Приказ ФСТЭК России от 11.02.2013 N 17
(ред. от 28.05.2019)
"Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"
(Зарегистрировано в Минюсте России 31.05.2013 N 28608)
(с изм. и доп., вступ. в силу с 01.01.2021)

Источник публикации
В данном виде документ опубликован не был.
Первоначальный текст документа опубликован в издании
"Российская газета", N 136, 26.06.2013.
Информацию о публикации документов, создающих данную редакцию, см. в справке к этим документам.

Примечание к документу
Начало действия редакции - 01.01.2021.

Изменения, внесенные Приказом ФСТЭК России от 28.05.2019 N 106 (ред. от 27.04.2020), вступают в силу с 1 января 2021 года, за исключением изменений, которые вступили в силу по истечении 10 дней после дня официального опубликования (опубликован на Официальном интернет-портале правовой информации http://www.pravo.gov.ru - 16.09.2019).

Название документа
Приказ ФСТЭК России от 11.02.2013 N 17
(ред. от 28.05.2019)
"Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"
(Зарегистрировано в Минюсте России 31.05.2013 N 28608)
(с изм. и доп., вступ. в силу с 01.01.2021)

Документ предоставлен КонсультантПлюс
Дата сохранения: 25.01.2021

Зарегистрировано в Минюсте России 31 мая 2013 г. N 28608

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ПРИКАЗ
от 11 февраля 2013 г. N 17

ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ О ЗАЩИТЕ ИНФОРМАЦИИ, НЕ СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Список изменяющих документов
(в ред. Приказов ФСТЭК России от 15.02.2017 N 27,
от 28.05.2019 N 106)

В соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3448; 2010, N 31, ст. 4196; 2011, N 15, ст. 2038; N 30, ст. 4600; 2012, N 31, ст. 4328) и Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. N 1085 (Собрание законодательства Российской Федерации, 2004, N 34, ст. 3541; 2006, N 49, ст. 5192; 2008, N 43, ст. 4921; N 47, ст. 5431; 2012, N 7, ст. 818), приказываю:

1. Утвердить прилагаемые Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

2. Установить, что указанные в пункте 1 настоящего приказа Требования применяются для защиты информации в государственных информационных системах с 1 сентября 2013 г.

Директор
Федеральной службы по техническому
и экспортному контролю
В.СЕЛИН

Утверждены
приказом ФСТЭК России
от 11 февраля 2013 г. N 17

ТРЕБОВАНИЯ О ЗАЩИТЕ ИНФОРМАЦИИ, НЕ СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Список изменяющих документов
(в ред. Приказов ФСТЭК России от 15.02.2017 N 27,
от 28.05.2019 N 106)

I. Общие положения

1. Настоящие Требования разработаны в соответствии с Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3448; 2010, N 31, ст. 4196; 2011, N 15, ст. 2038; N 30, ст. 4600; 2012, N 31, ст. 4328), а также с учетом национальных стандартов Российской Федерации в области защиты информации и в области создания автоматизированных систем (далее - национальные стандарты).

2. В документе устанавливаются требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее - информация), от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней (далее - защита информации) при обработке указанной информации в государственных информационных системах.

Настоящие Требования могут применяться для защиты общедоступной информации, содержащейся в государственных информационных системах, для достижения целей, указанных в пунктах 1 и 3 части 1 статьи 16 Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

В документе не рассматриваются требования о защите информации, связанные с применением криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации.

3. Настоящие Требования являются обязательными при обработке информации в государственных информационных системах, функционирующих на территории Российской Федерации, а также в муниципальных информационных системах, если иное не установлено законодательством Российской Федерации о местном самоуправлении.

Настоящие Требования не распространяются на государственные информационные системы Администрации Президента Российской Федерации, Совета Безопасности Российской Федерации, Федерального Собрания Российской Федерации, Правительства Российской Федерации, Конституционного Суда Российской Федерации, Верховного Суда Российской Федерации и Федеральной службы безопасности Российской Федерации.
(в ред. Приказа ФСТЭК России от 15.02.2017 N 27)

4. Настоящие Требования предназначены для обладателей информации, заказчиков, заключивших государственный контракт на создание государственной информационной системы (далее - заказчики) и операторов государственных информационных систем (далее - операторы).

Лицо, обрабатывающее информацию, являющуюся государственным информационным

ресурсом, по поручению обладателя информации (заказчика) или оператора и (или) предоставляющее им вычислительные ресурсы (мощности) для обработки информации на основании заключенного договора (далее - уполномоченное лицо), обеспечивает защиту информации в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации. В договоре должна быть предусмотрена обязанность уполномоченного лица обеспечивать защиту информации, являющейся государственным информационным ресурсом, в соответствии с настоящими Требованиями.

5. При обработке в государственной информационной системе информации, содержащей персональные данные, настоящие Требования применяются наряду с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 (Собрание законодательства Российской Федерации, 2012, N 45, ст. 6257).

6. По решению обладателя информации (заказчика) или оператора настоящие Требования могут применяться для защиты информации, содержащейся в негосударственных информационных системах.

7. Защита информации, содержащейся в государственной информационной системе (далее - информационная система), обеспечивается путем выполнения обладателем информации (заказчиком) и (или) оператором требований к организации защиты информации, содержащейся в информационной системе, и требований к мерам защиты информации, содержащейся в информационной системе.

II. Требования к организации защиты информации, содержащейся в информационной системе

8. В информационной системе объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

9. Для обеспечения защиты информации, содержащейся в информационной системе, оператором назначается структурное подразделение или должностное лицо (работник), ответственные за защиту информации.

10. Для проведения работ по защите информации в ходе создания и эксплуатации информационной системы обладателем информации (заказчиком) и оператором в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. N 99-ФЗ "О лицензировании отдельных видов деятельности" (Собрание законодательства Российской Федерации, 2011, N 19, ст. 2716; N 30, ст. 4590; N 43, ст. 5971; N 48, ст. 6728; 2012, N 26, ст. 3446; N 31, ст. 4322; 2013, N 9, ст. 874).

11. Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме

обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании" (Собрание законодательства Российской Федерации, 2002, N 52, ст. 5140; 2007, N 19, ст. 2293; N 49, ст. 6070; 2008, N 30, ст. 3616; 2009, N 29, ст. 3626; N 48, ст. 5711; 2010, N 1, ст. 6; 2011, N 30, ст. 4603; N 49, ст. 7025; N 50, ст. 7351; 2012, N 31, ст. 4322; 2012, N 50, ст. 6959).

12. Защита информации, содержащейся в информационной системе, является составной частью работ по созданию и эксплуатации информационной системы и обеспечивается на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках системы (подсистемы) защиты информации информационной системы (далее - система защиты информации информационной системы).
(в ред. Приказа ФСТЭК России от 15.02.2017 N 27)

Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации информационной системы, в зависимости от информации, содержащейся в информационной системе, целей создания информационной системы и задач, решаемых этой информационной системой, должны быть направлены на исключение:

неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);

неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);

неправомерного блокирования информации (обеспечение доступности информации).

13. Для обеспечения защиты информации, содержащейся в информационной системе, проводятся следующие мероприятия:

формирование требований к защите информации, содержащейся в информационной системе;

разработка системы защиты информации информационной системы;

внедрение системы защиты информации информационной системы;

аттестация информационной системы по требованиям защиты информации (далее - аттестация информационной системы) и ввод ее в действие;

обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

Формирование требований к защите информации, содержащейся в информационной системе

14. Формирование требований к защите информации, содержащейся в информационной системе, осуществляется обладателем информации (заказчиком).

Формирование требований к защите информации, содержащейся в информационной системе, осуществляется с учетом ГОСТ Р 51583 "Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения" (далее - ГОСТ Р 51583) и ГОСТ Р 51624 "Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования" (далее - ГОСТ Р 51624) и в том числе включает:

принятие решения о необходимости защиты информации, содержащейся в информационной системе;

классификацию информационной системы по требованиям защиты информации (далее - классификация информационной системы);

определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации;

определение требований к системе защиты информации информационной системы.

14.1. При принятии решения о необходимости защиты информации, содержащейся в информационной системе, осуществляется:

анализ целей создания информационной системы и задач, решаемых этой информационной системой;

определение информации, подлежащей обработке в информационной системе;

анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система;

принятие решения о необходимости создания системы защиты информации информационной системы, а также определение целей и задач защиты информации в информационной системе, основных этапов создания системы защиты информации информационной системы и функций по обеспечению защиты информации, содержащейся в информационной системе, обладателя информации (заказчика), оператора и уполномоченных лиц.

14.2. Классификация информационной системы проводится в зависимости от значимости обрабатываемой в ней информации и масштаба информационной системы (федеральный, региональный, объектовый).

Устанавливаются три класса защищенности информационной системы, определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс - третий, самый высокий - первый. Класс защищенности информационной системы определяется в соответствии с приложением N 1 к настоящим Требованиям.
(в ред. Приказа ФСТЭК России от 15.02.2017 N 27)

Класс защищенности определяется для информационной системы в целом и, при необходимости, для ее отдельных сегментов (составных частей). Требование к классу защищенности включается в техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, разрабатываемые с учетом ГОСТ 34.602 "Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы" (далее - ГОСТ 34.602), ГОСТ Р 51583 и ГОСТ Р 51624.

Класс защищенности информационной системы подлежит пересмотру при изменении масштаба информационной системы или значимости обрабатываемой в ней информации.

Результаты классификации информационной системы оформляются актом классификации.

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.
(абзац введен Приказом ФСТЭК России от 28.05.2019 N 106)

<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. N 127 (зарегистрирован Минюстом России 5 ноября 2013 г., регистрационный N 30318), с учетом изменений, внесенных приказом Минкомсвязи России от 15 июня 2016 г. N 266 (зарегистрирован Минюстом России 14 июля 2016 г., регистрационный N 42853).
(сноска введена Приказом ФСТЭК России от 28.05.2019 N 106)

14.3. Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).
(в ред. Приказа ФСТЭК России от 15.02.2017 N 27)

В качестве исходных данных для определения угроз безопасности информации используется банк данных угроз безопасности информации (bdu.fstec.ru), 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. N 1085 (Собрание законодательства Российской Федерации, 2004, N 34, ст. 3541; 2006, N 49, ст. 5192; 2008, N 43, ст. 4921; N 47, ст. 5431; 2012, N 7, ст. 818; 2013, N 26, ст. 3314; N 53, ст. 7137; 2014, N 36, ст. 4833; N 44, ст. 6041; 2015, N 4, ст. 641; 2016, N 1, ст. 211) (далее - банк данных угроз безопасности информации ФСТЭК России), а также иные источники, содержащие сведения об уязвимостях и угрозах безопасности информации.
(абзац введен Приказом ФСТЭК России от 15.02.2017 N 27)

При определении угроз безопасности информации учитываются

структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования.

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.
(абзац введен Приказом ФСТЭК России от 28.05.2019 N 106)

По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик информационной системы, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Модель угроз безопасности информации должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации применяются 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. N 1085 (Собрание законодательства Российской Федерации, 2004, N 34, ст. 3541; 2006, N 49, ст. 5192; 2008, N 43, ст. 4921; N 47, ст. 5431; 2012, N 7, ст. 818).

14.4. Требования к системе защиты информации информационной системы определяются в зависимости от класса защищенности информационной системы и угроз безопасности информации, включенных в модель угроз безопасности информации.

Требования к системе защиты информации информационной системы включаются в техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, разрабатываемые с учетом ГОСТ 34.602, ГОСТ Р 51583 и ГОСТ Р 51624, и должны в том числе содержать:

цель и задачи обеспечения защиты информации в информационной системе;

класс защищенности информационной системы;

перечень нормативных правовых актов, методических документов и национальных

стандартов, которым должна соответствовать информационная система;

перечень объектов защиты информационной системы;

требования к мерам и средствам защиты информации, применяемым в информационной системе;

стадии (этапы работ) создания системы защиты информационной системы;
(абзац введен Приказом ФСТЭК России от 15.02.2017 N 27)

требования к поставляемым техническим средствам, программному обеспечению, средствам защиты информации;
(абзац введен Приказом ФСТЭК России от 15.02.2017 N 27)

функции заказчика и оператора по обеспечению защиты информации в информационной системе;
(абзац введен Приказом ФСТЭК России от 15.02.2017 N 27)

требования к защите средств и систем, обеспечивающих функционирование информационной системы (обеспечивающей инфраструктуре);
(абзац введен Приказом ФСТЭК России от 15.02.2017 N 27)

требования к защите информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

При определении требований к системе защиты информации информационной системы учитываются положения политик обеспечения информационной безопасности обладателя информации (заказчика), а также политик обеспечения информационной безопасности оператора и уполномоченного лица в части, не противоречащей политикам обладателя информации (заказчика).
(в ред. Приказа ФСТЭК России от 15.02.2017 N 27)

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.
(абзац введен Приказом ФСТЭК России от 28.05.2019 N 106)

Разработка системы защиты информации информационной системы

15. Разработка системы защиты информации информационной системы организуется обладателем информации (заказчиком).

Разработка системы защиты информации информационной системы осуществляется в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным техническим заданием) на создание системы защиты информации

информационной системы с учетом ГОСТ 34.601 "Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания" (далее - ГОСТ 34.601), ГОСТ Р 51583 и ГОСТ Р 51624 и в том числе включает:

проектирование системы защиты информации информационной системы;

разработку эксплуатационной документации на систему защиты информации информационной системы;

макетирование и тестирование системы защиты информации информационной системы (при необходимости).

Система защиты информации информационной системы не должна препятствовать достижению целей создания информационной системы и ее функционированию.

При разработке системы защиты информации информационной системы учитывается ее информационное взаимодействие с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также применение вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

15.1. При проектировании системы защиты информации информационной системы:

определяются типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа);

определяются методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в информационной системе;

выбираются меры защиты информации, подлежащие реализации в системе защиты информации информационной системы;

определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;

определяется структура системы защиты информации информационной системы, включая состав (количество) и места размещения ее элементов;

осуществляется выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности информационной системы;

определяются требования к параметрам настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты

информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации;
(в ред. Приказа ФСТЭК России от 15.02.2017 N 27)

определяются меры защиты информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

Результаты проектирования системы защиты информации информационной системы отражаются в проектной документации (эскизном (техническом) проекте и (или) в рабочей документации) на информационную систему (систему защиты информации информационной системы), разрабатываемых с учетом ГОСТ 34.201 "Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем" (далее - ГОСТ 34.201).

Проектная документация на информационную систему и (или) ее систему защиты информации подлежат согласованию с оператором информационной системы в случае, если он определен таковым в соответствии с законодательством Российской Федерации к моменту окончания проектирования системы защиты информации информационной системы и не является заказчиком данной информационной системы.

При отсутствии необходимых средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, организуется разработка (доработка) средств защиты информации и их сертификация в соответствии с законодательством Российской Федерации или производится корректировка проектных решений по информационной системе и (или) ее системе защиты информации с учетом функциональных возможностей имеющихся сертифицированных средств защиты информации.

При проектировании системы защиты информации информационной системы, функционирование которой предполагается на базе информационно-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.
(абзац введен Приказом ФСТЭК России от 28.05.2019 N 106)

15.2. Разработка эксплуатационной документации на систему защиты информации информационной системы осуществляется в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным техническим заданием) на создание системы защиты информации информационной системы.

Эксплуатационная документация на систему защиты информации информационной системы разрабатывается с учетом ГОСТ 34.601, ГОСТ 34.201 и ГОСТ Р 51624 и должна в том числе содержать описание:

структуры системы защиты информации информационной системы;

состава, мест установки, параметров и порядка настройки средств защиты информации,

программного обеспечения и технических средств;

правил эксплуатации системы защиты информации информационной системы.

15.3. При макетировании и тестировании системы защиты информации информационной системы в том числе осуществляются:

проверка работоспособности и совместимости выбранных средств защиты информации с информационными технологиями и техническими средствами;

проверка выполнения выбранными средствами защиты информации требований к системе защиты информации информационной системы;

корректировка проектных решений, разработанных при создании информационной системы и (или) системы защиты информации информационной системы;

абзац исключен. - Приказ ФСТЭК России от 15.02.2017 N 27.

Макетирование системы защиты информации информационной системы и ее тестирование может проводиться в том числе с использованием средств и методов моделирования информационных систем и технологий виртуализации.

Внедрение системы защиты информации информационной системы

16. Внедрение системы защиты информации информационной системы организуется обладателем информации (заказчиком).

Внедрение системы защиты информации информационной системы осуществляется в соответствии с проектной и эксплуатационной документацией на систему защиты информации информационной системы и в том числе включает:

установку и настройку средств защиты информации в информационной системе;

разработку документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации (далее - организационно-распорядительные документы по защите информации);

внедрение организационных мер защиты информации;

предварительные испытания системы защиты информации информационной системы;

опытную эксплуатацию системы защиты информации информационной системы;

анализ уязвимостей информационной системы и принятие мер защиты информации по их устранению;

приемочные испытания системы защиты информации информационной системы.

К внедрению системы защиты информации информационной системы привлекается

оператор информационной системы в случае, если он определен таковым в соответствии с законодательством Российской Федерации к моменту внедрения системы защиты информации информационной системы и не является заказчиком данной информационной системы.

16.1. Установка и настройка средств защиты информации в информационной системе должна проводиться в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и документацией на средства защиты информации.

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.
(абзац введен Приказом ФСТЭК России от 28.05.2019 N 106)

16.2. Разрабатываемые организационно-распорядительные документы по защите информации должны определять правила и процедуры:

управления (администрирования) системой защиты информации информационной системы;

выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности информации (далее - инциденты), и реагирования на них;

управления конфигурацией аттестованной информационной системы и системы защиты информации информационной системы;

контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;

защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации.

16.3. При внедрении организационных мер защиты информации осуществляются:

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 технических средств и программного обеспечения;

проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов информационной системы по реализации организационных мер защиты информации;

отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации.

16.4. Предварительные испытания системы защиты информации информационной системы проводятся с учетом ГОСТ 34.603 "Информационная технология. Виды испытаний

автоматизированных систем" (далее - ГОСТ 34.603) и включают проверку работоспособности системы защиты информации информационной системы, а также принятие решения о возможности опытной эксплуатации системы защиты информации информационной системы.

16.5. Опытная эксплуатация системы защиты информации информационной системы проводится с учетом ГОСТ 34.603 и включает проверку функционирования системы защиты информации информационной системы, в том числе реализованных мер защиты информации, а также готовность пользователей и администраторов к эксплуатации системы защиты информации информационной системы.

16.6. Анализ уязвимостей информационной системы проводится в целях оценки возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности информации.

Анализ уязвимостей информационной системы включает анализ уязвимостей средств защиты информации, технических средств и программного обеспечения информационной системы.

При анализе уязвимостей информационной системы проверяется отсутствие известных уязвимостей средств защиты информации, технических средств и программного обеспечения, в том числе с учетом информации, имеющейся у разработчиков и полученной из других общедоступных источников, правильность установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректность работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением.

В случае выявления уязвимостей информационной системы, приводящих к возникновению дополнительных угроз безопасности информации, проводится уточнение модели угроз безопасности информации и при необходимости принимаются дополнительные меры защиты информации, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителем выявленных уязвимостей.

По результатам анализа уязвимостей должно быть подтверждено, что в информационной системе отсутствуют уязвимости, содержащиеся в банке данных угроз безопасности информации ФСТЭК России, а также в иных источниках, или их использование (эксплуатация) нарушителем невозможно.
(абзац введен Приказом ФСТЭК России от 15.02.2017 N 27)

16.7. Приемочные испытания системы защиты информации информационной системы проводятся с учетом ГОСТ 34.603 и включают проверку выполнения требований к системе защиты информации информационной системы в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным техническим заданием) на создание системы защиты информации информационной системы.

Аттестация информационной системы и ввод ее в действие

17. Аттестация информационной системы организуется обладателем информации (заказчиком) или оператором и включает проведение комплекса организационных и технических мероприятий (аттестационных испытаний), в результате которых подтверждается соответствие

системы защиты информации информационной системы настоящим Требованиям.

Проведение аттестационных испытаний информационной системы должностными лицами (работниками), осуществляющими проектирование и (или) внедрение системы защиты информации информационной системы, не допускается.
(абзац введен Приказом ФСТЭК России от 15.02.2017 N 27; в ред. Приказа ФСТЭК России от 28.05.2019 N 106)

17.1. В качестве исходных данных, необходимых для аттестации информационной системы, используются модель угроз безопасности информации, акт классификации информационной системы, техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, проектная и эксплуатационная документация на систему защиты информации информационной системы, организационно-распорядительные документы по защите информации, результаты анализа уязвимостей информационной системы, материалы предварительных и приемочных испытаний системы защиты информации информационной системы, а также иные документы, разрабатываемые в соответствии с настоящими Требованиями.

17.2. Аттестация информационной системы проводится в соответствии с программой и методиками аттестационных испытаний до начала обработки информации, подлежащей защите в информационной системе. Для проведения аттестации информационной системы применяются национальные стандарты, а также 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. N 1085.

По решению заказчика (оператора) аттестационные испытания могут быть совмещены с проведением приемочных испытаний информационной системы.
(абзац введен Приказом ФСТЭК России от 28.05.2019 N 106)

По результатам аттестационных испытаний оформляются протоколы аттестационных испытаний, заключение о соответствии информационной системы требованиям о защите информации и аттестат соответствия в случае положительных результатов аттестационных испытаний.

При проведении аттестационных испытаний должны применяться следующие методы проверок (испытаний):
(абзац введен Приказом ФСТЭК России от 15.02.2017 N 27)

экспертно-документальный метод, предусматривающий проверку соответствия системы защиты информации информационной системы установленным требованиям по защите информации, на основе оценки эксплуатационной документации, организационно-распорядительных документов по защите информации, а также условий функционирования информационной системы;
(абзац введен Приказом ФСТЭК России от 15.02.2017 N 27)

анализ уязвимостей информационной системы, в том числе вызванных неправильной настройкой (конфигурированием) программного обеспечения и средств защиты информации;

(абзац введен Приказом ФСТЭК России от 15.02.2017 N 27)

испытания системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) к информационной системе в обход ее системы защиты информации.
(абзац введен Приказом ФСТЭК России от 15.02.2017 N 27)

17.3. Допускается аттестация информационной системы на основе результатов аттестационных испытаний выделенного набора сегментов информационной системы, реализующих полную технологию обработки информации.

В этом случае распространение аттестата соответствия на другие сегменты информационной системы осуществляется при условии их соответствия сегментам информационной системы, прошедшим аттестационные испытания.

Сегмент считается соответствующим сегменту информационной системы, в отношении которого были проведены аттестационные испытания, если для указанных сегментов установлены одинаковые классы защищенности, угрозы безопасности информации, реализованы одинаковые проектные решения по информационной системе и ее системе защиты информации.

Соответствие сегмента, на который распространяется аттестат соответствия, сегменту информационной системы, в отношении которого были проведены аттестационные испытания, подтверждается в ходе приемочных испытаний информационной системы или сегментов информационной системы.

В сегментах информационной системы, на которые распространяется аттестат соответствия, оператором обеспечивается соблюдение эксплуатационной документации на систему защиты информации информационной системы и организационно-распорядительных документов по защите информации.

Особенности аттестации информационной системы на основе результатов аттестационных испытаний выделенного набора ее сегментов, а также условия и порядок распространения аттестата соответствия на другие сегменты информационной системы определяются в программе и методиках аттестационных испытаний, заключении и аттестате соответствия.

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.
(п. 17.4 в ред. Приказа ФСТЭК России от 28.05.2019 N 106)

17.5. Ввод в действие информационной системы осуществляется в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации и с учетом ГОСТ 34.601 и при наличии аттестата соответствия.

17.6. Информационные системы, функционирующие на базе общей инфраструктуры (средств вычислительной техники, серверов телекоммуникационного оборудования) в качестве прикладных сервисов, подлежат аттестации в составе указанной инфраструктуры.

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.
(в ред. Приказа ФСТЭК России от 28.05.2019 N 106)

При аттестации информационной системы должны используются результаты аттестации общей инфраструктуры оператора информационной системы.
(п. 17.6 введен Приказом ФСТЭК России от 15.02.2017 N 27)

Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы

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.
(п. 18 в ред. Приказа ФСТЭК России от 28.05.2019 N 106)

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.
(п. 18.1 в ред. Приказа ФСТЭК России от 28.05.2019 N 106)

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.
(п. 18.2 в ред. Приказа ФСТЭК России от 28.05.2019 N 106)

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.
(п. 18.3 в ред. Приказа ФСТЭК России от 28.05.2019 N 106)

18.4. В ходе управления конфигурацией информационной системы 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.
(п. 18.4 в ред. Приказа ФСТЭК России от 28.05.2019 N 106)

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.
(п. 18.5 введен Приказом ФСТЭК России от 28.05.2019 N 106)

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.
(п. 18.6 введен Приказом ФСТЭК России от 28.05.2019 N 106)

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.
(п. 18.7 введен Приказом ФСТЭК России от 28.05.2019 N 106)

Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации

19. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и организационно-распорядительными документами по защите информации и в том числе включает:

архивирование информации, содержащейся в информационной системе;

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

19.1. Архивирование информации, содержащейся в информационной системе, должно осуществляться при необходимости дальнейшего использования информации в деятельности оператора.

19.2. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю информационной системы или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей информации.

III. Требования к мерам защиты информации, содержащейся в информационной системе

20. Организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать:

идентификацию и аутентификацию субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защиту машинных носителей информации;

регистрацию событий безопасности;

антивирусную защиту;

обнаружение (предотвращение) вторжений;

контроль (анализ) защищенности информации;

целостность информационной системы и информации;

доступность информации;

защиту среды виртуализации;

защиту технических средств;

защиту информационной системы, ее средств, систем связи и передачи данных.

Состав мер защиты информации и их базовые наборы для соответствующих классов защищенности информационных систем приведены в приложении N 2 к настоящим Требованиям.

20.1. Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

20.2. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

20.3. Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

20.4. Меры по защите машинных носителей информации (средства обработки (хранения) информации, съемные машинные носители информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации.

20.5. Меры по регистрации событий безопасности должны обеспечивать сбор, запись,

хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

20.6. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

20.7. Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

20.8. Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

20.9. Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

20.10. Меры по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в информационной системе, в штатном режиме функционирования информационной системы.

20.11. Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

20.12. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

20.13. Меры по защите информационной системы, ее средств, систем связи и передачи

данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

21. Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации включает:

определение базового набора мер защиты информации для установленного класса защищенности информационной системы в соответствии с базовыми наборами мер защиты информации, приведенными в приложении N 2 к настоящим Требованиям;

адаптацию базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы, информационным технологиям, особенностям функционирования информационной системы (в том числе предусматривающую исключение из базового набора мер защиты информации мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);

уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации, приведенных в приложении N 2 к настоящим Требованиям, в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации, включенных в модель угроз безопасности информации;

дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты персональных данных.

Для выбора мер защиты информации для соответствующего класса защищенности информационной системы применяются 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. N 1085.

22. В информационной системе соответствующего класса защищенности в рамках ее системы защиты информации должны быть реализованы меры защиты информации, выбранные в соответствии с пунктом 21 настоящих Требований и обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации.

При этом в информационной системе должен быть, как минимум, реализован адаптированный базовый набор мер защиты информации, соответствующий установленному классу защищенности информационной системы.

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.
(п. 22.1 введен Приказом ФСТЭК России от 28.05.2019 N 106)

23. При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

В этом случае в ходе разработки системы защиты информации информационной системы должно быть проведено обоснование применения компенсирующих мер защиты информации, а при аттестационных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

24. Меры защиты информации выбираются и реализуются в информационной системе в рамках ее системы защиты информации 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 и облачных вычислений.

25. Организационные меры и средства защиты информации, применяемые в информационной системе, должны обеспечивать:

в информационных системах 1 класса защищенности - защиту от угроз безопасности информации, связанных с действиями нарушителей с высоким потенциалом;

в информационных системах 2 класса защищенности - защиту от угроз безопасности информации, связанных с действиями нарушителей с потенциалом не ниже усиленного базового;

в информационных системах 3 класса защищенности - защиту от угроз безопасности информации, связанных с действиями нарушителей с потенциалом не ниже базового.

Потенциал нарушителей определяется в ходе оценки их возможностей, проводимой при определении угроз безопасности информации в соответствии с пунктом 14.3 настоящих Требований.

Оператором может быть принято решение о применении в информационной системе соответствующего класса защищенности мер защиты информации, обеспечивающих защиту от угроз безопасности информации, реализуемых нарушителями с более высоким потенциалом.
(п. 25 в ред. Приказа ФСТЭК России от 15.02.2017 N 27)

26. Технические меры защиты информации реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности. При этом:

в информационных системах 1 класса защищенности применяются средства защиты информации не ниже 4 класса, а также средства вычислительной техники не ниже 5 класса;

в информационных системах 2 класса защищенности применяются средства защиты информации не ниже 5 класса, а также средства вычислительной техники не ниже 5 класса;

в информационных системах 3 класса защищенности применяются средства защиты информации 6 класса, а также средства вычислительной техники не ниже 5 класса.

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.
(в ред. Приказа ФСТЭК России от 28.05.2019 N 106)

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. N 1085.
(в ред. Приказа ФСТЭК России от 28.05.2019 N 106)

В информационных системах применяются средства защиты информации, сертифицированные на соответствие обязательным требованиям по безопасности информации, установленным ФСТЭК России, или на соответствие требованиям, указанным в технических условиях (заданиях по безопасности). При этом функции безопасности таких средств должны обеспечивать выполнение настоящих Требований.
(п. 26 в ред. Приказа ФСТЭК России от 15.02.2017 N 27)

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).
(п. 26.1 введен Приказом ФСТЭК России от 28.05.2019 N 106)

<2> Пункт 4 главы II Классификации средств программного, технического обеспечения, работ и услуг (приложение N 2 к Методическим указаниям по осуществлению учета информационных систем и компонентов информационно-телекоммуникационной инфраструктуры, утвержденным приказом Минкомсвязи России от 31 мая 2013 г. N 127).
(сноска введена Приказом ФСТЭК России от 28.05.2019 N 106)

27. В случае обработки в информационной системе информации, содержащей персональные данные, реализуемые в соответствии с пунктами 21 и 22 настоящих Требований меры защиты информации:

для информационной системы 1 класса защищенности обеспечивают 1, 2, 3 и 4 уровни защищенности персональных данных <1>;

<1> Устанавливается в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119.

для информационной системы 2 класса защищенности обеспечивают 2, 3 и 4 уровни защищенности персональных данных <*>;

для информационной системы 3 класса защищенности обеспечивают 3 и 4 уровни защищенности персональных данных <*>;

абзац исключен. - Приказ ФСТЭК России от 15.02.2017 N 27.

28. При использовании в информационных системах новых информационных технологий и выявлении дополнительных угроз безопасности информации, для которых не определены меры защиты информации, должны разрабатываться компенсирующие меры в соответствии с пунктом 23 настоящих Требований.

Приложение N 1
к Требованиям о защите информации,
не составляющей государственную тайну,
содержащейся в государственных
информационных системах

ОПРЕДЕЛЕНИЕ КЛАССА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Список изменяющих документов
(в ред. Приказа ФСТЭК России от 15.02.2017 N 27)

1. Класс защищенности информационной системы (первый класс (К1), второй класс (К2), третий класс (К3)) определяется в зависимости от уровня значимости информации (УЗ), обрабатываемой в этой информационной системе, и масштаба информационной системы (федеральный, региональный, объектовый).
(в ред. Приказа ФСТЭК России от 15.02.2017 N 27)

Класс защищенности (К) = [уровень значимости информации; масштаб системы].

2. Уровень значимости информации определяется степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности

(неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации.

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)],

где степень возможного ущерба определяется обладателем информации (заказчиком) и (или) оператором самостоятельно экспертным или иными методами и может быть:

высокой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции;

средней, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций;

низкой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

Информация имеет высокий уровень значимости (УЗ 1), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба. Информация имеет средний уровень значимости (УЗ 2), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба. Информация имеет низкий уровень значимости (УЗ 3), если для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определены низкие степени ущерба.

Абзац исключен. - Приказ ФСТЭК России от 15.02.2017 N 27.

При обработке в информационной системе двух и более видов информации (служебная тайна, налоговая тайна и иные установленные законодательством Российской Федерации виды информации ограниченного доступа) уровень значимости информации (УЗ) определятся отдельно для каждого вида информации. Итоговый уровень значимости информации, обрабатываемой в информационной системе, устанавливается по наивысшим значениям степени возможного ущерба, определенным для конфиденциальности, целостности, доступности информации каждого вида информации.

3. Информационная система имеет федеральный масштаб, если она функционирует на территории Российской Федерации (в пределах федерального округа) и имеет сегменты в субъектах Российской Федерации, муниципальных образованиях и (или) организациях.

Информационная система имеет региональный масштаб, если она функционирует на территории субъекта Российской Федерации и имеет сегменты в одном или нескольких муниципальных образованиях и (или) подведомственных и иных организациях.

Информационная система имеет объектовый масштаб, если она функционирует на объектах одного федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, муниципального образования и (или) организации и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях.

4. Класс защищенности информационной системы определяется в соответствии с таблицей:

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ 1	К1	К1	К1
УЗ 2	К1	К2	К2
УЗ 3	К2	К3	К3

(таблица в ред. Приказа ФСТЭК России от 15.02.2017 N 27)

Приложение N 2
к Требованиям о защите информации,
не составляющей государственную тайну,
содержащейся в государственных
информационных системах

СОСТАВ
МЕР ЗАЩИТЫ ИНФОРМАЦИИ И ИХ БАЗОВЫЕ НАБОРЫ ДЛЯ СООТВЕТСТВУЮЩЕГО КЛАССА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Список изменяющих документов
(в ред. Приказа ФСТЭК России от 15.02.2017 N 27)

Условное	Меры защиты информации в информационных	Классы

обозначение и номер меры	системах	защищенности информационной системы		
		3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)				
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных		+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+
ИАФ.7	Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа			
II. Управление доступом субъектов доступа к объектам доступа (УПД)				
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+	+
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные	+	+	+

	способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами			
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	+	+
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	+
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации			
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему			
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы			+
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	+	+	+
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	+	+	+
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки			
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+	+	+
УПД.14	Регламентация и контроль использования в	+	+	+

	информационной системе технологий беспроводного доступа			
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	+
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	+	+
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники		+	+
III. Ограничение программной среды (ОПС)				
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения			+
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения		+	+
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	+	+	+
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов			
IV. Защита машинных носителей информации (ЗНИ)				
ЗНИ.1	Учет машинных носителей информации	+	+	+
ЗНИ.2	Управление доступом к машинным носителям информации	+	+	+
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны			
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием информации,			

	хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах			
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации		+	+
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации			
ЗНИ.7	Контроль подключения машинных носителей информации			
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)	+	+	+
V. Регистрация событий безопасности (РСБ)				
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти	+	+	+
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	+	+	+
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	+	+	+
РСБ.7	Защита информации о событиях безопасности	+	+	+
РСБ.8	Обеспечение возможности просмотра и анализа			

	информации о действиях отдельных пользователей в информационной системе			
VI. Антивирусная защита (АВЗ)				
АВЗ.1	Реализация антивирусной защиты	+	+	+
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+
VII. Обнаружение вторжений (СОВ)				
СОВ.1	Обнаружение вторжений		+	+
СОВ.2	Обновление базы решающих правил		+	+
VIII. Контроль (анализ) защищенности информации (АНЗ)				
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	+	+	+
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	+	+	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	+	+	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе	+	+	+
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)				
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации		+	+
ОЦЛ.2	Контроль целостности информации, содержащейся в базах данных информационной системы			

ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	+	+	+
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)		+	+
ОЦЛ.5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы			
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему			+
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему			
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях			
X. Обеспечение доступности информации (ОДТ)				
ОДТ.1	Использование отказоустойчивых технических средств			+
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы			+
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование		+	+
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители		+	+

	информации			
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала		+	+
ОДТ.6	Кластеризация информационной системы и (или) ее сегментов			
ОДТ.7	Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации		+	+
XI. Защита среды виртуализации (ЗСВ)				
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+	+
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	+	+	+
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры		+	+
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией			
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных		+	+
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций		+	+
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры		+	+

ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	+	+	+
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей	+	+	+
XII. Защита технических средств (ЗТС)				
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам			
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования	+	+	+
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены	+	+	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)			+
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)				
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке		+	+

	информации и иных функций информационной системы			
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом			
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	+	+	+
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)			
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	+	+	+
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационными системами			
ЗИС.7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода		+	+
ЗИС.8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи		+	+
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в		+	+

	том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации			
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам			
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов		+	+
ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю		+	+
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя		+	+
ЗИС.14	Использование устройств терминального доступа для обработки информации			
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации		+	+
ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов			
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы		+	+
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения			
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти			

ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	+	+	+
ЗИС.21	Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы			+
ЗИС.22	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы		+	+
ЗИС.23	Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями		+	+
ЗИС.24	Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения		+	+
ЗИС.25	Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды)			
ЗИС.26	Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем			
ЗИС.27	Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации			
ЗИС.28	Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы			

Документ предоставлен КонсультантПлюс
Дата сохранения: 25.01.2021

ЗИС.29	Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы			
ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе	+	+	+

"+" - мера защиты информации включена в базовый набор мер для соответствующего класса защищенности информационной системы.

Меры защиты информации, не обозначенные знаком "+", применяются при адаптации базового набора мер и уточнении адаптированного базового набора мер, а также при разработке компенсирующих мер защиты информации в информационной системе соответствующего класса защищенности.