**ФЕДЕРАЛЬНАЯ СЛУЖБА**
**ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ**
**(ФСТЭК России)**

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 53924
от "13" сентября 2019 г.

# П Р И К А З

«28» мая 2019 г. Москва № 106

**О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17**

---

В соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2014, № 30, ст. 4243) 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; 2005, № 13, ст. 1138; 2006, № 49, ст. 5192; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818; 2013, № 26, ст. 3314; № 52, ст. 7137; 2014, № 36, ст. 4833, № 44, ст. 6041; 2015, № 4, ст. 641; 2016, № 1, ст. 211; 2017, № 48, ст. 7198; 2018, № 20, ст. 2818), **П Р И К А З Ы В А Ю**:

1. Внести в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 (зарегистрирован Министерством юстиции Российской Федерации 31 мая 2013 г.,

регистрационный № 28608) (с изменениями, внесёнными приказом Федеральной службы по техническому и экспортному контролю от 15 февраля 2017 г. № 27 (зарегистрирован Министерством юстиции Российской Федерации 14 марта 2017 г., регистрационный № 45933), изменения согласно приложению к настоящему приказу.

2. Установить, что пункт 13 изменений, утвержденных настоящим приказом, вступает в силу с 1 июня 2020 г.

**ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ**
**ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ**

**В.СЕЛИН**

Приложение
к приказу ФСТЭК России
от «28» мая 2019 г. № 106

**Изменения, которые вносятся в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17**

1. Пункт 14.2 дополнить абзацем следующего содержания:

«Класс защищенности информационной системы, функционирование которой предполагается на базе информационно-телекоммуникационной инфраструктуры центра обработки данных,[1] не должен быть выше класса защищенности информационно-телекоммуникационной инфраструктуры центра обработки данных.».

2. Пункт 14.3 после абзаца третьего дополнить абзацем следующего содержания:

«При определении угроз безопасности информации в информационной системе, функционирование которой предполагается на базе информационно-телекоммуникационной инфраструктуры центра обработки данных, должны учитываться угрозы безопасности информации, актуальные для информационно-телекоммуникационной инфраструктуры центра обработки данных.».

3. Пункт 14.4 дополнить абзацем следующего содержания:

«В случае создания информационной системы, функционирование которой предполагается на базе информационно-телекоммуникационной инфраструктуры центра обработки данных, дополнительно определяются требования по защите информации, подлежащие реализации в информационно-телекоммуникационной инфраструктуре центра обработки данных.».

4. Пункт 15.1 дополнить абзацем следующего содержания:

«При проектировании системы защиты информации информационной системы, функционирование которой предполагается на базе информационно-

---

[1] Пункт 5.3 Методических указаний по осуществлению учета информационных систем и компонентов информационно-телекоммуникационной инфраструктуры, утвержденных приказом Минкомсвязи России от 31 мая 2013 г. № 127 (зарегистрирован Минюстом России 5 ноября 2013 г., регистрационный № 30318), с учетом изменений, внесенных приказом Минкомсвязи России от 15 июня 2016 г. № 266 (зарегистрирован Минюстом России 14 июля 2016 г., регистрационный № 42853).

телекоммуникационной инфраструктуры центра обработки данных, для блокирования актуальных угроз безопасности информации могут быть применены меры защиты информации, реализуемые в информационно-телекоммуникационной инфраструктуре центра обработки данных.».

5. Пункт 16.1 дополнить абзацем следующего содержания:

«Средства защиты информации, устанавливаемые в информационной системе, функционирующей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных, должны быть совместимы между собой, а также со средствами защиты информации, установленными в информационно-телекоммуникационной инфраструктуре центра обработки данных.».

6. Абзац второй пункта 17 после слов «должностными лицами» дополнить словом «(работниками)».

7. Пункт 17.2 после абзаца первого дополнить абзацем следующего содержания:

«По решению заказчика (оператора) аттестационные испытания могут быть совмещены с проведением приемочных испытаний информационной системы.».

8. Пункт 17.4 изложить в следующей редакции:

«17.4. Аттестат соответствия выдается на весь срок эксплуатации информационной системы. Оператор (обладатель информации) в ходе эксплуатации информационной системы должен обеспечивать поддержку соответствия системы защиты информации аттестату соответствия в рамках реализации мероприятий, предусмотренных пунктом 18 настоящих Требований.».

9. Абзац второй пункта 17.6 изложить в следующей редакции:

«В случае если информационная система создается на базе информационно-телекоммуникационной инфраструктуры центра обработки данных уполномоченного лица, такая инфраструктура центра обработки данных должна быть аттестована на соответствие настоящим Требованиям.».

10. Пункты 18 – 18.4 изложить в следующей редакции:

«18. Обеспечение защиты информации в ходе эксплуатации информационной системы должно осуществляться оператором в соответствии с эксплуатационной документацией и организационно-распорядительными документами по защите информации и включать следующие мероприятия:

планирование мероприятий по защите информации в информационной системе;

анализ угроз безопасности информации в информационной системе;

управление (администрирование) системой защиты информации информационной системы;

управление конфигурацией информационной системы и ее системой защиты информации;

реагирование на инциденты;

информирование и обучение персонала информационной системы;

контроль за обеспечением уровня защищенности информации, содержащейся в информационной системе.

18.1. В ходе планирования мероприятий по защите информации в информационной системе осуществляются:

определение лиц, ответственных за планирование и контроль мероприятий по защите информации в информационной системе;

определение лиц, ответственных за выявление инцидентов и реагирование на них;

разработка, утверждение и актуализация плана мероприятий по защите информации в информационной системе;

определение порядка контроля выполнения мероприятий по обеспечению защиты информации в информационной системе, предусмотренных утвержденным планом.

План мероприятий по защите информации в информационной системе утверждается вместе с правовым актом органа исполнительной власти о вводе информационной системы в эксплуатацию.

Контроль выполнения мероприятий, предусмотренных планом мероприятий по защите информации в информационной системе, осуществляется в сроки, определенные указанным планом.

18.2. В ходе анализа угроз безопасности информации в информационной системе в ходе ее эксплуатации осуществляются:

выявление, анализ и устранение уязвимостей информационной системы;

анализ изменения угроз безопасности информации в информационной системе;

оценка возможных последствий реализации угроз безопасности информации в информационной системе.

Периодичность проведения указанных работ определяется оператором в организационно-распорядительных документах по защите информации.

18.3. В ходе управления (администрирования) системой защиты информации информационной системы осуществляются:

определение лиц, ответственных за управление (администрирование) системой защиты информации информационной системы;

управление учетными записями пользователей и поддержание в актуальном состоянии правил разграничения доступа в информационной системе;

управление средствами защиты информации информационной системы;

управление обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации, с учетом особенностей функционирования информационной системы;

централизованное управление системой защиты информации информационной системы (при необходимости);

мониторинг и анализ зарегистрированных событий в информационной системе, связанных с обеспечением безопасности (далее - события безопасности);

обеспечение функционирования системы защиты информации информационной системы в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документов по защите информации.

18.4. В ходе управления конфигурацией информационной систем и ее системы защиты информации осуществляются:

определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и ее системы защиты информации, и их полномочий;

определение компонентов информационной системы и ее системы защиты информации, подлежащих изменению в рамках управления конфигурацией (идентификация объектов управления конфигурацией): программно-аппаратные, программные средства, включая средства защиты информации, их настройки и программный код, эксплуатационная документация, интерфейсы, файлы и иные компоненты, подлежащие изменению и контролю;

управление изменениями информационной системы и ее системы защиты информации: разработка параметров настройки, обеспечивающих защиту информации, анализ потенциального воздействия планируемых изменений на обеспечение защиты информации, санкционирование внесения изменений в информационную систему и ее систему защиты информации, документирование действий по внесению изменений в информационную систему и сохранение данных об изменениях конфигурации;

контроль действий по внесению изменений в информационную систему и ее систему защиты информации.

Реализованные процессы управления изменениями информационной системы и ее системы защиты информации должны включать процессы гарантийного и (или) технического обслуживания, в том числе дистанционного (удаленного), программных и программно-аппаратных средств, включая средства защиты информации, информационной системы.

11. Дополнить пунктами 18.5 – 18.7 следующего содержания:

«18.5. В ходе реагирования на инциденты осуществляются:

обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

своевременное информирование пользователями и администраторами лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе;

анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

планирование и принятие мер по устранению инцидентов, в том числе по восстановлению информационной системы и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

планирование и принятие мер по предотвращению повторного возникновения инцидентов.

18.6. В ходе информирования и обучения персонала информационной системы осуществляются:

информирование персонала информационной системы о появлении актуальных угрозах безопасности информации, о правилах безопасной эксплуатации информационной системы;

доведение до персонала информационной системы требований по защите информации, а также положений организационно-распорядительных документов по защите информации с учетом внесенных в них изменений;

обучение персонала информационной системы правилам эксплуатации отдельных средств защиты информации;

проведение практических занятий и тренировок с персоналом информационной системы по блокированию угроз безопасности информации и реагированию на инциденты;

контроль осведомленности персонала информационной системы об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения защиты информации.

Периодичность проведения практических занятий и тренировок с персоналом, мероприятий по обучению персонала и контролю осведомленности персонала устанавливается оператором в организационно-распорядительных документах по защите информации с учетом особенностей функционирования информационной системы, но не реже 1 раза в два года.

18.7. В ходе контроля за обеспечением уровня защищенности информации, содержащейся в информационной системе, осуществляются:

контроль (анализ) защищенности информации с учетом особенностей функционирования информационной системы;

анализ и оценка функционирования информационной системы и ее системы защиты информации, включая анализ и устранение уязвимостей и иных недостатков в функционировании системы защиты информации информационной системы;

документирование процедур и результатов контроля за обеспечением уровня защищенности информации, содержащейся в информационной системе;

принятие решения по результатам контроля за обеспечением уровня защищенности информации, содержащейся в информационной системе, о необходимости доработки (модернизации) ее системы защиты информации.

Контроль за обеспечением уровня защищенности информации, содержащейся в информационной системе, проводится оператором самостоятельно и (или) с привлечением организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

Периодичность проведения контроля за обеспечением уровня защищенности информации, содержащейся в информационной системе 1 класса защищенности, устанавливается оператором в организационно-распорядительных документах по защите информации с учетом особенностей функционирования информационной системы, но не реже 1 раза в год.

Периодичность проведения контроля за обеспечением уровня защищенности информации, содержащейся в информационных системах 2 и 3 классов защищенности, устанавливается оператором в организационно-распорядительных документах по защите информации с учетом особенностей функционирования информационных систем, но не реже 1 раза в два года.».

12. Дополнить пунктом 22.1 следующего содержания:

«22.1. В случае если меры защиты информации, реализованные в информационно-телекоммуникационной инфраструктуре центра обработки данных, обеспечивают блокирование угроз безопасности информации, актуальных для функционирующей на его базе информационной системы, принятие дополнительных мер защиты информации в данной информационной системе не требуется. При этом полномочия в части защиты информации должны быть распределены между оператором информационной системы и оператором информационно-телекоммуникационной инфраструктуры центра обработки данных.».

13. В пункте 26:

абзац пятый изложить в следующей редакции:

«В информационных системах 1 класса защищенности применяются

сертифицированные средства защиты информации, соответствующие 4 или более высокому уровню доверия. В информационных системах 2 класса защищенности применяются сертифицированные средства защиты информации, соответствующие 5 или более высокому уровню доверия. В информационных системах 3 класса защищенности применяются сертифицированные средства защиты информации, соответствующие 6 или более высокому уровню доверия.»;

абзац шестой после слов «Классы защиты» дополнить словами «и уровни доверия».

14. Дополнить пунктом 26.1 следующего содержания:

«26.1. При проектировании вновь создаваемых или модернизируемых информационных систем, имеющих доступ к информационно-телекоммуникационной сети «Интернет», должны выбираться маршрутизаторы[2], сертифицированные на соответствие требованиям по безопасности информации (в части реализованных в них функций безопасности).».

---

[2] Пункт 4 главы II Классификации средств программного, технического обеспечения, работ и услуг (приложение № 2 к Методическим указаниям по осуществлению учета информационных систем и компонентов информационно-телекоммуникационной инфраструктуры, утвержденным приказом Минкомсвязи России от 31 мая 2013 г. № 127).