимости выбранных средств защиты информации с программными и аппаратными средствами значимого объекта;

практическую отработку выполнения средствами защиты информации функций безопасности, а также выполнения требований по безопасности, предъявляемых к программным и программно-аппаратным средствам, в том числе средствам защиты информации, в соответствии с пунктами 27-31 настоящих Требований;

исключение влияния подсистемы безопасности на функционирование значимого объекта.

Макетирование подсистемы безопасности значимого объекта и ее тестирование может проводиться с использованием средств и методов моделирования, а также с использованием технологий виртуализации.

При проектировании подсистем безопасности значимых объектов, являющихся информационно-телекоммуникационными сетями, настоящие Требования применяются с учетом Требований к проектированию сетей электросвязи, утвержденных приказом Минкомсвязи России от 9 марта 2017 г. № 101 (зарегистрирован Минюстом России 31 мая 2017 г., регистрационный № 46915), а также иных нормативных правовых актов федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в области связи.

11.3. Разработка рабочей (эксплуатационной) документации на значимый объект осуществляется в соответствии с техническим заданием на создание значимого объекта и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимого объекта на основе проектной документации.

Рабочая (эксплуатационная) документация на значимый объект должна содержать:

описание архитектуры подсистемы безопасности значимого объекта;

порядок и параметры настройки программных и программно-аппаратных средств, в том числе средств защиты информации;

правила эксплуатации программных и программно-аппаратных средств, в том числе средств защиты информации (правила безопасной эксплуатации).

Состав и формы рабочей (эксплуатационной) документации определяются в соответствии с техническим заданием на создание значимого объекта и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимого объекта.

Внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие

12. Внедрение организационных и технических мер по обеспечению безопасности значимого объекта организуется субъектом критической информационной инфраструктуры в соответствии с проектной и рабочей (эксплуатационной) документацией на значимый объект, стандартами организаций и включает:

а) установку и настройку средств защиты информации, настройку программных и программно-аппаратных средств;

б) разработку организационно-распорядительных документов, регламентирующих правила и процедуры обеспечения безопасности значимого объекта;

в) внедрение организационных мер по обеспечению безопасности значимого объекта;

г) предварительные испытания значимого объекта и его подсистемы безопасности;

д) опытную эксплуатацию значимого объекта и его подсистемы безопасности;

е) анализ уязвимостей значимого объекта и принятие мер по их устранению;

ж) приемочные испытания значимого объекта и его подсистемы безопасности.

По решению субъекта критической информационной инфраструктуры к разработке и внедрению организационных и технических мер по обеспечению безопасности значимого объекта может привлекаться лицо, эксплуатирующее (планирующее эксплуатировать) значимый объект.

12.1. Установка и настройка средств защиты информации должна проводиться в соответствии с проектной и рабочей (эксплуатационной) документацией на значимый объект, а также в соответствии с эксплуатационной документацией на отдельные средства защиты информации.

При установке и настройке средств защиты информации должно быть обеспечено выполнение ограничений на эксплуатацию этих средств защиты информации, в случае их наличия в эксплуатационной документации.

12.2. Разрабатываемые организационно-распорядительные документы по безопасности значимого объекта должны определять правила и процедуры реализации отдельных организационных и (или) технических мер (политик безопасности), разработанных и внедренных в рамках подсистемы безопасности значимого объекта в соответствии с главой III настоящих Требований.

Организационно-распорядительные документы по безопасности значимого объекта должны в том числе устанавливать правила безопасной работы работников, эксплуатирующих значимые объекты, и работников, обеспечивающих функционирование значимых объектов, а также действия работников при возникновении нештатных ситуаций, в том числе вызванных компьютерными инцидентами.

Состав и формы организационно-распорядительных документов по безопасности значимых объектов определяются субъектом критической информационной инфраструктуры с учетом особенностей его деятельности.

12.3. При внедрении организационных мер по обеспечению безопасности значимого объекта осуществляются:

а) организация контроля физического доступа к программно-аппаратным средствам значимого объекта и его линиям связи;

б) реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации программных и программно-аппаратных средств;

в) проверка полноты и детальности описания в организационно-распорядительных документах по безопасности значимых объектов действий пользователей и администраторов значимого объекта по реализации организационных мер;

г) определение администратора безопасности значимого объекта;

д) отработка действий пользователей и администраторов значимого объекта по реализации мер по обеспечению безопасности значимого объекта.

12.4. Предварительные испытания значимого объекта и его подсистемы безопасности должны проводиться в соответствии с программой и методиками предварительных испытаний и включать проверку работоспособности подсистемы безопасности значимого объекта и отдельных средств защиты информации, оценку выполнения требований по безопасности, предъявляемых к программным и программно-аппаратным средствам, в том числе средствам защиты информации, в соответствии с пунктами 27-31 настоящих Требований, оценку влияния подсистемы безопасности на функционирование значимого объекта при проектных режимах его работы, установленных проектной документацией, а также принятие решения о возможности опытной эксплуатации значимого объекта и его подсистемы безопасности.

12.5. Опытная эксплуатация значимого объекта и его подсистемы безопасности должна проводиться в соответствии с программой и методиками опытной эксплуатации и включать проверку функционирования подсистемы безопасности значимого объекта, в том числе реализованных организационных и технических мер, а также знаний и умений пользователей и администраторов, необходимых для эксплуатации значимого объекта и его подсистемы безопасности. По результатам опытной эксплуатации принимается решение о возможности (или невозможности) проведения приемочных испытаний значимого объекта и его подсистемы безопасности.

12.6. Анализ уязвимостей значимого объекта проводится в целях выявления недостатков (слабостей) в подсистеме безопасности значимого объекта и оценки возможности их использования для реализации угроз безопасности информации. При этом анализу подлежат уязвимости кода, конфигурации и архитектуры значимого объекта.

Анализ уязвимостей проводится для всех программных и программно-аппаратных средств, в том числе средств защиты информации, значимого объекта.

При проведении анализа уязвимостей применяются следующие способы их выявления:

а) анализ проектной, рабочей (эксплуатационной) документации и организационно-распорядительных документов по безопасности значимого объекта;

б) анализ настроек программных и программно-аппаратных средств, в том числе средств защиты информации, значимого объекта;

в) выявление известных уязвимостей программных и программно-аппаратных средств, в том числе средств защиты информации, посредством анализа состава установленного программного обеспечения и обновлений безопасности с применением средств контроля (анализа) защищенности и (или) иных средств защиты информации;

г) выявление известных уязвимостей программных и программно-аппаратных средств, в том числе средств защиты информации, сетевых служб, доступных для сетевого взаимодействия, с применением средств контроля (анализа) защищенности;

д) тестирование на проникновение в условиях, соответствующих возможностям нарушителей, определенных в модели угроз безопасности информации.

Применение способов и средств выявления уязвимостей осуществляется субъектом критической информационной инфраструктуры с учетом особенностей функционирования значимого объекта.

Допускается проведение анализа уязвимостей на макете (в тестовой зоне) значимого объекта или макетах отдельных сегментов значимого объекта.

Анализ уязвимостей значимого объекта проводится до ввода его в эксплуатацию на этапах, определяемых субъектом критической информационной инфраструктуры.

В случае выявления уязвимостей значимого объекта, которые могут быть использованы для реализации (способствовать возникновению) угроз безопасности информации, принимаются меры, направленные на их устранение или исключающие возможность использования (эксплуатации) нарушителем выявленных уязвимостей.

По результатам анализа уязвимостей должно быть подтверждено, что в значимом объекте, отсутствуют уязвимости, как минимум содержащиеся в банке данных угроз безопасности информации ФСТЭК России, указанном в пункте 11.1 настоящих Требований, или выявленные уязвимости не приводят к возникновению угроз безопасности информации в отношении значимого объекта.

12.7. В ходе приемочных испытаний значимого объекта и его подсистемы безопасности должен быть проведен комплекс организационных и технических мероприятий (испытаний), в результате которых подтверждается соответствие значимого объекта и его подсистемы безопасности настоящим Требованиям, а также требованиям технического задания на создание значимого объекта и

(или) технического задания (частного технического задания) на создание подсистемы безопасности значимого объекта.

В качестве исходных данных при приемочных испытаниях используются модель угроз безопасности информации, результаты (акт) категорирования, техническое задание на создание (модернизацию) значимого объекта и (или) техническое задание (частное техническое задание) на создание подсистемы безопасности значимого объекта, проектная и рабочая (эксплуатационная) документация на значимый объект, организационно-распорядительные документы по безопасности значимых объектов, результаты анализа уязвимостей значимого объекта, материалы предварительных испытаний и опытной эксплуатации, а также иные документы, разрабатываемые в соответствии с настоящими Требованиями и требованиями стандартов организации.

Приемочные испытания значимого объекта и его подсистемы безопасности проводятся в соответствии с программой и методикой приемочных испытаний. Результаты приемочных испытаний значимого объекта и его подсистемы безопасности с выводом о ее соответствии установленным требованиям включаются в акт приемки значимого объекта в эксплуатацию.

В случае если значимый объект является государственной информационной системой, в иных случаях, установленных законодательством Российской Федерации, а также в случае принятия решения субъектом критической информационной инфраструктуры, оценка значимого объекта и его подсистемы безопасности проводится в форме аттестации значимого объекта 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.

Ввод в эксплуатацию значимого объекта и его подсистемы безопасности осуществляется при положительном заключении (выводе) в акте приемки (или в аттестате соответствия) о соответствии значимого объекта установленным требованиям по обеспечению безопасности.

Обеспечение безопасности значимого объекта в ходе его эксплуатации

13. Обеспечение безопасности в ходе эксплуатации значимого объекта осуществляется субъектом критической информационной инфраструктуры в соответствии с эксплуатационной документацией и организационно-распорядительными документами по безопасности значимого объекта и должно включать реализацию следующих мероприятий:

а) планирование мероприятий по обеспечению безопасности значимого объекта;

б) анализ угроз безопасности информации в значимом объекте и последствий от их реализации;

в) управление (администрирование) подсистемой безопасности значимого объекта;

г) управление конфигурацией значимого объекта и его подсистемой безопасности;

д) реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта;

е) обеспечение действий в нештатных ситуациях в ходе эксплуатации значимого объекта;

ж) информирование и обучение персонала значимого объекта;

з) контроль за обеспечением безопасности значимого объекта.

13.1. В ходе планирования мероприятий по обеспечению безопасности значимого объекта осуществляются:

а) определение лиц, ответственных за планирование и контроль мероприятий по обеспечению безопасности значимого объекта;

б) разработка, утверждение и актуализация плана мероприятий по обеспечению безопасности значимого объекта;

в) определения порядка контроля выполнения мероприятий по обеспечению безопасности значимого объекта, предусмотренных утвержденным планом.

Планирование мероприятий по обеспечению безопасности значимого объекта должно осуществляться в рамах процесса планирования, внедренного в соответствии с требованиями к созданию систем безопасности значимых объектов и обеспечению их функционирования, утвержденными в соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

13.2. В ходе анализа угроз безопасности информации в значимом объекте и возможных последствий их реализации осуществляются:

а) анализ уязвимостей значимого объекта, возникающих в ходе его эксплуатации;

б) анализ изменения угроз безопасности информации в значимом объекте, возникающих в ходе его эксплуатации;

в) оценка возможных последствий реализации угроз безопасности информации в значимом объекте.

Периодичность проведения указанных работ определяется субъектом критической информационной инфраструктуры в организационно-распорядительных документах по безопасности значимых объектов с учетом категории значимости объекта и особенностей его функционирования.

13.3. В ходе управления (администрирования) подсистемой безопасности значимого объекта осуществляются:

а) определение лиц, ответственных за управление (администрирование) подсистемой безопасности значимого объекта;

б) управление учетными записями пользователей и поддержание в актуальном состоянии правил разграничения доступа в значимом объекте;

в) управление средствами защиты информации значимого объекта;

г) управление обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации, с учетом особенностей функционирования значимого объекта;

д) централизованное управление подсистемой безопасности значимого объекта (при необходимости);

е) мониторинг и анализ зарегистрированных событий в значимом объекте, связанных с обеспечением безопасности (далее - события безопасности);

ж) сопровождение функционирования подсистемы безопасности значимого объекта в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документов по безопасности значимого объекта.

13.4. В ходе управления конфигурацией значимого объекта и его подсистемы безопасности для целей обеспечения его безопасности осуществляются:

а) определение лиц, которым разрешены действия по внесению изменений в конфигурацию значимого объекта и его подсистемы безопасности, и их полномочий;

б) определение компонентов значимого объекта и его подсистемы безопасности, подлежащих изменению в рамках управления конфигурации (идентификация объектов управления конфигурации): программно-аппаратные, программные средства, включая средства защиты информации, и их настройки и программный код, эксплуатационная документация, интерфейсы, файлы и иные компоненты, подлежащие изменению и контролю;

в) управление изменениями значимого объекта и его подсистемы безопасности: разработка параметров настройки, обеспечивающих безопасность значимого объекта, анализ потенциального воздействия планируемых изменений на обеспечение безопасности значимого объекта, санкционирование внесения изменений в значимый объект и его подсистему безопасности, документирование действий по внесению изменений в значимый объект и сохранение данных об изменениях конфигурации;

г) контроль действий по внесению изменений в значимый объект и его подсистему безопасности.

Реализованные процессы управления изменениями значимого объекта и его подсистемы безопасности должны охватывать процессы гарантийного

и (или) технического обслуживания, в том числе дистанционного (удаленного), программных и программно-аппаратных средств, включая средства защиты информации, значимого объекта.

13.5. Реагирование на компьютерные инциденты осуществляется в порядке, установленном в соответствии с пунктом 6 части 4 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Для реагирования на компьютерные инциденты определяются работники, ответственные за выявление компьютерных инцидентов и реагирование на них, и определяются их функции.

13.6. Для обеспечения действий в нештатных ситуациях при эксплуатации значимого объекта осуществляются:

а) планирование мероприятий по обеспечению безопасности значимого объекта на случай возникновения нештатных ситуаций;

б) обучение и отработка действий персонала по обеспечению безопасности значимого объекта в случае возникновения нештатных ситуаций;

в) создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций;

г) резервирование программных и программно-аппаратных средств, в том числе средств защиты информации, каналов связи на случай возникновения нештатных ситуаций;

д) обеспечение возможности восстановления значимого объекта и (или) его компонентов в случае возникновения нештатных ситуаций;

е) определение порядка анализа возникших нештатных ситуаций и принятия мер по недопущению их повторного возникновения.

13.7. В ходе информирования и обучения персонала значимого объекта осуществляются:

а) информирование персонала об угрозах безопасности информации, о правилах безопасной эксплуатации значимого объекта;

б) доведение до персонала требований по обеспечению безопасности значимых объектов, а также положений организационно-распорядительных документов по безопасности значимых объектов в части, их касающейся;

в) обучение персонала правилам эксплуатации отдельных средств защиты информации, включая проведение практических занятий с персоналом;

г) контроль осведомленности персонала об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения безопасности критической информационной инфраструктуры.

Периодичность проведения указанных мероприятий устанавливается субъектом критической информационной инфраструктуры в организационно-распорядительных документах по безопасности значимого объекта с учетом категории значимости и особенностей функционирования значимого объекта.

13.8. В ходе контроля за обеспечением безопасности значимого объекта осуществляются:

а) контроль (анализ) защищенности значимого объекта с учетом особенностей его функционирования;

б) анализ и оценка функционирования значимого объекта и его подсистемы безопасности, включая анализ и устранение уязвимостей и иных недостатков в функционировании подсистемы безопасности значимого объекта;

в) документирование процедур и результатов контроля за обеспечением безопасности значимого объекта;

г) принятие решения по результатам контроля за обеспечением безопасности значимого объекта о необходимости доработки (модернизации) его подсистемы безопасности.

Обеспечение безопасности значимого объекта при выводе его из эксплуатации

14. Обеспечение безопасности значимого объекта при выводе его из эксплуатации или после принятия решения об окончании обработки информации осуществляется субъектом критической информационной инфраструктуры в соответствии с эксплуатационной документацией на значимый объект и организационно-распорядительными документами по безопасности значимого объекта.

Обеспечение безопасности значимого объекта при выводе его из эксплуатации должно предусматривать:

а) архивирование информации, содержащейся в значимом объекте;

б) уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации;

в) уничтожение или архивирование данных об архитектуре и конфигурации значимого объекта;

г) архивирование или уничтожение эксплуатационной документации на значимый объект и его подсистему безопасности и организационно-распорядительных документов по безопасности значимого объекта.

14.1. Архивирование информации, содержащейся в значимом объекте, должно осуществляться в случае ее дальнейшего использования в деятельности субъекта критической информационной инфраструктуры.

14.2. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации осуществляется в случае обработки значимым объектом информации ограниченного доступа или в случае принятия такого решения субъектом критической информационной инфраструктуры.

Уничтожение (стирание) данных и остаточной информации с машинных

носителей информации производится при необходимости передачи машинного носителя информации другому пользователю значимого объекта или в иные организации для ремонта, технического обслуживания или дальнейшего уничтожения.

При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, производится или физическое уничтожение самих машинных носителей информации или уничтожение содержащейся на машинных носителях информации методами, не предусматривающими возможность ее восстановления.

Уничтожение (стирание) данных и остаточной информации с машинных носителей информации подлежит документированию в соответствии с организационно-распорядительными документами по безопасности значимого объекта.

14.3. При выводе значимого объекта из эксплуатации должен быть осуществлен сброс настроек программных и программно-аппаратных средств, в том числе средств защиты информации, удалена информация о субъектах доступа и объектах доступа, удалены учетные записи пользователей, а также идентификационная и аутентификационная информация субъектов доступа.

14.4. При выводе значимого объекта из эксплуатации вся эксплуатационная документация на значимый объект и его подсистему безопасности, эксплуатационная документация на отдельные средства защиты информации подлежит архивному хранению.

Сроки хранения документации определяются субъектом критической информационной инфраструктуры в организационно-распорядительных документах по безопасности значимого объекта.

По решению субъекта критической информационной инфраструктуры эксплуатационная документация на значимый объект и его подсистему безопасности, а также организационно-распорядительные документы по безопасности значимого объекта (инструкции, руководства) могут быть уничтожены. В этом случае факт уничтожения подлежит документированию субъектом критической информационной инфраструктуры с указанием наименования, состава документов, способов и даты их уничтожения.

III. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов

15. Целью обеспечения безопасности значимого объекта является обеспечение его устойчивого функционирования в проектных режимах работы в условиях реализации в отношении значимого объекта угроз безопасности информации.

16. Задачами обеспечения безопасности значимого объекта являются:

а) предотвращение неправомерного доступа к информации, обрабатываемой значимым объектом, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

б) недопущение информационного воздействия на программные и программно-аппаратные средства, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта;

в) обеспечение функционирования значимого объекта в проектных режимах его работы в условиях воздействия угроз безопасности информации;

г) обеспечение возможности восстановления функционирования значимого объекта критической информационной инфраструктуры.

17. В значимых объектах объектами, подлежащими защите от угроз безопасности информации (объектами защиты), являются:

а) в информационных системах:

информация, обрабатываемая в информационной системе;

программно-аппаратные средства (в том числе машинные носители информации, автоматизированные рабочие места, серверы, телекоммуникационное оборудование, линии связи, средства обработки буквенно-цифровой, графической, видео- и речевой информации);

программные средства (в том числе микропрограммное, общесистемное, прикладное программное обеспечение);

средства защиты информации;

архитектура и конфигурация информационной системы;

б) в информационно-телекоммуникационных сетях:

информация, передаваемая по линиям связи;

телекоммуникационное оборудование (в том числе программное обеспечение, система управления);

средства защиты информации;

архитектура и конфигурация информационно-телекоммуникационной сети;

в) в автоматизированных системах управления:

информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса (в том числе входная (выходная) информация, управляющая (командная) информация, контрольно-измерительная информация, иная критически важная (технологическая) информация);

программно-аппаратные средства (в том числе автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, линии связи, программируемые логические контроллеры, производственное, технологическое оборудование (исполнительные устройства);

программные средства (в том числе микропрограммное, общесистемное, прикладное программное обеспечение);

средства защиты информации;

архитектура и конфигурация автоматизированной системы управления.

18. Обеспечение безопасности значимого объекта достигается путем принятия в рамках подсистемы безопасности значимого объекта совокупности организационных и технических мер, направленных на блокирование (нейтрализацию) угроз безопасности информации, реализация которых может привести к прекращению или нарушению функционирования значимого объекта и обеспечивающего (управляемого, контролируемого) им процесса, а также нарушению безопасности обрабатываемой информации (нарушению доступности, целостности, конфиденциальности информации).

Организационные и технические меры по обеспечению безопасности значимого объекта принимаются субъектом критической информационной инфраструктуры совместно с лицом, эксплуатирующим значимый объект (при его наличии). При этом между субъектом критической информационной инфраструктуры и лицом, эксплуатирующим значимый объект, должно быть проведено разграничение функций по обеспечению безопасности значимого объекта в ходе его эксплуатации.

19. Меры по обеспечению безопасности выбираются и реализуются в значимом объекте с учетом угроз безопасности информации применительно ко всем объектам и субъектам доступа на аппаратном, системном, прикладном и сетевом уровнях, в том числе в среде виртуализации.

20. Меры по обеспечению безопасности значимого объекта принимаются 25субъектом критической информационной инфраструктуры самостоятельно или при необходимости с привлечением в соответствии с законодательством Российской Федерации организаций, имеющих в зависимости от информации, обрабатываемой значимым объектом, лицензию на деятельность по технической защите информации, составляющей государственную тайну, и (или) на деятельность по технической защите конфиденциальной информации.

21. Принимаемые организационные и технические меры по обеспечению безопасности значимого объекта должны соотноситься с мерами по промышленной, функциональной безопасности, иными мерами по обеспечению безопасности значимого объекта и обеспечивающего (управляемого, контролируемого) объекта или процесса. При этом меры по обеспечению безопасности значимого объекта не должны оказывать отрицательного влияния на функционирование значимого объекта в проектных режимах его работы.

22. В значимых объектах в зависимости от их категории значимости и угроз безопасности информации должны быть реализованы следующие организационные и технические меры:

идентификация и аутентификация (ИАФ);

управление доступом (УПД);
ограничение программной среды (ОПС);
защита машинных носителей информации (ЗНИ);
аудит безопасности (АУД);
антивирусная защита (АВЗ);
предотвращение вторжений (компьютерных атак) (СОВ);
обеспечение целостности (ОЦЛ);
обеспечение доступности (ОДТ);
защита технических средств и систем (ЗТС);
защита информационной (автоматизированной) системы и ее компонентов (ЗИС);
планирование мероприятий по обеспечению безопасности (ПЛН);
управление конфигурацией (УКФ);
управление обновлениями программного обеспечения (ОПО);
реагирование на инциденты информационной безопасности (ИНЦ);
обеспечение действий в нештатных ситуациях (ДНС);
информирование и обучение персонала (ИПО).

Состав мер по обеспечению безопасности значимых объектов в зависимости от категории значимости приведен в приложении к настоящим Требованиям.

При реализации мер по обеспечению безопасности значимых объектов применяются методические документы, разработанные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

23. Выбор мер по обеспечению безопасности значимых объектов для их реализации включает:

а) определение базового набора мер по обеспечению безопасности значимого объекта;

б) адаптацию базового набора мер по обеспечению безопасности значимого объекта;

в) дополнение адаптированного набора мер по обеспечению безопасности значимого объекта мерами, установленными иными нормативными правовыми актами в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации и защиты информации.

Базовый набор мер по обеспечению безопасности значимого объекта определяется на основе установленной категории значимости значимого объекта в соответствии с приложением к настоящим Требованиям.

Базовый набор мер по обеспечению безопасности значимого объекта подлежит адаптации в соответствии с угрозами безопасности информации, применяемыми информационными технологиями и особенностями

функционирования значимого объекта. При этом из базового набора могут быть исключены меры, непосредственно связанные с информационными технологиями, не используемыми в значимом объекте, или характеристиками, не свойственными значимому объекту. При адаптации базового набора мер по обеспечению безопасности значимого объекта для каждой угрозы безопасности информации, включенной в модель угроз, сопоставляется мера или группа мер, обеспечивающие блокирование одной или нескольких угроз безопасности или снижающие возможность ее реализации исходя из условий функционирования значимого объекта. В случае если базовый набор мер не позволяет обеспечить блокирование (нейтрализацию) всех угроз безопасности информации, в него дополнительно включаются меры, приведенные в приложении к настоящим Требованиям.

Дополнение адаптированного набора мер по обеспечению безопасности значимого объекта осуществляется с целью выполнения требований, установленных иными нормативными правовыми актами в области обеспечения безопасности критической информационной инфраструктуры и защиты информации. Дополнение адаптированного набора мер проводится в случае, если в отношении значимого объекта в соответствии с законодательством Российской Федерации также установлены требования о защите информации, содержащейся в государственных информационных системах, требования к защите персональных данных при их обработке в информационных системах персональных данных, требования к криптографической защите информации или иные требования в области защиты информации и обеспечения безопасности критической информационной инфраструктуры.

24. В случае если значимый объект является государственной информационной системой или информационной системой персональных данных, меры по обеспечению безопасности значимого объекта и меры защиты информации (по обеспечению персональных данных) принимаются в соответствии с более высокой категорией значимости, классом защищенности или уровнем защищенности персональных данных.

25. Если принятые в значимом объекте меры по обеспечению промышленной, функциональной безопасности и (или) физической безопасности достаточны для блокирования (нейтрализации) отдельных угроз безопасности информации, дополнительные меры, выбранные в соответствии с пунктами 22 и 23 настоящих Требований, могут не применяться. При этом в ходе разработки организационных и технических мер по обеспечению безопасности значимого объекта должна быть обоснована достаточность применения мер по обеспечению промышленной безопасности или физической безопасности для блокирования (нейтрализации) соответствующих угроз безопасности информации.

26. При отсутствии возможности реализации отдельных мер по обеспечению безопасности и (или) невозможности их применения к отдельным объектам и субъектам доступа, в том числе вследствие их негативного влияния на функционирование значимого объекта в проектных режимах значимого объекта, должны быть разработаны и внедрены компенсирующие меры, обеспечивающие блокирование (нейтрализацию) угроз безопасности информации с необходимым уровнем защищенности значимого объекта. При этом в ходе разработки организационных и технических мер по обеспечению безопасности значимого объекта должно быть обосновано применение компенсирующих мер, а при приемочных испытаниях (аттестации) оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

В качестве компенсирующих мер могут быть рассмотрены меры по обеспечению промышленной, функциональной и (или) физической безопасности значимого объекта, поддерживающие необходимый уровень его защищенности.

26.1. При использовании в значимых объектах новых информационных технологий и выявлении дополнительных угроз безопасности информации, для которых не определены меры по обеспечению безопасности, должны разрабатываться компенсирующие меры в соответствии с пунктом 26 настоящих Требований.

IV. Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов

27. Технические меры по обеспечению безопасности в значимом объекте реализуются посредством использования программных и программно-аппаратных средств, применяемых для обеспечения безопасности значимых объектов – средств защиты информации (в том числе встроенных в общесистемное, прикладное программное обеспечение), а также обеспечения безопасности программного обеспечения и программно-аппаратных средств, применяемых в значимых объектах.

При этом в приоритетном порядке подлежат применению средства защиты информации, встроенные в программное обеспечение и (или) программно-аппаратные средства значимых объектов (при их наличии).

28. Для обеспечения безопасности значимых объектов критической информационной инфраструктуры должны применяться средства защиты информации, прошедшие оценку на соответствие требованиям по безопасности в формах обязательной сертификации, испытаний или приемки.

Средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации, применяются в случаях, установленных законодательством Российской Федерации, а также в случае принятия решения субъектом критической информационной инфраструктуры.

В иных случаях применяются средства защиты информации, прошедшие оценку соответствия в форме испытаний или приемки, которые проводятся субъектами критической информационной инфраструктуры самостоятельно или с привлечением организаций, имеющих в соответствии с законодательством Российской Федерации лицензии на деятельность в области защиты информации.

29. В случае использования в значимом объекте сертифицированных на соответствие требованиям по безопасности информации средств защиты информации:

а) в значимых объектах 1 категории применяются средства защиты информации не ниже 4 класса защиты, а также средства вычислительной техники не ниже 5 класса;

б) в значимых объектах 2 категории применяются средства защиты информации не ниже 5 класса защиты, а также средства вычислительной техники не ниже 5 класса;

в) в значимых объектах 3 категории применяются средства защиты информации 6 класса защиты, а также средства вычислительной техники не ниже 5 класса.

При этом в значимых объектах 1 категории значимости применяются сертифицированные средства защиты информации, соответствующие 4 или более высокому уровню доверия. В значимых объектах 2 категории значимости применяются сертифицированные средства защиты информации, соответствующие 5 или более высокому уровню доверия. В значимых объектах 3 категории значимости применяются сертифицированные средства защиты информации, соответствующие 6 или более высокому уровню доверия.

Классы защиты и уровни доверия определяются в соответствии с нормативными правовыми актами ФСТЭК России, изданными в соответствии с подпунктом 13.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

При использовании в значимом объекте средств защиты информации, сертифицированных по требованиям безопасности информации, указанные средства должны быть сертифицированы на соответствие обязательным требованиям по безопасности информации, установленным нормативными правовыми актами, или требованиям, указанным в технических условиях (заданиях по безопасности).

Функции безопасности средств защиты информации должны обеспечивать выполнение настоящих Требований.

29.1. При проектировании вновь создаваемых или модернизируемых значимых объектов 1 категории значимости в качестве граничных маршрутизаторов, имеющих доступ к информационно-телекоммуникационной сети «Интернет», выбираются маршрутизаторы, сертифицированные на соответствие требованиям по безопасности информации (в части реализованных в них функций безопасности).

В случае отсутствия технической возможности применения в значимых объектах 1 категории значимости граничных маршрутизаторов, сертифицированных на соответствие требованиям по безопасности информации, функции безопасности граничных маршрутизаторов подлежат оценке на соответствие требованиям по безопасности в рамках приемки или испытаний значимых объектов.

Обоснование отсутствия технической возможности приводится в проектной документации на значимые объекты (подсистемы безопасности значимых объектов), разрабатываемой в соответствии с техническим заданием на создание значимых объектов и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимых объектов.

29.2. Средства защиты информации, оценка соответствия которых проводится в форме испытаний или приемки, должны соответствовать требованиям к функциям безопасности, установленным в соответствии с подпунктом «ж» пункта 10 настоящих Требований.

Не встроенные в общесистемное и прикладное программное обеспечение средства защиты информации, оценка соответствия которых проводится в форме испытаний или приемки, дополнительно к указанным требованиям должны соответствовать 6 или более высокому уровню доверия.

Испытания (приемка) средств защиты информации на соответствие требованиям к уровню доверия и требованиям к функциям безопасности проводятся на этапе предварительных испытаний в соответствии с пунктом 12.4 настоящих Требований.

Испытания (приемка) проводятся отдельно или в составе значимого объекта. Программа и методики испытаний (приемки) утверждаются субъектом критической информационной инфраструктуры в случае самостоятельного проведения испытаний. В случае проведения испытаний иным лицом, программа и методики испытаний (приемки) утверждаются этим лицом по согласованию с субъектом критической информационной инфраструктуры.

По результатам испытаний (приемки) средства защиты информации оформляется протокол испытаний, в котором указываются:

дата и место проведения испытаний (приемки);

описание испытываемого средства защиты информации;

описание проведенных испытаний;

результаты испытаний по каждому испытываемому параметру (характеристике);

выводы о соответствии (несоответствии) средства защиты информации требованиям по безопасности информации.

Протокол испытаний утверждается субъектом критической информационной инфраструктуры в случае самостоятельного проведения испытаний. В ином случае протокол испытаний утверждается лицом, проводившим испытания, и представляется субъекту критической информационной инфраструктуры на этапе приемочных испытаний для принятия решения о возможности применения средства защиты информации в значимом объекте.

Испытания (приемка), предусмотренные настоящим пунктом, проводятся в отношении средств защиты информации, планируемых к внедрению в рамках создания (модернизации или реконструкции, ремонта) значимых объектов.

29.3. Прикладное программное обеспечение, планируемое к внедрению в рамках создания (модернизации или реконструкции, ремонта) значимого объекта и обеспечивающее выполнение его функций по назначению (далее – программное обеспечение), должно соответствовать следующим требованиям по безопасности:

29.3.1. Требования по безопасной разработке программного обеспечения:

наличие руководства по безопасной разработке программного обеспечения;

проведение анализа угроз безопасности информации программного обеспечения;

наличие описания структуры программного обеспечения на уровне подсистем и результатов сопоставления функций программного обеспечения и интерфейсов, описанных в функциональной спецификации, с его подсистемами (для программного обеспечения, планируемого к применению в значимых объектах 1 категории значимости).

29.3.2. Требования к испытаниям по выявлению уязвимостей в программном обеспечении:

проведение статического анализа исходного кода программы;

проведение фаззинг-тестирования программы, направленного на выявление в ней уязвимостей;

проведение динамического анализа кода программы (для программного обеспечения, планируемого к применению в значимых объектах 1 категории значимости).

29.3.3. Требования к поддержке безопасности программного обеспечения:

наличие процедур отслеживания и исправления обнаруженных ошибок и уязвимостей программного обеспечения;

определение способов и сроков доведения разработчиком (производителем) программного обеспечения до его пользователей информации об уязвимостях программного обеспечения, о компенсирующих мерах по защите информации или ограничениях по применению программного обеспечения, способов получения пользователями программного обеспечения его обновлений, проверки их целостности и подлинности;

наличие процедур информирования субъекта критической информационной инфраструктуры об окончании производства и (или) поддержки программного обеспечения (для программного обеспечения, планируемого к применению в значимых объектах 1 категории значимости).

29.4. Выполнение требований по безопасности, указанных в подпунктах 29.3.1-29.3.3 пункта 29.3 настоящих Требований, оценивается лицом, выполняющим работы по созданию (модернизации, реконструкции или ремонту) значимого объекта и (или) обеспечению его безопасности, на этапе проектирования значимого объекта на основе результатов анализа материалов и документов, представляемых разработчиком (производителем) программного обеспечения в соответствии с техническим заданием (частным техническим заданием), разрабатываемым в соответствии с пунктом 10 настоящих Требований.

Результаты оценки включаются в проектную документацию на значимый объект (подсистему безопасности значимого объекта) и представляются субъекту критической информационной инфраструктуры.

30. Применяемые в значимом объекте программные и программно-аппаратные средства, в том числе средства защиты информации, должны эксплуатироваться в соответствии с инструкциями (правилами) по эксплуатации, разработанными разработчиками (производителями) этих средств, и иной эксплуатационной документацией.

31. Применяемые в значимом объекте программные и программно-аппаратные средства, в том числе средства защиты информации, должны быть обеспечены гарантийной и (или) технической поддержкой.

При выборе программных и программно-аппаратных средств, в том числе средств зашиты информации, необходимо учитывать наличие ограничений на возможность их применения субъектом критической информационной инфраструктуры на любом из принадлежащих ему значимых объектов критической информационной инфраструктуры со стороны разработчиков (производителей) или иных лиц.

В значимом объекте не допускаются:

наличие удаленного доступа к программным и программно-аппаратным средствам, в том числе средствам защиты информации, для обновления или управления со стороны лиц, не являющихся работниками субъекта критической информационной инфраструктуры, а также работниками его дочерних и зависимых обществ;

наличие локального бесконтрольного доступа к программным и программно-аппаратным средствам, в том числе средствам зашиты информации, для обновления или управления со стороны лиц, не являющихся работниками субъекта критической информационной инфраструктуры, его дочерних и зависимых обществ;

передача информации, в том числе технологической информации, разработчику (производителю) программных и программно-аппаратных средств, в том числе средств защиты информации, или иным лицам без контроля со стороны субъекта критической информационной инфраструктуры.

В случае технической невозможности исключения удаленного доступа к программным и программно-аппаратным средствам, в том числе средствам защиты информации, в значимом объекте принимаются организационные и технические меры по обеспечению безопасности такого доступа, предусматривающие:

определение лиц и устройств, которым разрешен удаленный доступ к программным и программно-аппаратным средствам значимого объекта, предоставление им минимальных полномочий при доступе к этим средствам;

контроль доступа к программным и программно-аппаратным средствам значимого объекта;

защиту информации и данных при их передаче по каналам связи при удаленном доступе к программным и программно-аппаратным средствам значимого объекта;

мониторинг и регистрацию действий лиц, которым разрешен удаленный доступ к программным и программно-аппаратным средствам значимого объекта, а также инициируемых ими процессов, анализ этих действий в целях выявления фактов неправомерных действий;

обеспечение невозможности отказа лиц от выполненных действий при осуществлении удаленного доступа к программным и программно-аппаратным средствам значимого объекта.

В значимом объекте могут приниматься дополнительные организационные и технические меры по обеспечению безопасности удаленного доступа к программным и программно-аппаратным средствам, в том числе средствам защиты информации, направленные на блокирование (нейтрализацию) угроз безопасности информации, приведенных в модели угроз безопасности информации, разрабатываемой в соответствии с пунктом 11.1 настоящих Требований.

Входящие в состав значимого объекта 1 и 2 категорий значимости программные и программно-аппаратные средства, осуществляющие хранение и обработку информации, должны размещаться на территории Российской Федерации (за исключением случаев, когда размещение указанных средств осуществляется в зарубежных обособленных подразделениях субъекта критической информационной инфраструктуры (филиалах, представительствах), а также случаев, установленных законодательством Российской Федерации и (или) международными договорами Российской Федерации).

Приложение
к Требованиям по обеспечению
безопасности значимых объектов
критической информационной
инфраструктуры Российской Федерации,
утвержденным приказом ФСТЭК России
от 25 декабря 2017 г. № 239

Состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости		
		3	2	1
I. Идентификация и аутентификация (ИАФ)				
ИАФ.0	Регламентация правил и процедур идентификации и аутентификации	+	+	+
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+	+	+
ИАФ.2	Идентификация и аутентификация устройств	+	+	+
ИАФ.3	Управление идентификаторами	+	+	+
ИАФ.4	Управление средствами аутентификации	+	+	+
ИАФ.5	Идентификация и аутентификация внешних пользователей	+	+	+
ИАФ.6	Двусторонняя аутентификация			
ИАФ.7	Защита аутентификационной информации при передаче	+	+	+
II. Управление доступом (УПД)				
УПД.0	Регламентация правил и процедур управления доступом	+	+	+
УПД.1	Управление учетными записями пользователей	+	+	+
УПД.2	Реализация модели управления доступом	+	+	+
УПД.3	Доверенная загрузка		+	+
УПД.4	Разделение полномочий (ролей) пользователей	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий	+	+	+
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+	+	+

УПД.7	Предупреждение пользователя при его доступе к информационным ресурсам			
УПД.8	Оповещение пользователя при успешном входе о предыдущем доступе к информационной (автоматизированной) системе			
УПД.9	Ограничение числа параллельных сеансов доступа			+
УПД.10	Блокирование сеанса доступа пользователя при неактивности	+	+	+
УПД.11	Управление действиями пользователей до идентификации и аутентификации	+	+	+
УПД.12	Управление атрибутами безопасности			
УПД.13	Реализация защищенного удаленного доступа	+	+	+
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	+	+	+
III. Ограничение программной среды (ОПС)				
ОПС.0	Регламентация правил и процедур ограничения программной среды		+	+
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения			+
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения		+	+
ОПС.3	Управление временными файлами			
IV. Защита машинных носителей информации (ЗНИ)				
ЗНИ.0	Регламентация правил и процедур защиты машинных носителей информации	+	+	+
ЗНИ.1	Учет машинных носителей информации	+	+	+
ЗНИ.2	Управление физическим доступом к машинным носителям информации	+	+	+
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны			
ЗНИ.4	Исключение возможности несанкционированного чтения информации на машинных носителях информации			
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации	+	+	+
ЗНИ.6	Контроль ввода (вывода) информации на съемные машинные носители информации			+
ЗНИ.7	Контроль подключения съемных машинных носителей информации	+	+	+
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	+	+	+
V. Аудит безопасности (АУД)				

АУД.0	Регламентация правил и процедур аудита безопасности	+	+	+
АУД.1	Инвентаризация информационных ресурсов	+	+	+
АУД.2	Анализ уязвимостей и их устранение	+	+	+
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	+	+	+
АУД.4	Регистрация событий безопасности	+	+	+
АУД.5	Контроль и анализ сетевого трафика			+
АУД.6	Защита информации о событиях безопасности	+	+	+
АУД.7	Мониторинг безопасности	+	+	+
АУД.8	Реагирование на сбои при регистрации событий безопасности	+	+	+
АУД.9	Анализ действий отдельных пользователей			+
АУД.10	Проведение внутренних аудитов	+	+	+
АУД.11	Проведение внешних аудитов			
VI. Антивирусная защита (АВЗ)				
АВЗ.0	Регламентация правил и процедур антивирусной защиты	+	+	+
АВЗ.1	Реализация антивирусной защиты	+	+	+
АВЗ.2	Антивирусная защита электронной почты и иных сервисов	+	+	+
АВЗ.3	Контроль использования архивных, исполняемых и зашифрованных файлов			+
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+
АВЗ.5	Использование средств антивирусной защиты различных производителей			+
VII. Предотвращение вторжений (компьютерных атак) (СОВ)				
СОВ.0	Регламентация правил и процедур предотвращения вторжений (компьютерных атак)		+	+
СОВ.1	Обнаружение и предотвращение компьютерных атак		+	+
СОВ.2	Обновление базы решающих правил		+	+
VIII. Обеспечение целостности (ОЦЛ)				
ОЦЛ.0	Регламентация правил и процедур обеспечения целостности	+	+	+

ОЦЛ.1	Контроль целостности программного обеспечения	+	+	+
ОЦЛ.2	Контроль целостности информации			
ОЦЛ.3	Ограничения по вводу информации в информационную (автоматизированную) систему			+
ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему		+	+
ОЦЛ.5	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях		+	+
ОЦЛ.6	Обезличивание и (или) деидентификация информации			
IX. Обеспечение доступности (ОДТ)				
ОДТ.0	Регламентация правил и процедур обеспечения доступности	+	+	+
ОДТ.1	Использование отказоустойчивых технических средств		+	+
ОДТ.2	Резервирование средств и систем		+	+
ОДТ.3	Контроль безотказного функционирования средств и систем		+	+
ОДТ.4	Резервное копирование информации	+	+	+
ОДТ.5	Обеспечение возможности восстановления информации	+	+	+
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	+	+	+
ОДТ.7	Кластеризация информационной (автоматизированной) системы			
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	+	+	+
X. Защита технических средств и систем (ЗТС)				
ЗТС.0	Регламентация правил и процедур защиты технических средств и систем	+	+	+
ЗТС.1	Защита информации от утечки по техническим каналам			
ЗТС.2	Организация контролируемой зоны	+	+	+
ЗТС.3	Управление физическим доступом	+	+	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+
ЗТС.5	Защита от внешних воздействий	+	+	+
ЗТС.6	Маркирование аппаратных компонентов системы относительно разрешенной к обработке информации			
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)				

ЗИС.0	Регламентация правил и процедур защиты информационной (автоматизированной) системы и ее компонентов	+	+	+
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	+	+	+
ЗИС.2	Защита периметра информационной (автоматизированной) системы	+	+	+
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы	+	+	+
ЗИС.4	Сегментирование информационной (автоматизированной) системы		+	+
ЗИС.5	Организация демилитаризованной зоны	+	+	+
ЗИС.6	Управление сетевыми потоками	+	+	+
ЗИС.7	Использование эмулятора среды функционирования программного обеспечения ("песочница")			
ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы	+	+	+
ЗИС.9	Создание гетерогенной среды			
ЗИС.10	Использование программного обеспечения, функционирующего в средах различных операционных систем			
ЗИС.11	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом			
ЗИС.12	Изоляция процессов (выполнение программ) в выделенной области памяти			
ЗИС.13	Защита неизменяемых данных		+	+
ЗИС.14	Использование неперезаписываемых машинных носителей информации			
ЗИС.15	Реализация электронного почтового обмена с внешними сетями через ограниченное количество контролируемых точек			
ЗИС.16	Защита от спама		+	+
ЗИС.17	Защита информации от утечек			
ЗИС.18	Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию			
ЗИС.19	Защита информации при ее передаче по каналам связи	+	+	+
ЗИС.20	Обеспечение доверенных канала, маршрута	+	+	+
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	+	+	+
ЗИС.22	Управление атрибутами безопасности при взаимодействии с иными информационными (автоматизированными) системами			

ЗИС.23	Контроль использования мобильного кода			
ЗИС.24	Контроль передачи речевой информации			
ЗИС.25	Контроль передачи видеоинформации			
ЗИС.26	Подтверждение происхождения источника информации			
ЗИС.27	Обеспечение подлинности сетевых соединений		+	+
ЗИС.28	Исключение возможности отрицания отправки информации			
ЗИС.29	Исключение возможности отрицания получения информации			
ЗИС.30	Использование устройств терминального доступа			
ЗИС.31	Защита от скрытых каналов передачи информации			
ЗИС.32	Защита беспроводных соединений	+	+	+
ЗИС.33	Исключение доступа через общие ресурсы			+
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)	+	+	+
ЗИС.35	Управление сетевыми соединениями	+	+	+
ЗИС.36	Создание (эмуляция) ложных компонентов информационных (автоматизированных) систем			
ЗИС.37	Перевод информационной (автоматизированной) системы в безопасное состояние при возникновении отказов (сбоев)			
ЗИС.38	Защита информации при использовании мобильных устройств	+	+	+
ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	+	+	+
XII. Реагирование на компьютерные инциденты (ИНЦ)				
ИНЦ.0	Регламентация правил и процедур реагирования на компьютерные инциденты	+	+	+
ИНЦ.1	Выявление компьютерных инцидентов	+	+	+
ИНЦ.2	Информирование о компьютерных инцидентах	+	+	+
ИНЦ.3	Анализ компьютерных инцидентов	+	+	+
ИНЦ.4	Устранение последствий компьютерных инцидентов	+	+	+
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	+	+	+
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах	+	+	+
XIII. Управление конфигурацией (УКФ)				
УКФ.0	Регламентация правил и процедур управления конфигурацией информационной (автоматизированной) системы	+	+	+

УКФ.1	Идентификация объектов управления конфигурацией			
УКФ.2	Управление изменениями	+	+	+
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения	+	+	+
УКФ.4	Контроль действий по внесению изменений			
XIV. Управление обновлениями программного обеспечения (ОПО)				
ОПО.0	Регламентация правил и процедур управления обновлениями программного обеспечения	+	+	+
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника	+	+	+
ОПО.2	Контроль целостности обновлений программного обеспечения	+	+	+
ОПО.3	Тестирование обновлений программного обеспечения	+	+	+
ОПО.4	Установка обновлений программного обеспечения	+	+	+
XV. Планирование мероприятий по обеспечению безопасности (ПЛН)				
ПЛН.0	Регламентация правил и процедур планирования мероприятий по обеспечению защиты информации	+	+	+
ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации	+	+	+
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации	+	+	+
XVI. Обеспечение действий в нештатных ситуациях (ДНС)				
ДНС.0	Регламентация правил и процедур обеспечения действий в нештатных ситуациях	+	+	+
ДНС.1	Разработка плана действий в нештатных ситуациях	+	+	+
ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях	+	+	+
ДНС.3	Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций		+	+
ДНС.4	Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций		+	+

ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций	+	+	+
ДНС.5	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения			
XVII. Информирование и обучение персонала (ИПО)				
ИПО.0	Регламентация правил и процедур информирования и обучения персонала	+	+	+
ИПО.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы	+	+	+
ИПО.2	Обучение персонала правилам безопасной работы	+	+	+
ИПО.3	Проведение практических занятий с персоналом по правилам безопасной работы		+	+
ИПО.4	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы	+	+	+

«+» – мера обеспечения безопасности включена в базовый набор мер для соответствующей категории значимого объекта.

Меры обеспечения безопасности, не обозначенные знаком «+», применяются при адаптации и дополнении базового набора мер, а также при разработке компенсирующих мер в значимом объекте критической информационной инфраструктуры соответствующей категории значимости.