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**

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](#Par30) о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

2. Установить, что указанные в [пункте 1](#Par14) настоящего приказа [Требования](#Par30) 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**

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, Высшего Арбитражного Суда Российской Федерации и Федеральной службы безопасности Российской Федерации.

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 и в ходе 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).

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 четыре класса защищенности информационной системы, определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс - четвертый, самый высокий - первый. Класс защищенности информационной системы определяется в соответствии с [приложением N 1](#Par313) к настоящим Требованиям.

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.

14.3. Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) 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).

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.

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;

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) в случае их разработки по ГОСТ Р ИСО/МЭК 27001 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования", а также политик обеспечения информационной безопасности оператора и уполномоченного лица в части, не противоречащей политикам обладателя информации (заказчика).

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 параметры 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;

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.

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;

корректировка проектной и эксплуатационной документации на систему защиты информации информационной системы.

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.

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.

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.

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 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.

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. Повторная аттестация информационной системы осуществляется в случае окончания срока действия аттестата соответствия или повышения класса защищенности информационной системы. При увеличении состава угроз безопасности информации или изменения проектных решений, реализованных при создании системы защиты информации информационной системы, проводятся дополнительные аттестационные испытания в рамках действующего аттестата соответствия.

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.

Обеспечение защиты информации в ходе эксплуатации

аттестованной информационной системы

18. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты информации и организационно-распорядительными документами по защите информации и в том числе включает:

управление (администрирование) системой защиты информации информационной системы;

выявление инцидентов и реагирование на них;

управление конфигурацией аттестованной информационной системы и ее системы защиты информации;

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

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

заведение и удаление учетных записей пользователей, управление полномочиями пользователей информационной системы и поддержание правил разграничения доступа в информационной системе;

управление средствами защиты информации в информационной системе, в том числе параметрами настройки программного обеспечения, включая программное обеспечение средств защиты информации, управление учетными записями пользователей, восстановление работоспособности средств защиты информации, генерацию, смену и восстановление паролей;

установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации или по их поручению;

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

регистрация и анализ событий в информационной системе, связанных с защитой информации (далее - события безопасности);

информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации информационной системы и отдельных средств защиты информации, а также их обучение;

сопровождение функционирования системы защиты информации информационной системы в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации;

18.2. В ходе выявления инцидентов и реагирования на них осуществляются:

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

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

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.

18.3. В ходе управления конфигурацией аттестованной информационной системы и ее системы защиты информации осуществляются:

поддержание конфигурации информационной системы и ее системы защиты информации (структуры системы защиты информации информационной системы, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации информационной системы и ее системы защиты информации);

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

управление изменениями базовой конфигурации информационной системы и ее системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации информационной системы и ее системы защиты информации, санкционирование внесения изменений в базовую конфигурацию информационной системы и ее системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации, сохранение данных об изменениях базовой конфигурации информационной системы и ее системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации;

анализ потенциального воздействия планируемых изменений в базовой конфигурации информационной системы и ее системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность информационной системы;

определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию информационной системы и ее системы защиты информации;

внесение информации (данных) об изменениях в базовой конфигурации информационной системы и ее системы защиты информации в эксплуатационную документацию на систему защиты информации информационной системы;

принятие решения по результатам управления конфигурацией о повторной аттестации информационной системы или проведении дополнительных аттестационных испытаний.

18.4. В ходе контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе, осуществляются:

контроль за событиями безопасности и действиями пользователей в информационной системе;

контроль (анализ) защищенности информации, содержащейся в информационной системе;

анализ и оценка функционирования системы защиты информации информационной системы, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации информационной системы;

периодический анализ изменения угроз безопасности информации в информационной системе, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;

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

принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) системы защиты информации информационной системы, повторной аттестации информационной системы или проведении дополнительных аттестационных испытаний.

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](#Par359) 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](#Par359) 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](#Par359) 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](#Par262) 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.

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. Выбранные и реализованные в информационной системе в рамках ее системы защиты информации меры защиты информации должны обеспечивать:

в информационных системах 1 класса защищенности - нейтрализацию (блокирование) угроз безопасности информации, связанных с действиями нарушителя с высоким потенциалом;

в информационных системах 2 класса защищенности - нейтрализацию (блокирование) угроз безопасности информации, связанных с действиями нарушителя с потенциалом не ниже среднего;

в информационных системах 3 и 4 классов защищенности - нейтрализацию (блокирование) угроз безопасности информации, связанных с действиями нарушителя с низким потенциалом.

Потенциал нарушителя определяется в ходе оценки его возможностей, проводимой при определении угроз безопасности информации в соответствии с [пунктом 14.3](#Par87) 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 нарушителем с более высоким потенциалом.

26. Технические меры защиты информации реализуются посредством применения средств защиты информации, имеющих необходимые функции безопасности.

В этом случае в информационных системах 1 и 2 класса защищенности применяются:

средства вычислительной техники не ниже 5 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса;

межсетевые экраны не ниже 3 класса в случае взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 4 класса в случае отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена.

В информационных системах 3 класса защищенности применяются:

средства вычислительной техники не ниже 5 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса в случае взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 5 класса в случае отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

межсетевые экраны не ниже 3 класса в случае взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 4 класса в случае отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена.

В информационных системах 4 класса защищенности применяются:

средства вычислительной техники не ниже 5 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса;

межсетевые экраны не ниже 4 класса.

В информационных системах 1 и 2 классов защищенности применяются средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.

27. В случае обработки в информационной системе информации, содержащей персональные данные, реализуемые в соответствии с [пунктами 21](#Par262) и [22](#Par268) 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 <\*>;

для информационной системы 4 класса защищенности, обеспечивают 4 уровень защищенности персональных данных <\*>.

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](#Par270) настоящих Требований.

Приложение N 1

к Требованиям о защите информации,

не составляющей государственную тайну,

содержащейся в государственных

информационных системах

ОПРЕДЕЛЕНИЕ КЛАССА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

1. Класс защищенности информационной системы (первый класс (К1), второй класс (К2), третий класс (К3), четвертый класс (К4)) определяется в зависимости от уровня значимости информации (УЗ), обрабатываемой в этой информационной системе, и масштаба информационной системы (федеральный, региональный, объектовый).

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.

Информация имеет минимальный уровень значимости (УЗ 4), если обладателем информации (заказчиком) и (или) оператором степень ущерба от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности) не может быть определена, но при этом информация подлежит защите в соответствии с законодательством Российской Федерации.

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  |
|  УЗ 4  |  К3  |  К3  |  К4  |

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

|  |  |  |
| --- | --- | --- |
| Услов- ное обозна-чение иномер меры  |  Меры защиты информации в информационных  системах  |  Классы  защищенности  информационной  системы  |
|  4  |  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 томчисле стационарных, мобильных и портативных  |  |  |  +  |  +  |
|  ИАФ.3  | Управление идентификаторами, в том числесоздание, присвоение, уничтожениеидентификаторов  |  +  |  +  |  +  |  +  |
|  ИАФ.4  | Управление средствами аутентификации, в томчисле хранение, выдача, инициализация,блокирование средств аутентификации и принятиемер в случае утраты и (или) компрометациисредств аутентификации  |  +  |  +  |  +  |  +  |
|  ИАФ.5  | Защита обратной связи при вводеаутентификационной информации  |  +  |  +  |  +  |  +  |
|  ИАФ.6  | Идентификация и аутентификация пользователей,не являющихся работниками оператора (внешнихпользователей)  |  +  |  +  |  +  |  +  |
|  ИАФ.7  | Идентификация и аутентификация объектовфайловой системы, запускаемых и исполняемыхмодулей, объектов систем управления базамиданных, объектов, создаваемых прикладным испециальным программным обеспечением, иныхобъектов доступа  |  |  |  |  |
|  II. Управление доступом  субъектов доступа к объектам доступа (УПД)  |
|  УПД.1  | Управление (заведение, активация, блокированиеи 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) иправил разграничения доступа  |  +  |  +  |  +  |  +  |
|  УПД.3  | Управление (фильтрация, маршрутизация, контрольсоединений, однонаправленная передача и иныеспособы управления) информационными потокамимежду устройствами, сегментами информационнойсистемы, а также между информационнымисистемами  |  |  |  +  |  +  |
|  УПД.4  | Разделение полномочий (ролей) пользователей,администраторов и лиц, обеспечивающихфункционирование информационной системы  |  |  +  |  +  |  +  |
|  УПД.5  | Назначение минимально необходимых прав ипривилегий пользователям, администраторам илицам, обеспечивающим функционированиеинформационной системы  |  |  +  |  +  |  +  |
|  УПД.6  | Ограничение неуспешных попыток входа винформационную систему (доступа кинформационной системе)  |  +  |  +  |  +  |  +  |
|  УПД.7  | Предупреждение пользователя при его входе винформационную систему о том, что винформационной системе реализованы меры защитыинформации, и о необходимости соблюдения имустановленных оператором правил обработкиинформации  |  |  |  |  |
|  УПД.8  | Оповещение пользователя после успешного входа винформационную систему о его предыдущем входе винформационную систему  |  |  |  |  |
|  УПД.9  | Ограничение числа параллельных сеансов доступадля каждой учетной записи пользователяинформационной системы  |  |  |  |  +  |
| УПД.10  | Блокирование сеанса доступа в информационнуюсистему после установленного временибездействия (неактивности) пользователя или поего запросу  |  |  +  |  +  |  +  |
| УПД.11  | Разрешение (запрет) действий пользователей,разрешенных до идентификации и аутентификации  |  +  |  +  |  +  |  +  |
| УПД.12  | Поддержка и сохранение атрибутов безопасности(меток безопасности), связанных с информацией впроцессе ее хранения и обработки  |  |  |  |  |
| УПД.13  | Реализация защищенного удаленного доступасубъектов доступа к объектам доступа черезвнешние информационно-телекоммуникационные сети  |  +  |  +  |  +  |  +  |
| УПД.14  | Регламентация и контроль использования винформационной системе технологий беспроводногодоступа  |  +  |  +  |  +  |  +  |
| УПД.15  | Регламентация и контроль использования винформационной системе мобильных техническихсредств  |  +  |  +  |  +  |  +  |
| УПД.16  | Управление взаимодействием с информационнымисистемами сторонних организаций (внешниеинформационные системы)  |  +  |  +  |  +  |  +  |
| УПД.17  | Обеспечение доверенной загрузки средстввычислительной техники  |  |  |  +  |  +  |
|  III. Ограничение программной среды (ОПС)  |
|  ОПС.1  | Управление запуском (обращениями) компонентовпрограммного обеспечения, в том числеопределение запускаемых компонентов, настройкапараметров запуска компонентов, контроль зазапуском компонентов программного обеспечения  |  |  |  |  +  |
|  ОПС.2  | Управление установкой (инсталляцией)компонентов программного обеспечения, в томчисле определение компонентов, подлежащихустановке, настройка параметров установкикомпонентов, контроль за установкой компонентовпрограммного обеспечения  |  |  |  +  |  +  |
|  ОПС.3  | Установка (инсталляция) только разрешенного киспользованию программного обеспечения и (или)его компонентов  |  +  |  +  |  +  |  +  |
|  ОПС.4  | Управление временными файлами, в том числезапрет, разрешение, перенаправление записи,удаление временных файлов  |  |  |  |  |
|  IV. Защита машинных носителей информации (ЗНИ)  |
|  ЗНИ.1  | Учет машинных носителей информации  |  +  |  +  |  +  |  +  |
|  ЗНИ.2  | Управление доступом к машинным носителяминформации  |  +  |  +  |  +  |  +  |
|  ЗНИ.3  | Контроль перемещения машинных носителейинформации за пределы контролируемой зоны  |  |  |  |  |
|  ЗНИ.4  | Исключение возможности несанкционированногоознакомления с содержанием информации,хранящейся на машинных носителях, и (или)использования носителей информации в иныхинформационных системах  |  |  |  |  |
|  ЗНИ.5  | Контроль использования интерфейсов ввода(вывода) информации на машинные носителиинформации  |  |  |  +  |  +  |
|  ЗНИ.6  | Контроль ввода (вывода) информации на машинныеносители информации  |  |  |  |  |
|  ЗНИ.7  | Контроль подключения машинных носителейинформации  |  |  |  |  |
|  ЗНИ.8  | Уничтожение (стирание) информации на машинныхносителях при их передаче между пользователями,в сторонние организации для ремонта илиутилизации, а также контроль уничтожения(стирания)  |  +  |  +  |  +  |  +  |
|  V. Регистрация событий безопасности (РСБ)  |
|  РСБ.1  | Определение событий безопасности, подлежащихрегистрации, и сроков их хранения  |  +  |  +  |  +  |  +  |
|  РСБ.2  | Определение состава и содержания информации особытиях безопасности, подлежащих регистрации  |  +  |  +  |  +  |  +  |
|  РСБ.3  | Сбор, запись и хранение информации о событияхбезопасности в течение установленного временихранения  |  +  |  +  |  +  |  +  |
|  РСБ.4  | Реагирование на сбои при регистрации событийбезопасности, в том числе аппаратные ипрограммные ошибки, сбои в механизмах сбораинформации и достижение предела илипереполнения объема (емкости) памяти  |  +  |  +  |  +  |  +  |
|  РСБ.5  | Мониторинг (просмотр, анализ) результатоврегистрации событий безопасности и реагированиена них  |  +  |  +  |  +  |  +  |
|  РСБ.6  | Генерирование временных меток и (или)синхронизация системного времени винформационной системе  |  +  |  +  |  +  |  +  |
|  РСБ.7  | Защита информации о событиях безопасности  |  +  |  +  |  +  |  +  |
|  РСБ.8  | Обеспечение возможности просмотра и анализаинформации о действиях отдельных пользователейв информационной системе  |  |  |  |  |
|  VI. Антивирусная защита (АВЗ)  |
|  АВЗ.1  | Реализация антивирусной защиты  |  +  |  +  |  +  |  +  |
|  АВЗ.2  | Обновление базы данных признаков вредоносныхкомпьютерных 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 информационнойсистемы и оперативное устранение вновьвыявленных уязвимостей  |  |  +  |  +  |  +  |
|  АНЗ.2  | Контроль установки обновлений программногообеспечения, включая обновление программногообеспечения средств защиты информации  |  +  |  +  |  +  |  +  |
|  АНЗ.3  | Контроль работоспособности, параметровнастройки и правильности функционированияпрограммного обеспечения и средств защитыинформации  |  |  +  |  +  |  +  |
|  АНЗ.4  | Контроль состава технических средств,программного обеспечения и средств защитыинформации  |  |  +  |  +  |  +  |
|  АНЗ.5  | Контроль правил генерации и смены паролейпользователей, заведения и удаления учетныхзаписей пользователей, реализации правилразграничения доступом, полномочийпользователей в информационной системе  |  |  +  |  +  |  +  |
|  IX. Обеспечение целостности информационной  системы и информации (ОЦЛ)  |
|  ОЦЛ.1  | Контроль целостности программного обеспечения,включая программное обеспечение средств защитыинформации  |  |  |  +  |  +  |
|  ОЦЛ.2  | Контроль целостности информации, содержащейся вбазах данных информационной системы  |  |  |  |  |
|  ОЦЛ.3  | Обеспечение возможности восстановленияпрограммного обеспечения, включая программноеобеспечение средств защиты информации, привозникновении нештатных ситуаций  |  +  |  +  |  +  |  +  |
|  ОЦЛ.4  | Обнаружение и реагирование на поступление винформационную систему незапрашиваемыхэлектронных сообщений (писем, документов) ииной информации, не относящихся кфункционированию информационной системы (защитаот спама)  |  |  |  +  |  +  |
|  ОЦЛ.5  | Контроль содержания информации, передаваемой изинформационной системы (контейнерный,основанный на свойствах объекта доступа, иконтентный, основанный на поиске запрещенной кпередаче информации с использованием сигнатур,масок и иных методов), и исключениенеправомерной передачи информации изинформационной системы  |  |  |  |  |
|  ОЦЛ.6  | Ограничение прав пользователей по вводуинформации в информационную систему  |  |  |  |  +  |
|  ОЦЛ.7  | Контроль точности, полноты и правильностиданных, вводимых в информационную систему  |  |  |  |  |
|  ОЦЛ.8  | Контроль ошибочных действий пользователей повводу и (или) передаче информации ипредупреждение пользователей об ошибочныхдействиях  |  |  |  |  |
|  X. Обеспечение доступности информации (ОДТ)  |
|  ОДТ.1  | Использование отказоустойчивых техническихсредств  |  |  |  |  +  |
|  ОДТ.2  | Резервирование технических средств,программного обеспечения, каналов передачиинформации, средств обеспеченияфункционирования информационной системы  |  |  |  |  +  |
|  ОДТ.3  | Контроль безотказного функционированиятехнических средств, обнаружение и локализацияотказов функционирования, принятие мер повосстановлению отказавших средств и ихтестирование  |  |  |  +  |  +  |
|  ОДТ.4  | Периодическое резервное копирование информациина резервные машинные носители информации  |  |  |  +  |  +  |
|  ОДТ.5  | Обеспечение возможности восстановленияинформации с резервных машинных носителейинформации (резервных копий) в течениеустановленного временного интервала  |  |  |  +  |  +  |
|  ОДТ.6  | Кластеризация информационной системы и (или) еесегментов  |  |  |  |  |
|  ОДТ.7  | Контроль состояния и качества предоставленияуполномоченным лицом вычислительных ресурсов(мощностей), в том числе по передаче информации  |  |  |  +  |  +  |
|  XI. Защита среды виртуализации (ЗСВ)  |
|  ЗСВ.1  | Идентификация и аутентификация субъектовдоступа и объектов доступа в виртуальнойинфраструктуре, в том числе администраторовуправления средствами виртуализации  |  +  |  +  |  +  |  +  |
|  ЗСВ.2  | Управление доступом субъектов доступа кобъектам доступа в виртуальной инфраструктуре,в том числе внутри виртуальных машин  |  +  |  +  |  +  |  +  |
|  ЗСВ.3  | Регистрация событий безопасности в виртуальнойинфраструктуре  |  |  +  |  +  |  +  |
|  ЗСВ.4  | Управление (фильтрация, маршрутизация, контрольсоединения, однонаправленная передача) потокамиинформации между компонентами виртуальнойинфраструктуры, а также по периметрувиртуальной инфраструктуры  |  |  |  +  |  +  |
|  ЗСВ.5  | Доверенная загрузка серверов виртуализации,виртуальной машины (контейнера), серверовуправления виртуализацией  |  |  |  |  |
|  ЗСВ.6  | Управление перемещением виртуальных машин(контейнеров) и обрабатываемых на них данных  |  |  |  +  |  +  |
|  ЗСВ.7  | Контроль целостности виртуальной инфраструктурыи ее конфигураций  |  |  |  +  |  +  |
|  ЗСВ.8  | Резервное копирование данных, резервированиетехнических средств, программного обеспечениявиртуальной инфраструктуры, а также каналовсвязи внутри виртуальной инфраструктуры  |  |  |  +  |  +  |
|  ЗСВ.9  | Реализация и управление антивирусной защитой ввиртуальной инфраструктуре  |  |  +  |  +  |  +  |
| ЗСВ.10  | Разбиение виртуальной инфраструктуры насегменты (сегментирование виртуальнойинфраструктуры) для обработки информацииотдельным пользователем и (или) группойпользователей  |  |  |  +  |  +  |
|  XII. Защита технических средств (ЗТС)  |
|  ЗТС.1  | Защита информации, обрабатываемой техническимисредствами, от ее утечки по техническим каналам  |  |  |  |  |
|  ЗТС.2  | Организация контролируемой зоны, в пределахкоторой постоянно размещаются стационарныетехнические средства, обрабатывающиеинформацию, и средства защиты информации, атакже средства обеспечения функционирования  |  +  |  +  |  +  |  +  |
|  ЗТС.3  | Контроль и управление физическим доступом ктехническим средствам, средствам защитыинформации, средствам обеспеченияфункционирования, а также в помещения исооружения, в которых они установлены,исключающие несанкционированный физическийдоступ к средствам обработки информации,средствам защиты информации и средствамобеспечения функционирования информационнойсистемы и помещения и сооружения, в которых ониустановлены  |  +  |  +  |  +  |  +  |
|  ЗТС.4  | Размещение устройств вывода (отображения)информации, исключающее ее несанкционированныйпросмотр  |  +  |  +  |  +  |  +  |
|  ЗТС.5  | Защита от внешних воздействий (воздействийокружающей среды, нестабильностиэлектроснабжения, кондиционирования и иныхвнешних факторов)  |  |  |  |  +  |
|  XIII. Защита информационной системы, ее средств,  систем связи и передачи данных (ЗИС)  |
|  ЗИС.1  | Разделение в информационной системе функций поуправлению (администрированию) информационнойсистемой, управлению (администрированию)системой защиты информации, функций пообработке информации и иных функцийинформационной системы  |  |  |  +  |  +  |
|  ЗИС.2  | Предотвращение задержки или прерываниявыполнения процессов с высоким приоритетом состороны процессов с низким приоритетом  |  |  |  |  |
|  ЗИС.3  | Обеспечение защиты информации от раскрытия,модификации и навязывания (ввода ложнойинформации) при ее передаче (подготовке кпередаче) по каналам связи, имеющим выход запределы контролируемой зоны, в том числебеспроводным каналам связи  |  +  |  +  |  +  |  +  |
|  ЗИС.4  | Обеспечение доверенных канала, маршрута междуадминистратором, пользователем и средствамизащиты информации (функциями безопасностисредств защиты информации)  |  |  |  |  |
|  ЗИС.5  | Запрет несанкционированной удаленной активациивидеокамер, микрофонов и иных периферийныхустройств, которые могут активироватьсяудаленно, и оповещение пользователей обактивации таких устройств  |  +  |  +  |  +  |  +  |
|  ЗИС.6  | Передача и контроль целостности атрибутовбезопасности (меток безопасности), связанных синформацией, при обмене информацией с инымиинформационными системами  |  |  |  |  |
|  ЗИС.7  | Контроль санкционированного и исключениенесанкционированного использования технологиймобильного кода, в том числе регистрациясобытий, связанных с использованием технологиймобильного кода, их анализ и реагирование нанарушения, связанные с использованиемтехнологий мобильного кода  |  |  |  +  |  +  |
|  ЗИС.8  | Контроль санкционированного и исключениенесанкционированного использования технологийпередачи речи, в том числе регистрация событий,связанных с использованием технологий передачиречи, их анализ и реагирование на нарушения,связанные с использованием технологий передачиречи  |  |  |  +  |  +  |
|  ЗИС.9  | Контроль санкционированной и исключениенесанкционированной передачи видеоинформации, втом числе регистрация событий, связанных спередачей видеоинформации, их анализ иреагирование на нарушения, связанные спередачей видеоинформации  |  |  |  +  |  +  |
| ЗИС.10  | Подтверждение происхождения источникаинформации, получаемой в процессе определениясетевых адресов по сетевым именам илиопределения сетевых имен по сетевым адресам  |  |  |  |  |
| ЗИС.11  | Обеспечение подлинности сетевых соединений(сеансов взаимодействия), в том числе длязащиты от подмены сетевых устройств и сервисов  |  |  |  +  |  +  |
| ЗИС.12  | Исключение возможности отрицания пользователемфакта отправки информации другому пользователю  |  |  |  +  |  +  |
| ЗИС.13  | Исключение возможности отрицания пользователемфакта получения информации от другогопользователя  |  |  |  +  |  +  |
| ЗИС.14  | Использование устройств терминального доступадля обработки информации  |  |  |  |  |
| ЗИС.15  | Защита архивных файлов, параметров настройкисредств защиты информации и программногообеспечения и иных данных, не подлежащихизменению в процессе обработки информации  |  |  |  +  |  +  |
| ЗИС.16  | Выявление, анализ и блокирование винформационной системе скрытых каналов передачиинформации в обход реализованных мер защитыинформации или внутри разрешенных сетевыхпротоколов  |  |  |  |  |
| ЗИС.17  | Разбиение информационной системы на сегменты(сегментирование информационной системы) иобеспечение защиты периметров сегментовинформационной системы  |  |  |  +  |  +  |
| ЗИС.18  | Обеспечение загрузки и исполнения программногообеспечения с машинных носителей информации,доступных только для чтения, и контрольцелостности данного программного обеспечения  |  |  |  |  |
| ЗИС.19  | Изоляция процессов (выполнение программ) ввыделенной области памяти  |  |  |  |  |
| ЗИС.20  | Защита беспроводных соединений, применяемых винформационной системе  |  |  +  |  +  |  +  |
| ЗИС.21  | Исключение доступа пользователя к информации,возникшей в результате действий предыдущегопользователя через реестры, оперативную память,внешние запоминающие устройства и иные общиедля пользователей ресурсы информационнойсистемы  |  |  |  |  +  |
| ЗИС.22  | Защита информационной системы от угрозбезопасности информации, направленных на отказв обслуживании информационной системы  |  |  |  +  |  +  |
| ЗИС.23  | Защита периметра (физических и (или) логическихграниц) информационной системы при еевзаимодействии с иными информационнымисистемами и информационно-телекоммуникационнымисетями  |  |  |  +  |  +  |
| ЗИС.24  | Прекращение сетевых соединений по их завершенииили по истечении заданного операторомвременного интервала неактивности сетевогосоединения  |  |  |  +  |  +  |
| ЗИС.25  | Использование в информационной системе или еесегментах различных типов общесистемного,прикладного и специального программногообеспечения (создание гетерогенной среды)  |  |  |  |  |
| ЗИС.26  | Использование прикладного и специальногопрограммного обеспечения, имеющих возможностьфункционирования в средах различныхоперационных систем  |  |  |  |  |
| ЗИС.27  | Создание (эмуляция) ложных информационныхсистем или их компонентов, предназначенных дляобнаружения, регистрации и анализа действийнарушителей в процессе реализации угрозбезопасности информации  |  |  |  |  |
| ЗИС.28  | Воспроизведение ложных и (или) скрытие истинныхотдельных информационных технологий и (или)структурно-функциональных характеристикинформационной системы или ее сегментов,обеспечивающее навязывание нарушителю ложногопредставления об истинных информационныхтехнологиях и (или) структурно-функциональныххарактеристиках информационной системы  |  |  |  |  |
| ЗИС.29  | Перевод информационной системы или ее устройств(компонентов) в заранее определеннуюконфигурацию, обеспечивающую защиту информации,в случае возникновении отказов (сбоев) всистеме защиты информации информационнойсистемы  |  |  |  |  |
| 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.