МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 59793
от "11" сентября 2020 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

« 20 » февраля 2020 г. Москва № 35

О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239

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), пунктом 2 и подпунктом 9.1 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; 2017, № 48, ст. 7198; 2018, № 20, ст. 2818), **П Р И К А З Ы В А Ю**:

1. Внести в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 (зарегистрирован Министерством юстиции Российской Федерации 26 марта 2018 г., регистрационный № 50524) (с изменениями, внесенными приказом Федеральной службы по техническому

и экспортному контролю от 9 августа 2018 г. № 138 (зарегистрирован Министерством юстиции Российской Федерации 5 сентября 2018 г., регистрационный № 52071) и приказом Федеральной службы по техническому и экспортному контролю от 26 марта 2019 г. № 60 (зарегистрирован Министерством юстиции Российской Федерации 18 апреля 2019 г., регистрационный № 54443), изменения согласно приложению к настоящему приказу.

2. Установить, что положения пунктов 7 и 8 изменений, прилагаемых к настоящему приказу, вступают в силу с 1 января 2023 г.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

Приложение
к приказу ФСТЭК России
от «20» февраля 2020 г. № 35

Изменения, которые вносятся в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239

1. В пункте 7 слово «(модернизации)» заменить словами «(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)».

2. Абзац шестнадцатый пункта 11.2 после слов «функций безопасности» дополнить словами «, 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».

3. Пункт 12.4 после слов «и отдельных средств защиты информации,» дополнить словами «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,».

4. Дополнить пунктом 26.1 следующего содержания:

«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.»;

5. После пункта 26.1 дополнить наименованием главы IV следующего содержания:

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

6. Абзац первый пункта 27 дополнить словами «, а также обеспечения безопасности программного обеспечения и программно-аппаратных средств, применяемых в значимых объектах».

7. Абзац четвертый пункта 28 признать утратившим силу.

8. Дополнить пунктами 29.2-29.4 следующего содержания:

«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.».

9. В пункте 31:

абзац четвертый изложить в следующей редакции:

«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;»;

абзац пятый после слов «информационной инфраструктуры» дополнить словами «, его дочерних и зависимых обществ»;

после абзаца шестого дополнить абзацами следующего содержания:

«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.»;

в абзаце седьмом слова «1 категории» заменить словами «1 и 2 категорий».

10. Пункт 32 признать утратившим силу.