КРЕДО-С

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

Экз. № 1

Утвержден ФСТЭК России
12 апреля 2026 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

СОСТАВ И СОДЕРЖАНИЕ МЕРОПРИЯТИЙ И МЕР ПО ЗАЩИТЕ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

2026

ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий методический документ «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах» (далее – методический документ) разработан в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

1.2. Методический документ определяет общие подходы, состав и содержание мероприятий (процессов) и мер по защите информации, содержащейся в:

информационных системах, автоматизированных системах управления, информационно-телекоммуникационных сетях (далее – информационные системы) государственных органов, государственных унитарных предприятий, государственных учреждений, организаций, в том числе субъектов критической информационной инфраструктуры (далее – органы (организации));

используемых для создания и эксплуатации государственных информационных систем, иных информационных систем государственных органов технических средствах, программах для электронных вычислительных машин и базах данных, доступ к которым предоставляется с использованием информационно-телекоммуникационных сетей, в порядке, установленном Правительством Российской Федерации;

информационно-телекоммуникационных инфраструктурах, выполняющих общие технологические функции и обеспечивающих основу функционирования указанных информационных систем, а также по обеспечению безопасности принадлежащих органам (организациям) значимых объектов критической информационной инфраструктуры.

1.3. Методический документ детализирует мероприятия (процессы), которые подлежат реализации в органе (организации) для достижения целей защиты информации и (или) обеспечения безопасности значимых объектов критической информационной инфраструктуры, а также определяет содержание мер по защите информации (обеспечению безопасности), принимаемых в информационных системах и на значимых объектах критической информационной инфраструктуры (далее – меры по защите информации) в соответствии с требованиями по защите информации (обеспечению безопасности)[1].

---

[1] Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденные приказом ФСТЭК России от 11 апреля 2025 г. № 117.

В методическом документе не рассматриваются содержание, правила выбора и реализации мер по защите информации, связанных с применением криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации. Принятие таких мер защиты информации обеспечивается в соответствии с требованиями, установленными ФСБ России.

1.4. Методический документ предназначен для обладателей информации, заказчиков, заключивших государственный контракт на создание информационных систем (далее – заказчики), операторов информационных систем (далее – операторы), а также организаций, которым на основании договора или иного документа передается информация, предоставляется доступ к информационным системам оператора (обладателя информации) и (или) содержащейся в них информации для оказания услуг, проведения работ по обработке, хранению информации, созданию (развитию), обеспечению эксплуатации информационных систем, а также для выполнения работ, оказания услуг по защите информации (далее – подрядные организации).

1.5. Настоящий методический документ применяется в ходе:

организации в органе (организации) деятельности по защите информации, создания системы защиты информации органа (организации) и управления ею;

создания информационных систем, эксплуатации таких информационных систем и поддержания необходимого уровня защищенности;

оценки эффективности деятельности по защите информации и управления системой защиты информации органа (организации);

аттестации информационных систем на соответствие требованиям по защите информации (обеспечению безопасности), проведения иных форм оценки соответствия информационных систем требованиям по защите информации и достаточности принимаемых мер по защите информации

Требования к обеспечению защиты информации, содержащейся в информационных системах управления производством, используемых предприятиями оборонно-промышленного комплекса, утвержденные приказом ФСТЭК России от 28 февраля 2017 г. № 31.

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239.

Требования к обеспечению защиты информации в автоматизированных системах управления производственными процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом ФСТЭК России от 14 марта 2013 г. № 31.

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом ФСТЭК России от 18 февраля 2013 г. № 21.

(обеспечению безопасности).

1.6. Для целей настоящего методического документа используются термины и определения, установленные национальными стандартами в области защиты информации и обеспечения информационной безопасности, а также термины и определения, приведенные в приложении № 1 к настоящему методическому документу.

1.7. В связи с утверждением настоящего методического документа не применяются положения методического документа «Меры защиты информации в государственных информационных системах», утвержденного ФСТЭК России 11 февраля 2014 г.

II. ФАКТОРЫ, ВЛИЯЮЩИЕ НА СОСТОЯНИЕ ЗАЩИТЫ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

2.1. Повышение уровня цифровой зрелости органов (организаций), усиленная цифровизация производственных, промышленных, бизнес-процессов привела к критической зависимости реализуемых полномочий (функций), проводимых работ (оказываемых услуг) от устойчивости функционирования информационных систем и защищенности содержащейся в них информации. Определение негативных последствий (событий) от нарушения функционирования информационных систем вследствие реализации (возникновения) угроз безопасности информации является необходимым условием эффективной деятельности по защите информации, содержащейся в информационных системах. Таким образом, определяемые в соответствии с требованиями по защите информации (обеспечению безопасности) цели защиты информации, содержащейся в информационных системах, должны предусматривать исключение наступления событий, повлекших возникновение негативных последствий (ущерба). Для определения недопустимых событий используются исходные данные, содержащиеся в банке данных угроз безопасности информации ФСТЭК России.

2.2. Деятельность по защите информации, содержащейся в информационных системах, должна осуществляться непрерывно наряду с основными видами деятельности оператора, для обеспечения которых применяются информационные системы и содержащаяся в них информация. Эффективность защиты информации зависит от реализации оператором мероприятий (процессов) по защите информации.

2.3. Уровень реализации мероприятий (процессов) по защите информации, содержащейся в информационных системах, определяется степенью внедрения каждого мероприятия (процесса), компетенцией специалистов по защите

информации, эффективностью и качеством применяемых ими средств, а также полнотой документирования мероприятий (процессов) по защите информации.

Назначаемые на должности ответственных за защиту информации лица должны обладать соответствующими компетенциями. Кроме того, требуется осуществлять периодическое повышение их квалификации по разным направлениям защиты информации и непрерывное информирование о новых способах реализации угроз безопасности информации, методах и средствах противодействия им.

В случае отсутствия у оператора собственных квалифицированных специалистов целесообразно привлекать к проведению мероприятий (процессов) по защите информации организации, имеющие необходимые лицензии на деятельность в области защиты информации, и квалифицированных специалистов по требуемым направлениям деятельности. При этом требуется однозначное задокументированное разграничение полномочий (функций) и ответственности между работниками заказчика и специалистами привлекаемой для оказания услуг подрядной организации.

2.4. Программные, программно-аппаратные средства, применяемые специалистами по защите информации, должны обеспечивать реализацию мероприятий (процессов) по защите информации и соответствовать требованиям по защите информации (обеспечению безопасности). К таким средствам относятся в том числе средства выявления и анализа угроз безопасности информации, обнаружения и предотвращения вторжений, проведения контроля уровня защищенности информации, мониторинга информационной безопасности информационных систем, выявления уязвимостей, контроля настроек и конфигураций информационных систем, системы, предназначенные для автоматизации и аналитической поддержки деятельности по защите информации. Применяемые специалистами по защите информации средства не должны создавать угрозы безопасности информации.

В случае отсутствия у оператора собственных программных, программно-аппаратных средств или недостаточной квалификации специалистов к проведению мероприятий (процессов) по защите информации следует привлекать организации, имеющие необходимые средства защиты информации, управления и контроля. При этом требуется однозначное задокументированное определение мероприятий (процессов) по защите информации, для которых применяются средства подрядной организации, и порядка их подключения к информационным системам оператора для оказания услуг или их применения.

2.5. Регламенты, стандарты по защите информации, разрабатываемые оператором, должны в соответствии с требованиями по защите информации (обеспечению безопасности) определять порядок реализации мероприятий (процессов) и устанавливать меры по защите информации с учетом особенностей

деятельности органа (организации) и функционирования информационных систем. Регламенты, стандарты по защите информации должны быть направлены на недопущение возникновения организационных и архитектурных уязвимостей.

Эксплуатационная документация разрабатывается на каждую информационную систему и (или) отдельные программные, программно-аппаратные средства.

2.6. При организации деятельности по защите информации и управлении данной деятельностью требуется предусмотреть информирование работников об утвержденных в органе (организации) политике защиты информации и иных документах по защите информации (стандартах, регламентах), содержащих цели защиты информации и требования по защите информации (обеспечению безопасности), а также исключить осуществление полномочий (функций), проведение работ (оказание услуг) без учета требований по защите информации (обеспечению безопасности). Фактором, оказывающим существенное негативное влияние на состояние защиты информации, содержащейся в информационных системах, является отсутствие у оператора персональной ответственности работников, закрепленной в соответствующих должностных регламентах (инструкциях), за нарушение положений политики защиты информации, внутренних стандартов и регламентов по защите информации.

2.7. Защита информации, содержащейся в информационных системах, определяется защищенностью этих информационных систем. Меры по защите информационных систем принимаются на всех стадиях их жизненного цикла: создание, развитие, ввод в эксплуатацию, эксплуатация, вывод из эксплуатации. Защита информационных систем является неотъемлемой частью их создания и эксплуатации. Эффективность защиты информационных систем зависит от закладываемых на этапе создания проектных решений и возможности этих проектных решений за счет специально спроектированной архитектуры информационных систем уменьшить ширину и глубину поверхности компьютерных атак, снижая тем самым возможности нарушителей по реализации угроз безопасности информации.

2.8. Выбор архитектурных решений информационных систем на этапе их проектирования должен осуществляться на основе результатов моделирования угроз безопасности информации и описания поверхности компьютерных атак. Создание информационных систем в защищенном исполнении, в основе которых лежат национальные стандарты конструктивной безопасности, существенно повышают эффективность защиты информационных систем и содержащейся в них информации.

Организационные меры и наложенные средства защиты информации должны быть направлены на блокирование (нейтрализацию) угроз безопасности

информации, сохранивших свою актуальность после применения безопасных архитектурных решений.

2.9. Основными принципами создания информационных систем в защищенном исполнении являются:

дифференциация уровней значимости защищаемых информационных ресурсов в зависимости от их влияния на цели защиты информации и предоставление доступа к ним на основе проверок уровня доступа субъектов доступа;

установление минимальных прав доступа к соответствующему уровню значимости информационных ресурсов;

минимизация интерфейсов информационных систем, доступных для субъектов доступа, в соответствии с функциями информационной системы;

сегментация (микросегментация) информационных систем с учетом уровней значимости защищаемых информационных ресурсов (разбиение на сегменты безопасности) и контроль доступа в выделенные сегменты на основе уровня доступа субъектов доступа;

регистрация и анализ действий субъектов при доступе к сегментам информационной системы и к информационным ресурсам.

Указанные критерии подлежат учету в ходе проектирования информационных систем, проверке реализации в ходе аттестации на соответствие требованиям по защите информации (обеспечению безопасности) и контролю в ходе эксплуатации информационных систем.

2.10. Следствием все большей доступности в сети «Интернет» вредоносного программного обеспечения, средств его разработки является постоянное усложнение тактик и техник проведения компьютерных атак на информационные системы. В этих условиях выявление и оценка угроз безопасности информации не должны заключаться только в разработке модели угроз безопасности информации, а должны предусматривать организацию процессов по поиску, анализу и принятию мер, направленных на блокирование угроз безопасности информации. При анализе угроз безопасности информации подлежат оценке тактики, техники и инструменты, используемые для осуществления компьютерных атак, а также уязвимости информационных систем.

2.11. Рост числа сервисов, предоставляемых информационными системами, неразрывно связан с увеличением количества требуемых для их функционирования интерфейсов, что ведет к расширению поверхности компьютерных атак на информационные системы.

Уменьшение поверхности компьютерных атак является одной из важнейших задач по защите информационных систем и содержащейся в них информации. Решению данной задачи способствуют унификация применяемых

программных, программно-аппаратных средств и контроль их использования. Контроль интерфейсов информационных систем, прежде всего доступных из сети «Интернет», и недопущение их несанкционированного ввода в действие и эксплуатации обеспечивают снижение возможности нарушителей по реализации угроз безопасности информации.

2.12. Развитие функций (полномочий), проводимых работ (оказываемых услуг) с использованием информационных систем приводят к постоянным изменениям состава объектов и субъектов доступа и их полномочий. Зафиксировать конфигурацию информационных систем в базовых состояниях, в большинстве случаев, не представляется возможным. В этих условиях следует осуществлять мониторинг информационной безопасности информационных систем с учетом изменяющихся состава объектов и субъектов доступа и их полномочий.

2.13. Функционирование разных информационных систем и взаимодействие между ними может осуществляться на основе программно-технических комплексов и средств, выполняющих общие технологические функции и обеспечивающих основу функционирования указанных информационных систем. При этом информационно-телекоммуникационная инфраструктура[2] может принадлежать оператору или предоставляться как услуга сторонней организацией.

Использование общих программно-технических комплексов и средств для функционирования информационных систем, в том числе для хранения информации, передачи данных, осуществления вычислений, функционирования программных средств, предоставления доступа к сети «Интернет», приводит к необходимости отнесения к объектам защиты не только отдельных информационных систем и содержащейся в них информации, но и информационно-телекоммуникационной инфраструктуры, на основе которой они функционируют.

2.14. Применение в информационных системах зарубежных программных и программно-аппаратных средств создает угрозу использования недекларированных возможностей и закладок в программных, программно-аппаратных средствах для информационно-технического воздействия на информационные системы. Зарубежная электронная компонентная база создает риск внедрения в интегральные схемы логических уязвимостей. При этом возможности контроля производственного процесса и цепочек поставок

[2] Пункт 3 Положения об учете ИТ-активов, используемых для осуществления деятельности по цифровой трансформации системы государственного (муниципального) управления, утвержденного постановлением Правительства Российской Федерации от 1 июля 2024 г. N 900.

программно-аппаратных средств, электронной компонентной базы и телекоммуникационного оборудования в соответствии с требованиями по защите информации (обеспечению безопасности) отсутствуют. Подконтрольность иностранным государствам разработчиков зарубежных программных и программно-аппаратных средств существенно снижает уровень доверия к такой продукции. Для прекращения или нарушения функционирования информационных систем возможно использование каналов удаленного контроля и управления этими средствами и оборудованием.

В ходе проектирования информационных систем должен проводиться анализ доступных отечественных программных, программно-аппаратных и технических средств, должна быть предусмотрена возможность их применения в информационных системах или, как минимум, в сегментах, в которых хранится и обрабатывается наиболее значимая информация (данные). Это позволит снизить риски использования недекларированных возможностей для получения несанкционированного доступа и (или) воздействия на информацию.

2.15. В условиях большого количества субъектов и объектов доступа в распределенных информационных системах требуется обеспечение доверия при их взаимодействии. Обеспечение доверия может предусматривать:

первичную идентификацию пользователей и устройств, к которым осуществляется доступ пользователей для выполнения своих обязанностей (функций);

строгую аутентификацию пользователей, осуществляющих доступ для исполнения своих обязанностей (функций), и их устройств, к которым осуществляется доступ, с использованием сертификатов безопасности;

проверку подлинности и целостности устанавливаемого программного обеспечения и его обновлений с использованием сертификатов безопасности;

доверенную загрузку программного обеспечения устройств, страной происхождения которых является Российская Федерация, с использованием модулей безопасности этих средств, обеспечивающих в том числе безопасное хранение закрытых ключей и сертификатов безопасности.

Средства вычислительной техники и операционные системы, используемые в информационных системах, должны включать программное обеспечение, обеспечивающее функционирование модулей безопасности и осуществляющее проверку сертификатов безопасности устанавливаемого и запускаемого в их среде программного обеспечения.

2.16. Эффективность мероприятий по защите информации в органе (организации) и мер по защите информационных систем и содержащейся в них информации изменяется во времени под действием различных факторов, основными из которых являются изменение функций и процессов, изменение

состава и полномочий субъектов и объектов доступа, изменение конфигураций информационных технологий.

Для поддержки требуемой эффективности реализации мероприятий по защите информации, а также сохранения уровня защищенности информационных систем и содержащейся в них информации целесообразно проводить периодическую оценку как эффективности реализуемых мероприятий, так и достаточности принимаемых мер.

Оценка текущего состояния защиты информации проводится по результатам расчета показателя защищенности информационных систем ($К_{зи}$).

2.17. В основе качественной оценки текущего состояния защиты информации лежат результаты контроля уровня защищенности информации, содержащейся в информационных системах. Контроль уровня защищенности информации должен проводиться одним или совокупностью следующих методов:

автоматизированное и (или) ручное выявление уязвимостей информационных систем с последующей экспертной оценкой возможности их использования нарушителем для нарушения безопасности информации и (или) нарушения функционирования информационных систем;

выявление несанкционированных подключений устройств к информационным системам;

тестирование информационных систем путем моделирования реализации актуальных угроз с целью оценки возможностей несанкционированного доступа к ним (воздействий на них) или повышения привилегий с учетом реализованных мер и применяемых средств защиты информации;

проведение в соответствии с едиными замыслом и планом тренировок по отработке мероприятий и мер по обеспечению требуемого уровня защищенности информации, содержащейся в информационных системах, в условиях реализации актуальных угроз.

III. МЕРОПРИЯТИЯ (ПРОЦЕССЫ) ПО ЗАЩИТЕ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОРГАНОВ (ОРГАНИЗАЦИЙ)

3.1. Выявление и оценка угроз безопасности информации (ВУ)

Цель: Создание системы защиты информации, направленной на защиту от актуальных угроз безопасности информации (далее – актуальных угроз), а также своевременное выявление признаков реализации актуальных угроз, их оценку и принятие мер по защите информации в ходе эксплуатации информационных систем.

Требования к реализации: Выявление и оценка угроз безопасности информации должны проводиться в ходе создания (развития) информационных систем и в ходе их эксплуатации.

Выявление и оценка угроз безопасности информации должны проводиться для информационных систем с учетом актуальных угроз информационно-телекоммуникационной инфраструктуры, на базе которой они функционируют.

На стадии создания (развития) информационных систем выявление и оценка угроз безопасности информации должны предусматривать определение угроз безопасности информации, оценку возможности их реализации (возникновения) внешними и внутренними нарушителями, определение актуальности угроз безопасности информации в информационных системах с учетом их архитектуры и предполагаемых условий эксплуатации. Результаты выявления и оценки угроз безопасности информации подлежат включению в модель угроз безопасности информации, которая должна содержать характеристики информационных систем и информационно-телекоммуникационной инфраструктуры, на базе которой они функционируют, определяющие архитектуру, применяемые информационные технологии и процессы обработки информации, а также возможности нарушителей, перечень актуальных угроз. Для разработки модели угроз безопасности информации должны применяться методические документы, утвержденные ФСТЭК России.

На стадии эксплуатации информационных систем выявление и оценка угроз безопасности информации должны предусматривать:

анализ актуальных данных о составе информационных систем, их настройках и конфигурациях;

поиск данных и признаков, идентифицирующих актуальные угрозы, с учетом состава информационных систем, их настроек и конфигураций;

приоритизацию выявленных актуальных угроз исходя из критериев возможных последствий их реализации (возникновения);

оповещение заинтересованных подразделений (работников) оператора о выявленных актуальных угрозах;

анализ выявленных актуальных угроз с целью принятия решения о необходимости принятия мер.

В качестве исходных данных для выявления и оценки актуальных угроз используется банк данных угроз безопасности информации, ведение которого осуществляется ФСТЭК России (далее – банк данных угроз безопасности информации ФСТЭК России)[3], и иные источники, содержащие сведения

[3] Подпункт 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

об уязвимостях, нарушителях и используемых ими методах и средствах, доступных для оператора (обладателя информации).

Требования к документированию: Не предъявляются.

Требования к усилению[4]:

1) выявление и оценка актуальных угроз в ходе эксплуатации информационных систем осуществляются с учетом сведений, содержащихся в системах инвентаризации ИТ-активов;

2) выявление и оценка актуальных угроз в ходе эксплуатации информационных систем обогащаются данными от различных источников (систем управления событиями безопасности, систем обнаружения вторжений, средств антивирусной защиты, средств обнаружения и реагирования на уровне узла, межсетевых экранов и других средств защиты информации);

3) для выявления и оценки актуальных угроз привлекаются специализированные организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации с правом оказания услуг по мониторингу информационной безопасности средств и систем информатизации – центры мониторинга информационной безопасности;

4) для мониторинга актуальных угроз применяются средства анализа угроз, в том числе TI-платформы.

3.2. Контроль конфигураций информационных систем (КК)

Цель: Исключение несанкционированного изменения состава программных, программно-аппаратных средств информационных систем, их настроек и конфигураций, установленных во внутренних стандартах по защите информации, а также обеспечение своевременного обнаружения фактов несанкционированных изменений и выявление причин изменений.

Требования к реализации: Контроль конфигураций информационных систем должен осуществляться на основе анализа актуальных данных о составе информационных систем, их настройках и конфигурациях, установленных во внутренних стандартах по защите информации. Контроль конфигураций информационных систем должен предусматривать:

определение объектов инвентаризации, к которым должны быть отнесены программные, программно-аппаратные средства, включая коммуникационное

[4] Усиления мероприятий (процессов) по защите информации, приведенные в подразделах «требования к усилению» раздела 3, применяются по решению оператора (обладателя информации) для повышения эффективности реализации мероприятий по защите информации и повышения уровня защищенности информационных систем и содержащейся в них информации, а также для снижения возможности нарушителей по реализации угроз безопасности информации.

оборудование, информационно-телекоммуникационные сети и их подсети;

определение данных об объектах инвентаризации, подлежащих сбору, учету и хранению, включающих наименование объектов, версии программного обеспечения, сетевые адреса, используемые физические порты, сетевые связи, принадлежность подразделению и (или) работнику оператора;

сбор, учет и хранение данных об объектах инвентаризации;

актуализацию данных об объектах инвентаризации с установленной оператором периодичностью;

контроль состава объектов инвентаризации и выявление фактов несанкционированного добавления новых объектов или изменения текущих конфигураций;

определение конфигураций объектов инвентаризации и контроль их изменений, выявление фактов несанкционированного изменения конфигураций объектов инвентаризации;

сбор, анализ и регистрацию фактов несанкционированного изменения состава объектов инвентаризации и их конфигураций, реагирование на несанкционированные изменения.

Под конфигурацией объекта инвентаризации понимается совокупность установленных параметров, правил и настроек, определяющих способ функционирования объекта, его сетевое взаимодействие (если применимо), порядок администрирования и управления доступом, а также применяемые механизмы защиты.

По всем фактам несанкционированных изменений состава объектов инвентаризации и их конфигураций должны проводиться анализ и выявляться причины таких изменений.

Должны приниматься меры по защите собранных данных об объектах инвентаризации в соответствии с требованиями о защите информации.

Требования к документированию: Внутренние стандарты с типовыми конфигурациями и настройками программных, программно-аппаратных средств должны содержать:

перечень информационных систем и (или) отдельных типов (классов) программных, программно-аппаратных средств, к которым устанавливаются требования к настройкам и конфигурациям и подлежащих контролю в рамках контроля конфигураций;

описание настройки и конфигурации для каждого типа (класса) программных, программно-аппаратных средств, сегментов информационных систем, в отношении которых осуществляется контроль конфигураций, в том числе:

описание настройки и конфигурации программных, программно-аппаратных средств, предназначенных для обеспечения доступа пользователей к

сети «Интернет»;

описание настройки и конфигурации программных, программно-аппаратных средств, предназначенных для обеспечения удаленного доступа пользователей, включая требования к обеспечению безопасной дистанционной работы;

перечень подразделений (работников), ответственных за настройку и установку конфигураций программных, программно-аппаратных средств, а также за контроль конфигураций информационных систем;

порядок действий по изменению настроек и конфигураций программных, программно-аппаратных средств;

порядок действий при обнаружении фактов несанкционированного изменения настроек и конфигураций программных, программно-аппаратных средств.

Требования к усилению:

1) контроль конфигураций информационных систем осуществляется на основе данных автоматизированных систем сбора и хранения данных об объектах инвентаризации и их конфигурациях (CMDB-системы). Автоматизированный сбор данных об объектах инвентаризации должен осуществляться с использованием выделенной учетной записи, которой назначены минимально необходимые права для проведения автоматизированного сбора данных.

3.3. Управление уязвимостями (КУ)

Цель: Своевременное выявление уязвимостей информационных систем, оценка их критичности, определение методов и приоритетов устранения уязвимостей, а также контроль за устранением уязвимостей.

Требования к реализации: Управление уязвимостями должно предусматривать:

мониторинг уязвимостей и оценку их применимости;

оценку уязвимостей;

определение методов и приоритетов устранения уязвимостей;

устранение уязвимостей;

контроль устранения уязвимостей.

В ходе мониторинга уязвимостей и оценки их применимости осуществляются выявление уязвимостей на основании данных, получаемых из внешних (базы данных известных уязвимостей, официальные ресурсы разработчиков программных средств, специализированные публикации, форумы, иные источники) и внутренних (средства анализа защищенности, иные средства защиты информации, данные о составе программных, программно-

аппаратных средств) источников, и принятие решения о применимости уязвимостей к информационным системам.

В ходе оценки уязвимостей определяется уровень критичности уязвимостей применительно к информационным системам органа (организации).

В ходе определения методов и приоритетов устранения уязвимостей определяется приоритетность устранения уязвимостей и выбираются методы их устранения: обновление программного обеспечения и (или) применение компенсирующих мер защиты информации.

В ходе устранения уязвимостей принимаются меры, направленные на устранение или исключение возможности использования (эксплуатации) нарушителем выявленных уязвимостей. Время, в течение которого должны быть приняты меры по устранению уязвимостей, определяется исходя из уровня критичности уязвимости и в соответствии с требованиями о защите информации, утвержденными ФСТЭК России.

В ходе контроля устранения уязвимостей осуществляются сбор и обработка данных о процессе управления уязвимостями и его результатах, а также принятие решений по улучшению данного процесса.

Процесс управления уязвимостями организуется для всех информационных систем оператора и должен предусматривать постоянную и непрерывную актуализацию сведений об уязвимостях и составе программных, программно-аппаратных средств информационных систем. При изменении статуса уязвимостей (применимость к информационным системам, наличие исправлений, уровень критичности) должны корректироваться способы их устранения.

Требования к документированию: Внутренний регламент по управлению уязвимостями информационных систем должен содержать:

перечень подразделений (работников), ответственных за организацию и контроль управления уязвимостями, а также участвующих в реализации процессов управления уязвимостями, их обязанности (функции) и права (полномочия);

описание операций, осуществляемых при мониторинге уязвимостей и оценке их применимости, перечень исполнителей операций, продолжительность реализации, входные и выходные данные, используемые при мониторинге уязвимостей и оценке их применимости;

описание операций, осуществляемых при оценке уязвимостей, перечень исполнителей операций, продолжительность реализации, входные и выходные данные, используемые при оценке уязвимостей;

описание операций, осуществляемых при определении методов и приоритетов устранения уязвимостей, перечень исполнителей операций,

продолжительность реализации, входные и выходные данные, используемые при определении методов и приоритетов устранения уязвимостей;

описание операций, осуществляемых при устранении уязвимостей, перечень исполнителей операций, продолжительность реализации, входные и выходные данные, используемые при устранении уязвимостей;

описание операций, осуществляемых при контроле устранения уязвимостей, перечень исполнителей операций, продолжительность реализации, входные и выходные данные, используемые при контроле устранения уязвимостей;

схемы взаимодействия подразделений (работников) при реализации операций по управлению уязвимостями.

Требования к усилению:

1) для управления уязвимостями используются автоматизированные системы управления уязвимостями;

2) для мониторинга уязвимостей применяются средства анализа угроз, в том числе TI-платформы;

3) для оценки применимости уязвимостей используются данные, содержащиеся в автоматизированных системах сбора и хранения данных об объектах инвентаризации и их конфигурациях (CMDB-системы);

4) для контроля устранения уязвимостей используются результаты мониторинга информационной безопасности или управления обновлениями, или управления конфигурациями.

3.4. Управление обновлениями (КО)

Цель: Своевременная установка обновлений программного обеспечения, устраняющих уязвимости.

Требования к реализации: Управление обновлениями должно предусматривать:

контроль актуальности версий программных, программно-аппаратных средств;

получение обновлений программных, программно-аппаратных средств из источников, содержащих механизмы проверки подлинности и целостности обновлений;

проверку подлинности и целостности обновлений программных, программно-аппаратных средств;

тестирование обновлений до их применения в контурах промышленной эксплуатации информационных систем;

разработку безопасных настроек и конфигураций обновлений программных, программно-аппаратных средств (при необходимости);

применение обновлений программных, программно-аппаратных средств в контурах промышленной эксплуатации информационных систем;

возможность отмены обновлений программного обеспечения, в том числе возможность восстановления программного обеспечения из резервной копии.

Решение о применении обновлений программного обеспечения принимается подразделением (работниками), обеспечивающим функционирование информационных систем, по согласованию со структурным подразделением, специалистами по защите информации. Порядок применения обновлений программного обеспечения устанавливается во внутренних регламентах. Настройки и конфигурации обновлений программного обеспечения определяются во внутренних стандартах.

Для применения обновлений программных, программно-аппаратных средств в информационной инфраструктуре оператора должен быть развернут и функционировать выделенный север обновлений, предназначенный для их распространения и установки в информационных системах. Загрузка и установка в реальном режиме времени (онлайн) обновлений программных, программно-аппаратных средств не допускается за исключением случаев, когда реализована проверка целостности и аутентичности обновлений на основе сертификатов безопасности с применением российских криптографических стандартов.

Сроки применения обновлений программных, программно-аппаратных средств, предназначенных для устранения уязвимостей, устанавливаются во внутреннем регламенте по защите информации в зависимости от сроков устранения уязвимостей соответствующих уровней опасности и рисков, связанных с применением обновлений программных, программно-аппаратных средств.

Требования к документированию: Внутренний регламент по управлению обновлениями должен содержать:

перечень подразделений (работников), ответственных за организацию и контроль управления обновлениями, а также участвующих в реализации процессов управления обновлениями, их обязанности (функции) и права (полномочия);

описание операций, осуществляемых при управлении обновлениями;

схемы взаимодействия подразделений (работников) при реализации операций по управлению обновлениями.

Требования к усилению:

1) для контроля актуальности версий программных, программно-аппаратных средств используются данные, содержащиеся в автоматизированных системах сбора и хранения данных об объектах инвентаризации и их конфигурациях (CMDB-системы);

2) для тестирования обновлений применяется тестовая зона информационной системы («песочница»);

3) для применения обновлений программных, программно-аппаратных средств в информационной инфраструктуре оператора должен быть развернут и функционировать выделенный источник (сегмент информационной системы) обновлений, предназначенный для их распространения и установки в информационных системах.

3.5. Обеспечение защиты информации при обработке, хранении и обращении с информацией ограниченного доступа (ОД)

Цель: Исключение неправомерного распространения информации ограниченного доступа при обработке, хранении и обращении с ней (далее – обращение с информацией ограниченного доступа) вне зависимости от формы представления информации.

Требования к реализации: Защита информации при обращении с информацией ограниченного доступа должна предусматривать:

определение перечня информации ограниченного доступа и предназначенных для ее хранения программно-аппаратных средств, включая съемные внешние средства хранения информации;

обеспечение доступа к информации ограниченного доступа и предназначенных для ее хранения программно-аппаратным средствам только тем лицам, которым такой доступ разрешен в соответствии с внутренними регламентами по защите информации;

контроль передачи, распространения информации ограниченного доступа в информационной системе, в том числе контроль вывода информации ограниченного доступа из информационной системы;

контроль и регистрацию всех фактов доступа пользователей к программно-аппаратным средствам, в которых хранится информация ограниченного доступа, фактов вывода информации ограниченного доступа из информационной системы.

К информации ограниченного доступа следует относить сведения, для носителей которых установлена ограничительная пометка «для служебного пользования», персональные данные, сведения, составляющие коммерческую тайну, и иные виды информации, доступ к которой ограничен в соответствии с федеральными законами, нормативными правовыми актами Президента Российской Федерации и Правительства Российской Федерации.

В случае утраты необходимости хранения информации ограниченного доступа должно быть обеспечено удаление (стирание) указанной информации и форматирование машинных носителей, программно-аппаратных средств

хранения информации ограниченного доступа (при наличии технической возможности). При необходимости передачи программно-аппаратных средств хранения информации ограниченного доступа в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения должно обеспечиваться стирание информации ограниченного доступа путем перезаписи мест хранения файлов случайной битовой последовательностью, удаления записи о файлах, обнуление журнала файловой системы или полной перезаписи всего адресного пространства машинного носителя информации случайной битовой последовательностью с последующим форматированием. При отсутствии возможности форматирования допускается проведение ремонтных работ или уничтожения в присутствии сотрудника (работника) оператора.

При выводе из эксплуатации программно-аппаратных средств хранения информации ограниченного доступа осуществляется физическое уничтожение таких средств или уничтожение содержащейся на них информации с использованием средств уничтожения (стирания) информации. Способы физического уничтожения средств хранения информации должны быть определены во внутренних регламентах по защите информации.

В отношении средств хранения информации ограниченного доступа должны быть приняты меры физической защиты.

Контроль обработки, хранения информации ограниченного доступа в программно-аппаратных средствах и ее передачи должен обеспечиваться в соответствии с внутренним регламентом по защите информации.

О фактах неправомерного распространения информации ограниченного доступа и (или) доступа к средствам ее хранения должен быть незамедлительно проинформирован руководитель оператора (обладателя информации), ответственное лицо.

Требования к документированию: Внутренний регламент, определяющий порядок защиты информации при обращении с информацией ограниченного доступа, должен содержать:

перечень информации ограниченного доступа и предназначенных для ее хранения программно-аппаратных средств, включая съемные внешние средства хранения информации;

перечень лиц (категорий лиц, ролей пользователей), которым доступ к информации ограниченного доступа разрешен для выполнения своих обязанностей (функций), и соответствующих обязанностей (функций), требующих доступа к информации ограниченного доступа;

перечень программно-аппаратных средств, предназначенных для хранения информации ограниченного доступа, подлежащих учету, порядок учета таких средств;

порядок уничтожения программно-аппаратных средств хранения

информации ограниченного доступа и (или) их съемных машинных носителей информации;

перечень и содержание мероприятий по контролю за хранением, передачей и распространением информации ограниченного доступа, а также используемых при проведении таких мероприятий программных, программно-аппаратных средств;

перечень подразделений (работников), ответственных за контроль хранения, передачи и распространения информации ограниченного доступа, их обязанности (функции) и права (полномочия);

порядок установления причин неправомерного доступа пользователей к программно-аппаратным средствам, в которых хранится информация ограниченного доступа, неправомерных распространения, вывода, передачи информации ограниченного доступа из информационной системы;

схемы взаимодействия подразделений (работников) при реализации мероприятий по контролю передачи и распространения информации ограниченного доступа (при необходимости).

Требования к усилению:

1) хранение информации ограниченного доступа в программно-аппаратных средствах хранения в зашифрованном виде с использованием шифровальных (криптографических) средств защиты информации;

2) обеспечение хранения информации ограниченного доступа на учтенных съемных внешних средствах хранения информации, с присвоением учетных данных (регистрационных номеров). В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера средств, присвоенных производителями этих средств, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера;

3) обеспечение маркировки машинных носителей информации, съемных внешних средств хранения информации с использованием радиочастотных меток, иных технологий, обеспечивающих однозначную идентификацию и контроль использования носителей, средств;

4) обеспечение хранения программно-аппаратных средств, предназначенных для хранения информации ограниченного доступа, в помещениях, специально предназначенных для хранения носителей информации;

5) применение автоматизированной системы контроля физического доступа в помещения, в которых осуществляется хранение средств, предназначенных для хранения информации ограниченного доступа;

6) обеспечение контроля перемещения используемых в информационной системе съемных внешних средств хранения информации за пределы

контролируемой зоны;

7) применение средств защиты от неправомерной передачи информации из информационной системы (в том числе DLP-систем и средств однонаправленной передачи информации);

8) автоматическое маркирование носителя информации при выводе информации ограниченного доступа на печать.

3.6. Обеспечение защиты информации при использовании конечных устройств (ЗУ)

Цель: Исключение возможности несанкционированного доступа к информационным системам и конечным устройствам или воздействия на них через интерфейсы, непосредственно взаимодействующие с сетью «Интернет» и (или) доступные из сети «Интернет».

Требования к реализации: Защита информации при использовании конечных устройств должна предусматривать:

предоставление на конечных устройствах доступа к сети «Интернет» только работникам, которым такой доступ необходим для выполнения своих обязанностей (функций);

реализацию на конечных устройствах мер по защите информации от несанкционированного доступа;

осуществление на конечных устройствах мониторинга и анализа процессов и событий с целью выявления актуальных угроз;

предупреждение пользователя о произошедших на конечных устройствах событиях безопасности.

Предоставление пользователям доступа к сети «Интернет» с использованием конечных устройств должно осуществляться подразделением (работниками), обеспечивающим функционирование информационных систем, в соответствии с заявками подразделений, эксплуатирующих информационные системы, согласованными со структурным подразделением, специалистами по защите информации.

На конечных устройствах должны применяться программные средства, протоколы и порты, интерфейсы, минимально необходимые для выполнения обязанностей (функций) пользователей, связанных с доступом к сети «Интернет».

Изменение настроек и конфигураций конечных устройств должно осуществляться по согласованию со структурным подразделением, специалистами по защите информации.

Контроль использования конечных устройств (автоматизированных рабочих мест пользователей) должен осуществляться в соответствии с внутренними стандартами и регламентами по защите информации.

По всем фактам несанкционированного доступа в сеть «Интернет» или из сети «Интернет», несанкционированного изменения настроек и конфигураций конечных устройств относительно настроек и конфигураций, установленных во внутренних стандартах, структурным подразделением, специалистами по защите информации проводится анализ и выявляются причины таких доступов, изменений.

Требования к документированию: Внутренние стандарты по защите конечных устройств должны содержать:

требования к составу программных средств и средств защиты информации конечных устройств, их настройкам, конфигурациям;

требования к составу портов, интерфейсов, протоколов конечных устройств (автоматизированных рабочих мест пользователей), с использованием которых разрешен доступ к сети «Интернет», и их контролю;

требования к составу процессов и событий конечных устройств (автоматизированных рабочих мест пользователей), подлежащих мониторингу и анализу с целью выявления актуальных угроз;

требования к событиям безопасности, по которым осуществляется предупреждение пользователя.

Действия пользователя при работе на конечных устройствах при осуществлении доступа к сети «Интернет» определяются во внутреннем регламенте, определяющем порядок предоставления пользователям доступа из информационных систем в сеть «Интернет» и контроля использования конечных устройств в случае взаимодействия с сетью «Интернет».

Требования к усилению:

1) на конечных устройствах (автоматизированных рабочих местах пользователей) должны проводиться контроль и регистрация фактов доступа к ресурсам сети «Интернет» на основе URL-фильтрации, репутационных фильтров, потоковых антивирусов, ведение и обслуживание которых осуществляется структурным подразделением, специалистами по защите информации.

3.7. Обеспечение защиты информации при применении мобильных устройств (МУ)

Цель: Исключение возможности несанкционированного доступа к информационным системам и содержащейся в них информации, а также к взаимодействующим с ними мобильным устройствам и содержащейся

в них информации через каналы передачи мобильных данных, мобильные сервисы, интерфейсы и порты мобильных устройств.

Требования к реализации: Обеспечение защиты информации при применении в составе информационной системы мобильных устройств должно предусматривать:

предоставление доступа к информационным системам с использованием мобильных устройств только работникам, которым такой доступ необходим для выполнения своих обязанностей (функций);

реализацию в информационных системах мер по защите информации при доступе с использованием мобильных устройств;

реализацию в мобильных устройствах мер по защите информации от несанкционированного доступа;

защиту каналов передачи данных при доступе к информационным системам с использованием мобильных устройств с использованием шифровальных (криптографических) средств защиты информации.

Предоставление доступа к информационным системам с использованием мобильных устройств должно осуществляться в соответствии с заявками подразделений, эксплуатирующих информационные системы, согласованными со структурным подразделением, специалистами по защите информации.

В информационных системах при доступе к ним с использованием мобильных устройств должны быть приняты меры по идентификации и аутентификации подключаемых с использованием мобильных устройств пользователей, разграничению и контролю доступа пользователей к объектам доступа информационных систем, регистрации событий безопасности, связанных с доступом с использованием мобильных устройств, защите данных, передаваемых по сети «Интернет», с использованием шифровальных (криптографических) средств защиты информации, а также контролю сетевых доступов к сегментам информационной системы удаленных пользователей и обнаружению и предотвращению вторжений.

Мобильным устройствам, используемым для доступа к информационным системам, должны быть присвоены идентификаторы, обеспечивающие контроль подключения и доступа к информационным системам.

На мобильных устройствах должны применяться конфигурации и настройки программных, программно-аппаратных средств, обеспечивающие их защиту от актуальных угроз, определенные во внутренних стандартах.

Пользователем при использовании мобильных устройств для доступа к информационным системам с целью выполнения своих обязанностей (функций) должны приниматься все возможные меры по исключению несанкционированного физического доступа к мобильному устройству посторонних лиц.

В случае утраты мобильного устройства пользователь незамедлительно информирует о факте такой утраты структурное подразделение, специалистов по защите информации и подразделение (работников), обеспечивающее эксплуатацию информационных систем. Указанными подразделениями (работниками) должны быть приняты меры по блокированию возможности доступа в информационные системы оператора (обладателя информации) с использованием утраченного мобильного устройства.

При применении пользователями мобильных устройств для доступа к информационным системам и содержащейся в них информации, не связанного с выполнением пользователем своих обязанностей (функций), в том числе для доступа к общедоступной информации, оператором (обладателем информации) должны приниматься меры по защите информационных систем и содержащейся в них информации и, при необходимости, защита каналов передачи данных, используемых для осуществления доступа.

В случае использования для доступа к информационным системам более 10 мобильных устройств должно обеспечиваться автоматизированное управление и контроль использования мобильных устройств.

Изменение конфигурации и настроек мобильных устройств их пользователями не допускается. Изменение конфигурации и настроек мобильных устройств относительно конфигураций и настроек, определенных во внутренних стандартах, должно осуществляться только подразделением (работниками), обеспечивающим функционирование информационной системы, по согласованию со структурным подразделением, специалистами по защите информации.

По всем фактам несанкционированного изменения конфигураций и настроек мобильных устройств относительно конфигураций и настроек, определенных во внутренних стандартах, должен проводиться анализ и выявляться причины таких изменений.

Применение пользователями личных мобильных устройств для доступа к информационным системам и содержащейся в них информации с целью выполнения своих обязанностей (функций) допускается только в случае реализации в мобильных устройствах мер по защите информации, установленных настоящим методическим документом, и наличия у оператора (обладателя информации) возможности контроля использования мобильных устройств. Контроль использования мобильных устройств должен осуществляться в соответствии с внутренними стандартами и регламентами по защите информации.

Требования к документированию: Внутренние стандарты по защите мобильных устройств должны содержать:

требования к типам мобильных устройств, применяемых в составе

информационных систем;

требования к составу программных средств и средств защиты информации мобильных устройств, их настройкам, конфигурациям;

требования к составу интерфейсов мобильных устройств, с использованием которых разрешен доступ к сети «Интернет», и их контролю.

Действия пользователя при работе на мобильных устройствах при осуществлении доступа к информационным системам определяются во внутренних регламентах, определяющих порядок предоставления пользователям удаленного доступа к информационным системам и содержащейся в них информации и определяющих порядок предоставления пользователям доступа из информационных систем в сеть «Интернет» и контроля использования мобильных устройств в случае взаимодействия с сетью «Интернет».

Требования к усилению:

1) при хранении в мобильных устройствах информации ограниченного доступа ее защита обеспечивается с использованием шифровальных (криптографических) средств защиты информации.

3.8. Обеспечение защиты информации при удаленном доступе пользователей к информационным системам (УД)

Цель: Исключение возможности несанкционированного доступа (воздействия) к информационным системам и содержащейся в них информации, а также к взаимодействующим с ними программно-аппаратным средствам пользователей через каналы передачи данных, интерфейсы удаленно подключаемых программно-аппаратных средств.

Требования к реализации: Обеспечение защиты информации при удаленном доступе пользователей к информационным системам должно предусматривать:

предоставление удаленного доступа к информационным системам только тем пользователям, которым такой доступ необходим для выполнения своих обязанностей (функций);

определение информационных систем, их сегментов и (или) отдельных программных, программно-аппаратных средств, к которым предоставляется удаленный доступ;

реализацию в информационных системах мер по защите информации при удаленном доступе;

реализацию в удаленно подключаемом программно-аппаратном средстве пользователя мер по защите информации;

обеспечение контроля удаленного доступа к сегментам (компонентам) информационных систем.

Удаленным доступом является доступ пользователей к информационным системам и содержащейся в них информации из-за предела контролируемой зоны с использованием сетей связи общего пользования, включая сеть «Интернет».

В информационных системах при осуществлении удаленного доступа к ним пользователей должны быть приняты меры по идентификации и аутентификации удаленно подключаемых пользователей, разграничению и контролю доступа удаленных пользователей к объектам доступа информационных систем, регистрации событий безопасности, связанных с удаленным доступом, защите веб-технологий, используемых при удаленном доступе, защите данных, передаваемых по сети «Интернет», с использованием шифровальных (криптографических) средств защиты информации, а также контролю сетевых доступов к сегментам информационной системы удаленных пользователей и обнаружению и предотвращению вторжений на сетевом уровне при осуществлении удаленного доступа.

В удаленно подключаемых программно-аппаратных средствах пользователей принимаются меры по идентификации и аутентификации пользователей, разграничению и контролю доступа пользователей к объектам доступа программно-аппаратного средства, регистрации событий безопасности в программно-аппаратном средстве, антивирусной защите, поддержке механизмов строгой аутентификации пользователей и защите данных, передаваемых по сети «Интернет».

Учетные записи, выданные пользователям для удаленного доступа к информационным системам, должны использоваться для выполнения своих обязанностей (функций). Использование учетных записей в сторонних сервисах на допускается.

Публикация в сети «Интернет» сетевых сервисов информационной системы не допускается (за исключением публичных веб-приложений, сервисов электронной почты, телефонии и иных сервисов, функционирование которых необходимо в информационных системах).

Предоставление удаленного доступа к информационным системам с использованием личных программно-аппаратных средств работников допускается при условии применения средств обеспечения безопасной дистанционной работы и средств антивирусной защиты и по согласованию со структурным подразделением, специалистами по защите информации.

Удаленный доступ к информационным системам или их сегментам (средствам), несанкционированный доступ к которым или воздействия

на которые могут привести к существенным негативным последствиям, неприемлемым для обладателя информации или оператора, должен предоставляться только при необходимости и по согласованию со структурным подразделением, специалистами по защите информации и на ограниченный интервал времени (за исключением случаев перевода работников на удаленный режим работы).

В случае прекращения необходимости удаленного доступа к информационным системам возможность доступа с использованием выделенных для этого учетных записей пользователей должна быть исключена.

Удаленный доступ внутренних непривилегированных пользователей в информационную систему с личных средств вычислительной техники должен осуществляться с использованием средств обеспечения безопасной дистанционной работы.

Требования к документированию: Внутренний стандарт, устанавливающий требования к конфигурациям и настройкам программных, программно-аппаратных средств, предназначенных для обеспечения удаленного доступа пользователей, должен содержать:

требования к типам программно-аппаратных средств, с использованием которых разрешен удаленный доступ;

требования к составу программных средств и средств защиты информации программно-аппаратных средств, с использованием которых разрешен удаленный доступ, их настройкам, конфигурациям;

требования к составу портов, интерфейсов, протоколов программно-аппаратных средств, с использованием которых разрешен удаленный доступ, и их контролю;

требования к перечню настроек и конфигураций программных, программно-аппаратных средств, подлежащих контролю и реагированию в случае обнаружения факта их изменения.

Внутренний регламент, определяющий порядок предоставления пользователям удаленного доступа к информационным системам и содержащейся в них информации, должен содержать:

перечень лиц (категорий пользователей, ролей пользователей), которым разрешен удаленный доступ к информационным системам для выполнения своих обязанностей (функций) и (или) перечень обязанностей (функций), предусматривающий удаленный доступ;

перечень сегментов информационных систем, отдельных программно-аппаратных средств и содержащейся в них информации, к которым разрешен удаленный доступ соответствующих категорий, ролей пользователей;

перечень и содержание мероприятий по предоставлению пользователям удаленного доступа к информационным системам и содержащейся в них

информации, включая состав и функции работников, ответственных за принятие решения и осуществляющих предоставление удаленного доступа;

порядок действий пользователя в случае выявления факта изменения настроек и конфигураций программных, программно-аппаратных средств;

перечень и содержание мероприятий по контролю за удаленным доступом пользователей;

перечень подразделений (работников), ответственных за контроль удаленного доступа, их обязанности (функции) и права (полномочия);

порядок установления причин неправомерного изменения настроек и конфигураций программных, программно-аппаратных средств, используемых для удаленного доступа;

схемы взаимодействия подразделений (работников) при реализации мероприятий по контролю удаленного доступа (при необходимости).

Требования к усилению:

1) учетные записи работников, которым предоставлена возможность удаленного доступа к информационным системам, подлежат объединению в рамках одной или нескольких групп, для которых обеспечиваются централизованное управление и контроль учетными записями;

2) программно-аппаратным средствам, используемым для удаленного доступа к информационным системам, должны быть присвоены неизменяемые идентификаторы, обеспечивающие контроль подключения и доступа к информационным системам. Каждому средству, с использованием которого осуществляется удаленный доступ, должно присваиваться сетевое (доменное) имя;

3) должен осуществляться контроль удаленного доступа с применением средств, систем геопозиционирования программно-аппаратных средств, обеспечивающих определение места, из которого пользователь осуществляет уделенный доступ;

4) должно быть обеспечено блокирование удаленного доступа пользователей оператора при обнаружении признаков реализации угроз безопасности информации, связанных с таким доступом, включая блокировку учетных записей и сессий, созданных учетной записью;

5) должен быть обеспечен контроль удаленного доступа к сегментам (компонентам) информационных систем с возможностью автоматического прекращения доступа после истечения интервала времени, на который был предоставлен удаленный доступ, или принудительно;

6) на устройствах, с которых осуществляется удаленный доступ к информационным системам, должны применяться средства сетевого взаимодействия (в том числе, доверенные аппаратные сетевые интерфейсы).

3.9. Обеспечение защиты информации при беспроводном доступе пользователей к информационным системам (БД)

Цель: Исключение возможности несанкционированного доступа к информационным системам и содержащейся в них информации при применении в составе информационной инфраструктуры оператора точек беспроводного доступа.

Требования к реализации: Обеспечение защиты информации при применении точек беспроводного доступа должно предусматривать:

реализацию в информационных системах мер по защите информации при беспроводном доступе;

реализацию в подключаемых с использованием беспроводных сетей программно-аппаратных средствах пользователей мер по защите информации;

обеспечение защиты беспроводных каналов передачи данных;

защиту точек беспроводного доступа, с использованием которых осуществляется доступ к информационной системе и содержащейся в ней информации.

В информационных системах должны приниматься меры по идентификации и аутентификации точек беспроводного доступа, включенных в состав беспроводной сети, логическому разделению сегментов беспроводной сети, используемых пользователями для выполнения своих обязанностей (функций), и сегментов беспроводных сетей связи, предназначенных для доступа к сети «Интернет» и (или) общедоступной информации оператора (обладателя информации).

В точках беспроводного доступа должны быть реализованы идентификация и аутентификация подключаемых к ним устройств и пользователей, фильтрация и контроль доступа пользователей и их устройств, подключаемых к беспроводным точкам доступа, применение защищенных технологий беспроводного доступа, регулярное обновление встроенного программного обеспечения (прошивок), усиленная многофакторная аутентификация администраторов беспроводной сети, обеспечение физической защиты точек беспроводного доступа. Конфигурация и настройки точек беспроводного доступа, используемых для подключения пользователей к информационным системам в целях выполнения своих обязанностей (функций), должны исключать возможность подключения к ним лиц, не имеющих прав доступа к информационным системам.

Требования к документированию: Внутренний стандарт, устанавливающий требования к типовым конфигурациям и настройкам программных, программно-аппаратных средств, должен содержать:

требования к типам разрешенного беспроводного доступа /

к информационным системам;

перечень беспроводных сетей, разрешенных для подключения к ним для доступа к информационным системам;

требования к составу точек беспроводного доступа, используемых для подключения пользователей, их настройкам, конфигурациям;

требования к перечню настроек и конфигураций точек беспроводного доступа, подлежащих контролю и реагированию в случае обнаружения факта их изменения.

Требования к усилению:

1) уровни сигналов точек беспроводного доступа, используемых для подключения пользователей к информационным системам в целях выполнения своих обязанностей (функций), должны исключать возможность подключения к ним из-за границ охраняемой территории (контролируемой зоны) оператора (обладателя информации);

2) применение в точках беспроводного доступа полосовых фильтров, обеспечивающих затухание сигнала вне рабочего диапазона частот.

3.10. Обеспечение защиты информации при предоставлении пользователям привилегированного доступа (ПД)

Цель: Исключение возможности получения привилегированного доступа к информационным системам лицами, для которых такой доступ должен быть исключен, а также недопущение использования повышенных прав доступа с нарушением внутренних стандартов и регламентов по защите информации.

Требования к реализации: Обеспечение защиты информации при предоставлении пользователям привилегированного доступа должно предусматривать:

предоставление привилегированного доступа к информационным системам только тем работникам, в обязанности (функции) которых входит разработка, тестирование программного обеспечения информационной системы, обеспечение функционирования информационных систем или защита содержащейся в них информации;

создание для привилегированного доступа привилегированных учетных записей с правами доступа, минимально необходимыми для выполнения работниками возложенных на них обязанностей (функций);

наделение привилегированных учетных записей правами доступа в соответствии с моделями доступа информационных систем, определенными во внутренних стандартах, и контроль прав доступа;

применение для привилегированных учетных записей строгой аутентификации или усиленной многофакторной аутентификации;

регистрацию действий по доступу пользователей с использованием привилегированных учетных записей и контроль использования привилегированных учетных записей в соответствии с внутренними стандартами и регламентами по защите информации.

Все привилегированные учетные записи должны быть закреплены за соответствующими работниками.

Работники должны использовать привилегированные учетные записи в соответствии с внутренними регламентами и стандартами. Не допускается использование привилегированных учетных записей для целей, не указанных в заявке на создание привилегированных учетных записей. Использование привилегированных учетных записей без служебной необходимости запрещено.

Создание и использование групповых привилегированных записей допускается при условии однозначной идентификации лиц, использующих привилегированные учетные записи в конкретный момент времени.

Не допускается объединение в рамках одной привилегированной учетной записи или одной группы привилегированных учетных записей ролей по системному администрированию, ролей по разработке и тестированию программных, программно-аппаратных средств, ролей администраторов безопасности.

Созданные привилегированные учетные записи подлежат учету и контролю их использования.

Встроенные в программные, программно-аппаратные средства привилегированные учетные записи допускается использовать только для первоначальной настройки, ремонта или технического обслуживания, проведения аварийного восстановления информационных систем (в случае отсутствия возможности использования других привилегированных учетных записей), а также для создания локальных привилегированных учетных записей с правами по созданию других привилегированных учетных записей и назначению им прав доступа (далее – учетные записи главных администраторов).

Учетные записи главных администраторов должны иметь персональное закрепление за работниками, на которых возложены обязанности (функции) по созданию, изменению, блокированию привилегированных учетных записей (далее – главный администратор) (за исключением использования для создания привилегированных учетных записей автоматизированной системы управления привилегированными учетными записями). Факт привилегированного доступа главного администратора, должность и фамилия, имя, отчество (при наличии), время доступа и перечень совершаемых главным администратором действий в информационной системе должен регистрироваться в журнале учета действий

главного администратора, контроль за ведением которого осуществляется структурным подразделением, специалистами по защите информации.

Привилегированные учетные записи главных администраторов не должны иметь удаленного доступа, должны быть персонифицированы для конкретных работников, наделенных соответствующими обязанностями (функциями).

Встроенные привилегированные учетные записи должны быть отключены или, в случае невозможности отключения, переименованы после завершения настройки и установки конфигураций, заданных внутренними стандартами по защите информации (при наличии технической возможности). Аутентификационная информация встроенных привилегированных учетных записей должна быть изменена в соответствии с внутренними стандартами и регламентами по защите информации.

В случае необходимости временного предоставления привилегированного доступа к информационной системе или необходимости нестандартных прав доступа в запросе на создание привилегированной учетной записи должен быть указан срок и состав работ, для которых создается временная учетная запись. Временная привилегированная учетная запись подлежит учету и контролю использования. По истечении интервала времени использования, в который была создана временная привилегированная учетная запись, она подлежит блокированию в информационной системе и в автоматизированной системе управления привилегированными учетными записями (в случае их использования) в автоматическом или автоматизированном режиме.

Для взаимодействия информационных систем, отдельных программных, программно-аппаратных средств с использованием программных интерфейсов создаются неперсонифицированные технологические привилегированные учетные записи. Технологические привилегированные учетные записи должны быть закреплены за работниками подразделения, обеспечивающего функционирование информационных систем. Технологические привилегированные учетные записи должны подлежать учету и контролю использования.

Аутентификационная информация привилегированных учетных записей подлежит изменению в соответствии с внутренними регламентами и стандартами, но не реже одного раза в шесть месяцев (за исключением случаев использования для доступа сертификатов безопасности).

Аутентификационная информация привилегированных учетных записей, заданная разработчиком, производителем программных, программно-аппаратных средств по умолчанию, подлежит изменению при первоначальной настройке программных, программно-аппаратных средств.

Аутентификационная информация привилегированных учетных записей,

созданная в ходе настройки, ремонта, сервисного обслуживания, подлежит изменению после завершения указанных работ.

Не допускается использование одинаковой аутентификационной информации для привилегированных учетных записей, неперсонифицированных технологических привилегированных учетных записей, непривилегированных учетных записей.

Неиспользуемые привилегированные учетные записи должны быть заблокированы и удалены. В случае отстранения работника от выполнения обязанностей (функций), возможность использования его привилегированной учетной записи должна быть заблокирована не позднее 8 часов после отстранения работника от выполнения обязанностей (функций). Также должна быть изменена аутентификационная информация всех учетных записей, к которым у работника был доступ.

Использование системными администраторами и администраторами безопасности мобильных устройств для осуществления привилегированного доступа не допускается.

Удаленный привилегированный доступ предоставляется при необходимости только для выполнения работником обязанностей (функций) из мест, в которых отсутствует возможность физического доступа к программно-аппаратным средствам, входящим в состав информационной системы. Должна быть обеспечена возможность использования привилегированной учетной записи в отведенное для этого время.

Привилегированные учетные записи структурного подразделения, специалистов по защите информации создаются по решению руководителя, ответственного лица.

Требования к документированию: Внутренний регламент, определяющий порядок создания, учета, изменения и блокирования, контроля, удаления привилегированных учетных записей, должен содержать:

перечень лиц (в том числе категорий пользователей, ролей пользователей), которым предоставлены права по созданию, учету, изменению и блокированию, контролю, удалению привилегированных учетных записей;

перечень и содержание мероприятий по созданию, учету, изменению и блокированию, контролю, удалению привилегированных учетных записей;

перечень и содержание мероприятий по контролю за действиями в информационных системах привилегированных учетных записей.

Во внутреннем стандарте по первичной идентификации устанавливаются требования к первичной идентификации лиц, обладающих правами привилегированного доступа.

Во внутреннем стандарте по применяемым моделям доступа пользователей устанавливаются типы привилегированных учетных записей,

их права по доступу к объектам доступа информационных систем.

Во внутреннем стандарте по ограничению и запретам действий для пользователей устанавливаются запрещенные действия пользователей при осуществлении ими привилегированного доступа, а также ограничения и запреты при создании, учете, изменениях и блокировании, контроле, удалении привилегированных учетных записей.

Требования к усилению:

1) системные администраторы и администраторы безопасности для выполнения своих обязанностей (функций) должны использовать только выделенные оператором для администрирования программно-аппаратные средства. Доступ к информационным системам по протоколам управления должен быть разрешен только с выделенных автоматизированных рабочих мест. Использование для этих целей иных программно-аппаратных средств допускается только при использовании средств обеспечения безопасной дистанционной работы;

2) в информационной системе должны применяться средства управления привилегированными учетными записями для предоставления возможности использования, учета, изменения, блокирования и контроля использования привилегированных учетных записей;

3) создание, изменение, блокирование главным администратором привилегированных учетных записей по заявке подразделения, обеспечивающего функционирование информационных систем, или по заявкам подразделений, эксплуатирующих информационные системы, согласованным с подразделением, обеспечивающим функционирование информационных систем. Сведения о созданной, измененной, заблокированной учетной записи и ее правах доступа передаются в структурное подразделение, специалистам по защите информации для учета и контроля использования;

4) должна проводиться не реже одного раза в год оценка знаний работников, назначенных на роль системных администраторов и администраторов безопасности, мер по защите информации, установленных настоящим методическим документом, внутренними регламентами и стандартами в части касающейся;

5) в случае предоставления удаленного привилегированного доступа действия системных администраторов и администраторов безопасности подлежат постоянному мониторингу с записью действий в журналы событий безопасности и их хранением на машинных носителях информации не менее 6 месяцев;

6) применение средств, систем геопозиционирования программно-аппаратных средств, обеспечивающих определение места, из которого осуществляется удаленный привилегированный доступ;

7) при удаленном привилегированном доступе для выполнения ролей системных администраторов и администраторов безопасности должен быть обеспечен контроль загружаемых администраторами в информационные системы файлов на наличие в них вредоносного программного обеспечения, а также контроль выгружаемых администраторами файлов с целью выявления нарушений требований внутренних регламентов по обработке конфиденциальной информации.

3.11. Обеспечение мониторинга информационной безопасности (МБ)

Цель: Выявление признаков реализации угроз безопасности информации и (или) нарушений требований внутренних стандартов и регламентов по защите информации на основе сбора данных о событиях безопасности, их обработки и анализа.

Требования к реализации: Мониторинг информационной безопасности должен предусматривать:

сбор данных о событиях безопасности и иных данных мониторинга информационной безопасности, предусмотренных национальным стандартом Российской Федерации ГОСТ Р 59547-2021 «Защита информации. Мониторинг информационной безопасности. Общие положения» (далее – данные мониторинга);

обработку данных о событиях безопасности и иных данных мониторинга;

анализ событий безопасности и иных данных мониторинга;

сопоставление событий безопасности и иных данных мониторинга с характеристиками угроз безопасности информации;

контроль, учет и анализ действий пользователей информационных систем;

сбор и анализ данных о результатах контроля потоков информации в информационных системах;

выявление нарушений безопасности информации и (или) функционирования информационных систем и реагирование на них;

своевременное информирование о выявленных нарушениях безопасности информации и (или) нарушениях функционирования информационных систем.

Требования к документированию: Внутренний регламент, определяющий порядок мониторинга информационной безопасности информационных систем, должен содержать:

перечень подразделений (работников), на которые возложены функции по мониторингу информационной безопасности, их функции (обязанности) и права;

перечень и содержание мероприятий по мониторингу информационной безопасности;

перечень действий подразделений, пользователя в случае выявления

по результатам мониторинга информационной безопасности факта или признаков реализации угроз безопасности информации;

схемы взаимодействия подразделений (работников) при осуществлении мониторинга информационной безопасности (при необходимости).

Во внутреннем стандарте устанавливаются требования к сбору, регистрации и анализу событий безопасности, подлежащих мониторингу информационной безопасности.

Требования к усилению:

1) создание и обеспечение функционирования отдельного структурного подразделения по мониторингу информационной безопасности;

2) привлечение специализированной организации, имеющей лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации с правом оказания услуг по мониторингу информационной безопасности средств и систем информатизации[5] (далее – специализированная организация). В случае привлечения специализированной организации определяются работники структурного подразделения, специалисты по защите информации, ответственные за прием информации о результатах мониторинга информационной безопасности от специализированной организации, реагирование на выявленные актуальные угрозы безопасности информации;

3) должны применяться технические средства однонаправленного ответвления сетевого трафика;

4) должны применяться пассивные (энергонезависимые) технические средства однонаправленного ответвления сетевого трафика.

3.12. Обеспечение разработки безопасного программного обеспечения (БР)

Цель: Предотвращение появления, выявление и устранение уязвимостей при разработке программного обеспечения в информационной системе.

Требования к реализации: Разработка безопасного программного обеспечения должна предусматривать:

планирование мероприятий по разработке безопасного программного обеспечения;

обучение работников, осуществляющих разработку, поддержку безопасного программного обеспечения;

---

[5] Подпункт «в» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79.

формирование и предъявление требований по безопасности к программному обеспечению, включая требования к его архитектуре;

управление конфигурацией программного обеспечения;

управление недостатками и запросами на изменение безопасного программного обеспечения;

разработку, уточнение и анализ архитектуры программного обеспечения, обеспечивающей снижение или исключение возникновения потенциальных уязвимостей;

моделирование актуальных угроз и разработку описания поверхности атак;

формирование и поддержание в актуальном состоянии правил безопасного кодирования;

экспертизу исходного кода программного обеспечения;

проведение статического, динамического анализа кода программ;

использование безопасной системы сборки программного обеспечения;

обеспечение безопасности сборочной среды программного обеспечения;

управление доступом и контроль целостности программного кода в ходе разработки программного обеспечения;

проведение композиционного анализа программного обеспечения;

проверку программного кода на предмет внедрения вредоносного программного обеспечения через цепочки поставок его составных частей;

функциональное и нефункциональное тестирование программного обеспечения;

обеспечение безопасности при выпуске готовой к эксплуатации версии программного обеспечения;

безопасную доставку и установку программного обеспечения в информационных системах;

обеспечение поддержки программного обеспечения при эксплуатации пользователями;

реагирование на информацию об уязвимостях программного обеспечения, поступающую от пользователей;

устранение уязвимостей программного обеспечения, выявленных в ходе его эксплуатации;

поиск уязвимостей в программном обеспечении и разработку мер по их устранению.

Требования к документированию: Внутренний регламент по разработке безопасного программного обеспечения[6], в случае его самостоятельной

[6] Пункт 3.2 национального стандарта Российской Федерации ГОСТ Р 56939-2024
(М., ФГБУ «РСТ», 2024) (далее – ГОСТ Р 56939-2024).

разработки оператором (обладателем информации), должен содержать:

состав программного обеспечения, на разработку и эксплуатацию которого распространяются мероприятия (процессы) по разработке безопасного программного обеспечения;

перечень подразделений (работников), на которых возложены функции по организации и внедрению процессов разработки безопасного программного обеспечения, их функции и полномочия;

состав и содержание мероприятий (процессов) по разработке безопасного программного обеспечения;

перечень инструментальных средств, используемых при реализации мероприятий (процессов) по разработке безопасного программного обеспечения;

перечень подразделений (работников), на которых возложены функции по контролю процессов разработки безопасного программного обеспечения, их функции и полномочия;

описание порядка взаимодействия работников оператора при осуществлении разработки безопасного программного обеспечения.

Требования к усилению:

1) поиск уязвимостей в программном обеспечении в рамках открытых программ с привлечением внешних экспертов и разработка мер по их устранению.

3.13. Обеспечение физической защиты информационных систем (ФЗ)

Цель: Исключение возможности несанкционированного физического доступа к программно-аппаратным средствам обработки и хранения информации.

Требования к реализации: Мероприятия по обеспечению физической защиты информационных систем должны предусматривать:

определение программно-аппаратных средств информационных систем, предназначенных для обработки и (или) хранения информации, несанкционированный физический доступ к которым должен быть исключен (далее – средства обработки и хранения информации);

определение перечня лиц (категорий лиц), которым разрешен доступ в помещения (зоны помещений) и (или) физический доступ к средствам обработки и хранения информации, а также работников оператора, ответственных за контроль доступа в помещения (зоны помещений) и (или) к средствам обработки и хранения информации;

контроль физического доступа к средствам обработки и хранения информации и (или) в помещения (зоны помещений), в которых они установлены;

осуществление доступа посторонних лиц в помещения, в которых установлены средства обработки и хранения информации, и проведение в них работ только в сопровождении работников, ответственных за контроль доступа в помещения (зоны помещений), по согласованию со структурным подразделением, специалистами по защите информации;

размещение коммуникационного оборудования информационных систем в местах (шкафах, комнатах, ящиках), к которым исключен неконтролируемый доступ, определение перечня лиц, которым разрешен доступ к коммуникационному оборудованию, а также работников оператора, ответственных за контроль доступа к коммутационному оборудованию.

Физический доступ к средствам обработки и хранения информации должен быть предоставлен только тем пользователям, которым он необходим для выполнения возложенных на них обязанностей (функций).

Программно-аппаратные средства информационных систем, предназначенные для хранения информации, должны быть установлены в помещениях (зонах помещений, шкафах, футлярах, корпусах), несанкционированный физический доступ в которые должен быть исключен.

Запрещается оставлять съемные машинные носители информации, предназначенные для использования в информационных системах, а также незаблокированные экраны компьютеров с размещенной на них информацией на рабочих местах работников в нерабочее время за исключением помещений, в которых разрешено хранение информации в нерабочее время.

Контроль физического доступа к средствам обработки и хранения информации ограниченного доступа и (или) в помещения (зоны помещений, шкафы, футляры, корпуса), в которых они установлены, должен осуществляться в соответствии с внутренними регламентами по защите информации.

Съемные машинные носители информации, разрешенные для использования в информационных системах, подлежат учету и контролю использования. В информационных системах должны использоваться только съемные машинные носители информации, выдаваемые оператором (обладателем информации). В случае обнаружения пользователем съемного машинного носителя информации, принадлежность которого или владельца которого установить не удалось, такой съемный машинный носитель информации должен быть передан в структурное подразделение, специалистам по защите информации для анализа содержащихся на нем информации, программ и при необходимости дальнейшего уничтожения. Подключение обнаруженного съемного машинного носителя информации к информационным системам запрещается.

Требования к документированию: Внутренний регламент по обеспечению физической защиты информационных систем должен предусматривать:

состав средств обработки и хранения информации;

перечень помещений (зон помещений, шкафов, футляров, корпусов), в которых установлены, хранятся средства обработки и хранения информации;

перечень лиц (категорий лиц), которым разрешен доступ в помещения (зоны помещений) и (или) физический доступ к средствам обработки и хранения информации, а также работников оператора, ответственных за контроль доступа в помещения (зоны помещений) и (или) к средствам обработки и хранения информации;

состав и содержание мероприятий по контролю физического доступа в помещения (зоны помещений) и (или) к средствам обработки и хранения информации.

Требования к усилению:

1) применение автоматизированных систем контроля и управления доступом и (или) видеонаблюдения для контроля доступа в помещения (зоны помещений), в которых установлены средства обработки и хранения информации, а также к местам установки коммуникационного оборудования.

3.14. Обеспечение непрерывности функционирования информационных систем при возникновении нештатных ситуаций (НФ)

Цель: Обеспечение возможности восстановления выполнения социально значимых функций, иных функций (процессов, видов работ) информационных систем, для которых установлены требования к непрерывному режиму функционирования (далее – значимые функции), в пределах интервалов времени восстановления, установленных внутренними стандартами и регламентами по защите информации.

Требования к реализации: Мероприятия по обеспечению непрерывности функционирования информационных систем при возникновении нештатных ситуаций должны предусматривать:

определение значимых функции;

определение перечня программных, программно-аппаратных средств, обеспечивающих выполнение значимых функций;

определение перечня нештатных ситуаций, при возникновении которых должна быть обеспечена непрерывность выполнения значимых функций;

определение интервалов времени восстановления функционирования информационных систем, их сегментов, выполняющих значимые функции;

создание достаточного количества резервных копий программных, программно-аппаратных средств и их конфигураций, обеспечивающих выполнение значимых функций, необходимых для восстановления выполнения значимых функций в установленный интервал времени восстановления, и периодическое тестирование таких средств на работоспособность;

назначение необходимых для проведения работ по восстановлению функционирования информационных систем работников;

создание достаточного количества резервных копий информации, необходимой для обеспечения выполнения значимых функций, а также их хранение на разных типах машинных носителей информации в местах, исключающих несанкционированный доступ к резервным копиям информации.

Мероприятия по обеспечению непрерывности функционирования информационных систем при возникновении нештатных ситуаций должны позволять восстановить выполнение значимые функции в пределах интервалов времени восстановления, установленных внутренними стандартами и регламентами по защите информации.

Интервалы времени восстановления функционирования информационных систем, их сегментов, выполняющих значимые функции, устанавливаются в соответствии с актами, на основании которых осуществляется создание, эксплуатация информационных систем, или требованиями обладателя информации в зависимости от значимости функций для обеспечения его деятельности.

Должно быть обеспечено резервное копирование информации, содержащейся в информационных системах, необходимой для обеспечения выполнения значимых функций, а также ее хранение в местах, исключающих несанкционированный доступ к ее копиям. Периодичность резервного копирования, места хранения резервных копий и уровень критичности резервируемой информации определяется во внутренних регламентах.

Время восстановления устанавливается оператором в соответствии с актами, на основании которых осуществляется создание, функционирование информационных систем, или требованиями обладателя информации с учетом значимости функций для обеспечения его деятельности. В случае невозможности восстановления функционирования информационной системы в установленное время должно быть обеспечено информирование пользователей о прогнозируемых сроках восстановления функционирования информационных систем.

Доступ к значимым функциям информационной системы, для которых требуется восстановление в пределах установленного времени восстановления, должен осуществляться с использованием дублированных каналов передачи данных, которые предоставляются разными операторами связи и (или) разными

информационно-телекоммуникационными системами.

Должны проводиться периодические проверки возможности восстановления выполнения значимых функций с использованием резервных копий программных, программно-аппаратных средств и информации, необходимой для их выполнения, с привлечением работников, задействованных в проведении работ по восстановлению функционирования информационных систем.

В случае проведения мероприятий по восстановлению функционирования информационных систем, их сегментов, выполняющих значимые функции, с превышением интервалов времени их восстановления должна быть обеспечена возможность выполнения пользователями значимых функций, в том числе в неавтоматизированном режиме, в соответствии с внутренними регламентами по защите информации.

Требования к документированию: Во внутренних стандартах по обеспечению непрерывности функционирования устанавливаются:

состав значимых функций;

перечень нештатных ситуаций, при возникновении которых должна быть обеспечена непрерывность выполнения значимых функций;

интервалы времени восстановления функционирования информационных систем, их сегментов, выполняющих значимые функции;

требования к количеству резервных копий программных, программно-аппаратных средств и их конфигураций, обеспечивающих выполнение значимых функций, необходимых для восстановления выполнения значимых функций в установленный интервал времени восстановления;

требования к местам хранения резервных копий на разных типах машинных носителей информации.

Внутренний регламент, определяющий порядок обеспечения непрерывности функционирования, должен содержать:

состав подразделений (работников), ответственных за проведение работ по восстановлению функционирования информационных систем, их функции и полномочия;

состав и содержание мероприятий по восстановлению функционирования информационных систем;

порядок проведения проверок (тренировок) по восстановлению функционирования информационных систем.

Требования к усилению:

1) применение программных, программно-аппаратных средств, обеспечивающих выполнение значимых функций, в отказоустойчивой конфигурации, обеспечивающей восстановление выполнения значимых функций в установленный оператором (обладателем информации) интервал времени восстановления;

2) проведение периодических тренировок по восстановлению выполнения значимых функций с использованием резервных копий программных, программно-аппаратных средств и информации, необходимой для их выполнения, с привлечением работников, задействованных в проведении работ по восстановлению функционирования информационных систем. Положительным результатом проверок является возможность восстановления непрерывности функционирования информационных систем в установленные интервалы времени восстановления;

3) введение дежурств работников, обеспечивающих восстановление информационных систем в установленные интервалы, для обеспечения функционирования информационных систем;

4) применение систем мониторинга производительности и доступности средств вычислительной техники;

5) внедрение в информационной системе аппаратных средств гарантированной блокировки незадействованных линий резервного копирования данных;

6) использование средств синхронной настройки параметров безопасности общесистемного программного обеспечения и средств защиты информации при восстановлении функционирования информационной системы и ее системы защиты информации.

3.15. Повышение уровня знаний и информированности пользователей по вопросам защиты информации (УЗ)

Цель: Снижение возможности реализации угроз безопасности информации, связанных с недостаточным уровнем знаний (информированности), а также с воздействием нарушителей на пользователей, и реализации методов социальной инженерии.

Требования к реализации: Мероприятия по повышению уровня знаний и информированности пользователей по вопросам защиты информации должны включать:

доведение до пользователей политики, стандартов и регламентов по защите информации, а также иных информационных материалов, в том числе в форме памяток, баннеров, буклетов, по актуальным вопросам защиты информации;

проведение лекций, семинаров, обучающих игр по вопросам защиты информации.

Должны быть определены категории работников, для которых проводятся мероприятия по повышению уровня знаний и компетенций по вопросам защиты информации, а также работники, ответственные за организацию

и принятие мер по повышению уровня знаний и компетенций работников по вопросам защиты информации. Периодичность мероприятий по повышению уровня знаний и компетенций работников по вопросам защиты информации, а также привлекаемые для этого лица и используемые ими средства определяются во внутренних регламентах по защите информации.

Применяемые оператором (обладателем информации) способы повышения уровня знаний пользователей по вопросам защиты информации, периодичность и формы оценки уровня знаний должны определяться во внутренних регламентах по защите информации. Оценка уровня знаний должна проводиться в соответствии с внутренними стандартами и регламентами по защите информации. Для пользователей, показавших неудовлетворительный уровень знаний по вопросам защиты информации, должно быть организовано повторное прохождение обучающих курсов по вопросам защиты информации.

Работниками, ответственными за организацию и принятие мер по повышению уровня знаний и компетенций работников по вопросам защиты информации, проводится периодическое тестирование уровня знаний и компетенций работников по вопросам защиты информации. Периодичность и формы тестирования работников определяются во внутренних регламентах по защите информации.

Структурным подразделением, специалистами по защите информации ведется учет работников, систематически показывающих неудовлетворительный уровень знаний и компетенций по вопросам защиты информации. Сведения по указанным работникам представляются руководителю оператора, ответственному лицу при принятии управленческих решений.

Требования к документированию: Внутренний регламент по повышению уровня знаний и информированности пользователей по вопросам защиты информации должен включать:

перечень подразделений (работников, категорий работников), для которых требуется повышение уровня знаний и информированности пользователей по вопросам защиты информации;

описание применяемых способов повышения уровня знаний и компетенций работников по вопросам защиты информации, и условий их использования;

состав и содержание мероприятий по повышению уровня знаний и информированности пользователей по вопросам защиты информации, периодичность их проведения;

перечень подразделений (работников), ответственных за организацию и проведение повышения уровня знаний и информированности пользователей по вопросам защиты информации;

порядок проведения тренировок с пользователями по практической

отработке мероприятий по защите информации и формированию навыков по защите информации.

Требования к усилению:

1) проведение имитационных рассылок электронных писем на служебные адреса электронной почты, иные служебные средства коммуникаций с целью оценки устойчивости пользователей к методам социальной инженерии;

2) проведение тренировок с пользователями по практической отработке мероприятий по защите информации, предусмотренных внутренними регламентами по защите информации, и формированию навыков по защите информации;

3) разработка курсов для повышения уровня знаний и компетенций работников по вопросам защиты информации, организация периодического повышения уровня знаний и компетенций работников по вопросам защиты информации в соответствии с разработанными курсами;

4) разработка специализированных курсов для повышения уровня знаний и компетенций работников по вопросам защиты информации, предусматривающих углубленные знания способов и средств защиты информации, а также проведение тренингов по администрированию информационных систем и средств защиты информации;

5) использование автоматизированных систем (программных платформ), разрабатываемых оператором самостоятельно или доступных для приобретения или свободного использования в сети «Интернет», для обучения и прохождения тестирования уровня знаний и компетенций работников по вопросам защиты информации;

6) осуществление внеочередной проверки уровня знаний и компетенций по вопросам защиты информации работников, нарушивших внутренние стандарты или регламенты по защите информации.

3.16. Обеспечение защиты информации при взаимодействии с подрядными организациями (ЗП)

Цель: Исключение возможности несанкционированного доступа или воздействий на информационные системы и содержащуюся в них информацию через взаимодействующие с информационными системами программно-аппаратные средства подрядных организаций или каналы передачи данных и интерфейсы, используемые для доступа подрядных организаций к информационным системам.

Требования к реализации: Должны быть определены информационные системы, программные, программно-аппаратные средства и состав информации, к которым подрядным организациям предоставляется доступ

для выполнения условий договора, и обеспечен контроль доступа подрядных организаций к информационным системам, программным, программно-аппаратным средствам и информации.

В договорах или иных документах, на основании которых подрядным организациям предоставлен доступ к информационным системам или передана содержащаяся в них информация, должна быть предусмотрена необходимость обеспечения подрядными организациями защиты информации, к которой получен доступ, а также установлена ответственность за нарушения данных требований оператора. Не допускается копирование подрядными организациями информации, к которой им предоставлен доступ, в случае если это не предусмотрено в договорах или иных документах, на основании которых получен доступ к информационным системам.

Предоставление доступа к информационным системам, программным, программно-аппаратным средствам и информации работникам подрядных организаций осуществляется по заявке подразделения, обеспечивающего функционирование информационных систем, согласованной со структурным подразделением, специалистами по защите информации, или с использованием систем управления привилегированными учетными записями.

Для доступа работников подрядных организаций должны быть созданы отдельные учетные записи с правами доступа, минимально необходимыми для выполнения условий договора.

Подрядные организации должны осуществлять использование созданных для них учетных записей в соответствии с настоящим методическим документом, внутренними регламентами и стандартами по защите информации.

Должен осуществляться мониторинг и регистрация действий учетных записей, выделенных для подрядных организаций. При обнаружении попыток нарушения правил разграничения доступа или иных действий, не предусмотренных договором с подрядной организацией, учетные записи подрядных организаций незамедлительно блокируются.

В случае использования работниками подрядных организаций в ходе проведения работ по обслуживанию, сопровождению, иных регламентных работ в информационных системах отдельных программно-аппаратных средств в таких средствах должны использоваться средства защиты информации, исключающие несанкционированный доступ к ним.

В информационных системах, отдельных программно-аппаратных средствах подрядных организаций, в которых осуществляются обработка и хранение полученной в результате предоставленного доступа информации, должны быть приняты меры по защите информации.

Порядок вывода разработанного программного обеспечения из контуров разработки и (или) тестирования в эксплуатируемые информационные системы

оператора определяется во внутренних регламентах по защите информации, которые должны быть доведены до работников подрядных организаций в части их касающейся.

Разработка (развитие) и (или) тестирование программного обеспечения подрядными организациями непосредственно в контуре промышленной эксплуатации информационных систем оператора (обладателя информации) не допускается. Для проведения работ по разработке (развитию) и (или) тестированию программного обеспечения работникам подрядных организаций должен быть предоставлен доступ к специально выделенным для проведения таких работ стендам разработки и (или) тестирования. Контроль доступа подрядных организаций к стендам разработки (развития) и (или) тестирования должен осуществляться в соответствии с внутренними регламентами по защите информации.

Удаленный доступ работников подрядных организаций к информационным системам и содержащейся в них информации осуществляется с использованием шифровальных (криптографических) средств защиты информации, обеспечивающих защиту каналов передачи данных.

Удаленный доступ подрядных организаций к информационным системам должен осуществляться только с программно-аппаратных средств, размещенных на территории Российской Федерации.

В договорах или иных документах, на основании которых подрядным организациям предоставлен доступ к информационным системам или передана содержащаяся в них информация, должна быть предусмотрена необходимость обеспечения подрядными организациями защиты информации, к которой получен доступ, а также установлена ответственность за нарушения данных требований оператора.

В случае если в результате предоставленного доступа в информационных системах подрядных организаций осуществляется обработка и хранение полученной информации, в них должны быть приняты меры по защите информации в соответствии с настоящим методическим документом. Состав информации, цели ее защиты и классы защищенности, в соответствии с которыми подрядными организациями должны быть приняты меры по защите информации во взаимодействующих информационных системах, согласуются с оператором (обладателем информации).

Требования к документированию: Внутренний регламент по предоставлению работникам подрядных организаций доступа к информационным системам и содержащейся в них информации должен содержать:

цели предоставления подрядным организациям доступа к информационным системам и содержащейся в них информации, категории подрядных организаций, которым возможно предоставление доступа к информационным системам и содержащейся в них информации;

перечень информационных систем, сегментов информационных систем, отдельных программно-аппаратных средств, стендов разработки и тестирования, а также категории информации, к которым подрядным организациям предоставляется доступ;

виды доступа подрядных организаций к информационным системам и содержащейся в них информации, функции и полномочия подрядных организаций при каждом виде доступа;

основания и порядок предоставления доступа подрядных организаций к информационным системам и содержащейся в них информации;

условия предоставления доступа подрядных организаций к информационным системам и содержащейся в них информации, в том числе меры по защите программно-аппаратных средств, информационных систем, каналов передачи данных, используемых подрядными организациями;

обязанности и ответственность подрядных организаций при обработке и хранении информации оператора (обладателя), в том числе порядок удаления информации;

перечень подразделений (работников), ответственных за контроль выполнения подрядными организациями требований по защите информации, и порядок проведения контроля.

Требования к усилению:

1) должно быть обеспечено централизованное управление учетными записями (группами учетных записей) подрядных организаций и их аутентификационной информацией;

2) должны применяться средства, системы геопозиционирования программно-аппаратных средств, обеспечивающие определение места, из которого осуществляется удаленный доступ;

3) должен быть обеспечен контроль загружаемых подрядными организациями в информационные системы файлов на наличие в них вредоносного программного обеспечения, а также контроль выгружаемых подрядными организациями файлов.

3.17. Обеспечение защиты от компьютерных атак, направленных на отказ в обслуживании (ОО)

Цель: Исключение возможности блокирования доступа к информационным системам и (или) содержащейся в них информации

вследствие воздействий на интерфейсы, к которым должен быть обеспечен постоянный доступ из сети «Интернет».

Требования к реализации: Обеспечение защиты информационных систем от атак, направленных на отказ в обслуживании, должно предусматривать:

определение интерфейсов и сервисов информационных систем, которые должны быть постоянно доступны из сети «Интернет», и определение их принадлежности и назначения;

выявление публичных сетевых адресов, зарегистрированных за оператором и (или) полученных от провайдера хостинга, и доменных имен, используемых для обеспечения функционирования информационных систем, и определение их назначения;

ограничение доступа к интерфейсам и сервисам информационных систем, доступных из сети «Интернет», публичных сетевых адресов и доменных имен, не используемых для эксплуатации и (или) обеспечения функционирования информационных систем;

определение сетевых адресов, с которыми должно быть обеспечено взаимодействие информационных систем, и формирование списка разрешенных сетевых адресов в условиях реализации компьютерных атак, направленных на отказ в обслуживании;

использование программных, программно-аппаратных средств, обеспечивающих анализ и фильтрацию входящего трафика в соответствии с матрицей коммуникаций информационных систем с сетью «Интернет», и возможность блокирования входящего трафика, обладающего признаками компьютерных атак, направленных на отказ в обслуживании, от сетевого до прикладного уровня информационных систем;

использование данных информационной системы определения страновой принадлежности сетевых адресов центра мониторинга и управления сетями связи общего пользования[7] (GeoIP);

обеспечение хранения информации о фактах реализации атак, направленных на отказ в обслуживании, в соответствии с внутренними стандартами и регламентами по защите информации;

[7] Положения о Центре мониторинга и управления сетью связи общего пользования, утвержденного приказом Роскомнадзора от 31 июля 2019 г. № 225 (зарегистрирован Минюстом России 22 ноября 2019 г., регистрационный № 56583), с изменениями, внесенными приказом Роскомнадзора от 24 апреля 2024 г. № 73 (зарегистрирован Минюстом России 6 июня 2024 г., регистрационный № 78486).

анализ логической схемы сети с целью выявления сетевых узлов (сегментов) на пути прохождения трафика для выявления низкой пропускной способности.

Меры по защите от компьютерных атак, направленных на отказ в обслуживании, принимаются в отношении информационных систем, имеющих интерфейсы и сервисы, которые должны быть доступны из сети «Интернет».

Должно обеспечиваться взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Также должно быть обеспечено взаимодействие с Центром мониторинга и управления сетью связи общего пользования[8] при наличии такой возможности.

Мероприятия по обеспечению защиты от компьютерных атак, направленных на отказ в обслуживании, реализуются самостоятельно оператором (обладателем информации), и (или) с привлечением провайдеров хостинга, и (или) организаций, предоставляющих услуги связи, и (или) организаций, оказывающих услуги по контролю, фильтрации и блокированию сетевых запросов, обладающих признаками компьютерных атак, направленных на отказ в обслуживании.

С целью блокирования входящего трафика, обладающего признаками компьютерных атак, направленных на отказ в обслуживании, с участием организаций, предоставляющих услуги связи, или организаций, оказывающих услуги по контролю, фильтрации и блокированию сетевых запросов, обладающих признаками компьютерных атак, направленных на отказ в обслуживании, разрабатывается шаблон фильтрации атак, а также порядок взаимодействия по совместному блокированию компьютерных атак, направленных на отказ в обслуживании, в том числе на основе определения страновой принадлежности сетевых адресов, и разграничению зон ответственности при таком блокировании, а также содержащий порядок формирования перечней сетевых адресов, с которых идет компьютерная атака, направленная на отказ в обслуживании, или иных признаков атак, определение и передача «белых» списков сетевых адресов.

Требования к документированию: Во внутреннем стандарте, устанавливающем требования к непрерывности функционирования информационных систем, устанавливаются:

---

[8] Пункт 5 Положения о Центре мониторинга и управления сетью связи общего пользования, утвержденного приказом Роскомнадзора от 31 июля 2019 г. № 225 (зарегистрирован Минюстом России 22 ноября 2019 г., регистрационный № 56583), с изменениями, внесенными приказом Роскомнадзора от 24 апреля 2024 г. № 73 (зарегистрирован Минюстом России 6 июня 2024 г., регистрационный № 78486).

перечень подразделений (работников), на которых возложены функции по обеспечению защиты от компьютерных атак, направленных на отказ в обслуживании;

порядок действий подразделений (работников) при обеспечении защиты от компьютерных атак, направленных на отказ в обслуживании;

порядок взаимодействия оператора информации с провайдером хостинга или организацией, предоставляющей услуги связи, или организацией, оказывающей услуги по контролю, фильтрации и блокированию сетевых запросов, обладающих признаками компьютерных атак, направленных на отказ в обслуживании;

время восстановления функционирования в случае нарушения штатного режима функционирования вследствие реализации компьютерных атак, направленных на отказ в обслуживании.

Требования к усилению:

1) наличие системы мониторинга ресурсов и метрик производительности серверов, средств связи и средств защиты информации, используемых на пути прохождения трафика от точки публикации защищаемого ресурса до конечного хоста внутри информационной системы.

3.18. Обеспечение защиты информации при использовании искусственного интеллекта (ИИ)

Цель: Исключение возможности несанкционированного доступа к информационным системам и информации при использовании систем искусственного интеллекта.

Требования к реализации: Посредством проведения мероприятий по обеспечению защиты информации при использовании систем искусственного интеллекта[9] должна быть исключена возможность нарушения конфиденциальности, целостности и доступности информации, обрабатываемой в системе искусственного интеллекта, за счет действий внешних и внутренних нарушителей.

При создании систем искусственного интеллекта оператором (обладателем информации) должна быть проведена оценка угроз безопасности информации, связанных с разработкой и эксплуатацией системы искусственного интеллекта. Сведения об угрозах безопасности информации систем искусственного интеллекта содержатся в банке данных угроз безопасности информации ФСТЭК России.

[9] Подпункт «а» пункта 5 Национальной стратегии развития искусственного интеллекта.

По результатам оценки угроз безопасности информации должно быть разработано техническое задание, содержащее требования к реализации мер защиты информации в системе искусственного интеллекта.

При разработке системы искусственного интеллекта должна быть обеспечена защита следующих объектов:

объекты информационной инфраструктуры разработки системы искусственного интеллекта;

программное обеспечение, обеспечивающее разработку системы искусственного интеллекта (подготовка наборов обучающих данных, обучение и тестирование моделей искусственного интеллекта), в том числе входящие в его состав фреймворки, библиотеки, иные инструменты;

программное обеспечение, обеспечивающее разработку API-интерфейсов, агентов, системы фильтрации входных и выходных данных;

входная модель искусственного интеллекта, используемая для разработки (обучения) выходной модели искусственного интеллекта (при наличии);

наборы обучающих данных;

выходная модель искусственного интеллекта и ее параметры (веса);

программное обеспечение, обеспечивающее реализацию технологий искусственного интеллекта (модели искусственного интеллекта), а также агентов искусственного интеллекта, API-интерфейсов, систем фильтрации (контроля) входных и выходных данных.

В информационной инфраструктуре разработки системы искусственного интеллекта должны быть реализованы меры по защите информации по классу защищенности не ниже класса защищенности информационной системы оператора (обладателя информации).

Дополнительно в информационной инфраструктуре разработки должны быть обеспечены:

выделение информационной инфраструктуры разработки системы искусственного интеллекта от иной инфраструктуры разработчика, не связанной с разработкой данной системы, в отдельный изолированный сегмент;

отказ от использования небезопасных форматов обработки и хранения данных (например, pickle) и применение безопасных форматов данных (ONNX, protobuf и другие форматы);

целостность программного обеспечения, реализующего разработку системы искусственного интеллекта.

В информационной инфраструктуре разработки системы искусственного интеллекта не допускается решение задач, не связанных с разработкой системы искусственного интеллекта.

В отношении наборов обучающих данных должны быть обеспечены:

применение в приоритетном порядке наборов обучающих данных

из доверенных источников (например, информационные системы государственных органов, организаций и учреждений, значимые объекты критической информационной инфраструктуры Российской Федерации);

антивирусная проверка обучающих данных на предмет наличия в них вредоносного программного обеспечения;

хранение обучающих данных в обособленном хранилище;

целостность обучающих данных.

При использовании входной модели искусственного интеллекта должен быть проведен анализ сведений об уязвимостях указанной модели, получаемых из внешних источников (базы данных известных уязвимостей, официальные ресурсы разработчиков программных средств, специализированные публикации, форумы, иные источники). В отношении выявленных уязвимостей разработчиков системы искусственного интеллекта должны быть приняты меры, направленные на нейтрализацию выявленных уязвимостей.

В отношении программного обеспечения, обеспечивающего разработку и эксплуатацию системы искусственного интеллекта, должен быть проведен анализ уязвимостей программного обеспечения на основании данных, получаемых из внешних источников (базы данных известных уязвимостей, официальные ресурсы разработчиков программных средств, специализированные публикации, форумы, иные источники), и приняты меры по их устранению.

При эксплуатации системы искусственного интеллекта в информационной системе должна быть обеспечена защита следующих объектов:

объекты информационной инфраструктуры, обеспечивающей эксплуатацию системы искусственного интеллекта;

программное обеспечение, обеспечивающее реализацию технологий искусственного интеллекта (модели искусственного интеллекта), а также агентов искусственного интеллекта, API-интерфейсов, систем фильтрации (контроля) входных и выходных данных;

обученная и готовая к использованию модель искусственного интеллекта, ее расширения (LoRA, RAG и другие расширения (при необходимости).

В случае если для эксплуатации системы искусственного интеллекта используется инфраструктура, не входящая в информационную систему оператора, то в такой инфраструктуре должны быть реализованы меры по защите информации по классу защищенности не ниже класса защищенности информационной системы оператора (обладателя информации).

В случае применения технологии искусственного интеллекта в составе информационной системы оператором (обладателем информации) должны быть приняты меры защиты информации, направленные на предотвращение несанкционированного доступа или воздействия на систему искусственного

интеллекта, в соответствии с требованиями по защите информации (обеспечению безопасности), в том числе меры по:

идентификации и аутентификации пользователей системы искусственного интеллекта;

управлению доступом пользователей системы искусственного интеллекта;

контролю (фильтрации) входных и выходных данных;

обеспечению изоляции системы искусственного интеллекта;

защите данных системы искусственного интеллекта;

защите от вредоносного программного обеспечения;

выявлению уязвимостей в системе искусственного интеллекта;

ограничению и контролю функциональности системы искусственного интеллекта.

В информационной системе при эксплуатации системы искусственного интеллекта дополнительно должны быть реализованы следующие меры защиты информации:

обеспечение фильтрации (контроля) входных данных (запросов) системы искусственного интеллекта;

обеспечение фильтрации (контроля) выходных данных (ответов) системы искусственного интеллекта;

мониторинг и квотирование количества запросов к системе искусственного интеллекта;

обеспечение регистрации событий безопасности, связанных с запросами к системе искусственного интеллекта и ее ответами;

обеспечение целостности параметров (весов) модели искусственного интеллекта и конфигурации системы искусственного интеллекта.

В отношении программного обеспечения, реализующего технологию искусственного интеллекта, оператор совместно с разработчиком системы искусственного интеллекта должен проводить анализ уязвимостей программного обеспечения на основании данных, получаемых из внешних источников (базы данных известных уязвимостей, официальные ресурсы разработчиков программных средств, специализированные публикации, форумы, иные источники), и принимать меры по их устранению.

При предоставлении подрядной организации систем искусственного интеллекта в качестве внешнего сервиса, в информационной инфраструктуре подрядной организации, с использованием которой функционирует указанный сервис должны быть реализованы мероприятия и меры по защите информации, установленные требованиями по защите информации (обеспечению безопасности) по классу защищенности не ниже класса защищенности информационной системы оператора (обладателя информации).

Взаимодействие информационной системы оператора (обладателя информации) с информационной инфраструктурой подрядной организации, используемой для предоставления системы искусственного интеллекта в качестве сервиса, должно осуществляться с учетом требований по защите информации (обеспечению безопасности).

В случае если в системе искусственного интеллекта осуществляется обработка персональных данных граждан Российской Федерации, иной информации ограниченного доступа и (или) с применением системы искусственного интеллекта обеспечивается реализация значимых функций оператора, необходимо:

обеспечить реализацию мероприятий по безопасной разработке программного обеспечения, обеспечивающего реализацию системы искусственного интеллекта, предусмотренных национальными стандартами в области разработки безопасного программного обеспечения;

провести сертификацию программного обеспечения, обеспечивающего реализацию системы искусственного интеллекта, по требованиям безопасности информации, утвержденным ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должно быть обеспечено выделение информационной инфраструктуры разработки от иной инфраструктуры разработчика, не связанной с разработкой данной системы, в отдельный физически изолированный сегмент;

2) должно быть обеспечено хранение наборов обучающих данных в зашифрованном виде с использованием шифровальных (криптографических) средств защиты информации;

3) в отношении выходной модели искусственного интеллекта и ее параметров (весов) должны быть обеспечены:

а) применение методов состязательного обучения (включение состязательных примеров в обучающую выборку);

б) внедрение механизмов ограничения допустимых диапазонов данных, санитизации входных данных;

4) должно быть реализовано тестирование на устойчивость к промпт-атакам;

5) должно быть обеспечено выделение системы искусственного интеллекта в информационной системе в отдельный изолированный сегмент информационной системы;

6) должна быть обеспечена целостность модели искусственного интеллекта с использованием шифровальных (криптографических) средств защиты информации.

3.19. Проведение периодического контроля уровня защищенности информации, содержащейся в информационных системах (ПК)

Цель: Своевременная оценка возможностей нарушения безопасности информации и (или) нарушения функционирования информационных систем внешними и внутренними нарушителями.

Требования к реализации: Контроль уровня защищенности информации проводится с использованием следующих методов:

выявление уязвимостей информационных систем и экспертная оценка возможности их использования нарушителем для нарушения безопасности информации и (или) нарушения функционирования информационных систем;

тестирование информационных систем путем моделирования реализации актуальных угроз с целью оценки возможностей проникновения в них или повышения привилегий с учетом реализованных мер и применяемых средств защиты информации.

Периодичность и методы контроля уровня защищенности информации устанавливаются оператором во внутренних регламентах по защите информации в соответствии с имеющимися у него силами и выделенными на эти цели средствами. При этом проведение контроля уровня защищенности информации одним из методов должно проводиться не реже чем один раз в три года или после компьютерного инцидента, произошедшего у оператора (обладателя информации). Методы контроля уровня защищенности информации и периодичность его проведения определяются оператором (обладателем информации) во внутреннем регламенте по защите информации.

В случае выявления по результатам контроля уровня защищенности информации возможности реализации актуальных угроз и (или) признаков реализации актуальных угроз структурным подразделением, специалистами по защите информации совместно с подразделением, обеспечивающим функционирование информационных систем, осуществляется разработка и реализация мер, направленных на оперативное их блокирование.

Требования к документированию: Внутренний регламент по порядку контроля уровня защищенности информации, содержащейся в информационных системах, должен содержать:

перечень информационных систем, в отношении которых проводится контроль уровня защищенности информации;

перечень подразделений (работников), ответственных за организацию

и проведение контроля уровня защищенности информации;

применяемые методы контроля уровня защищенности информации и используемые при их реализации программные средства контроля;

состав и содержание мероприятий, реализуемых при проведении контроля уровня защищенности информации;

описание действий подразделений (работников) оператора (обладателя информации) при выявлении по результатам контроля уровня защищенности информации недостатков и уязвимостей в системах защиты информационных систем.

Требования к усилению:

1) проведение контроля уровня защищенности информации должно проводиться не реже чем один раз в год;

2) проведение тренировок по отработке работниками оператора (обладателя информации) действий по обеспечению требуемого уровня защищенности информации, содержащейся в информационных системах, в условиях реализации актуальных угроз.

IV. МЕРЫ ПО ЗАЩИТЕ ИНФОРМАЦИОННЫХ СИСТЕМ И СОДЕРЖАЩЕЙСЯ В НИХ ИНФОРМАЦИИ

4.1. Идентификация и аутентификация (ИАФ)

ИАФ.1 Идентификация пользователей

Цель: Исключение доступа к информационной системе лиц, не являющихся пользователями информационной системы.

Требования к реализации: В информационной системе должна осуществляться идентификация пользователей, получающих доступ к информационной системе со средств вычислительной техники (в том числе автоматизированных рабочих мест, конечных устройств, мобильных устройств) для выполнения возложенных на пользователей обязанностей (функций) (далее – внутренние пользователи).

Ко внутренним пользователям относятся работники оператора (обладателя информации), заказчика информационной системы, а также подведомственных ему государственных органов и организаций при их наличии (непривилегированные пользователи, привилегированные пользователи, в том числе главный администратор, администраторы информационной системы, администраторы безопасности), выполняющие свои обязанности (функции) с использованием информации, информационных технологий и средств вычислительной техники информационной системы в соответствии с внутренними стандартами

и регламентами по защите информации и которым в информационной системе присвоены учетные записи.

В качестве внутренних пользователей также рассматриваются работники подрядных организаций, привлекаемые на договорной основе для оказания услуг, проведения работ по обработке, хранению информации, созданию (развитию), обеспечению эксплуатации информационных систем, а также для выполнения работ, оказания услуг по защите информации (разработка и тестирование программного обеспечения, обеспечение функционирования информационных систем или защита содержащейся в них информации) и которым в информационной системе также присвоены учетные записи.

При доступе в информационную систему должна осуществляться идентификация пользователей, получающих доступ к информационной системе со средств вычислительной техники, не входящих в состав информационной системы или для которых оператором информационной системы не могут устанавливаться и контролироваться требования о защите информации (далее – внешние пользователи).

Примером внешних пользователей являются граждане, на законных основаниях через сеть «Интернет» получающие доступ к информационным ресурсам Единого портала государственных и муниципальных услуг (функций) или официальным сайтам в сети «Интернет» органов государственной власти, физические и юридические лица, осуществляющие доступ к информационным системам для получения информации с применением учетных записей или без них (анонимные пользователи).

Пользователи информационной системы должны однозначно идентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации в соответствии с мерой защиты информации УПД.9.

Идентификация внешних пользователей в целях предоставления государственных услуг осуществляется в том числе с использованием единой системы идентификации и аутентификации, созданной в соответствии с постановлением Правительства Российской Федерации от 28 ноября 2011 г. № 977.

Идентификация пользователей должна производиться в два этапа: первичная и вторичная идентификация.

Первичная идентификация должна включать подготовку, формирование и регистрацию информации о пользователях, а также присвоение пользователю идентификатора доступа и его регистрацию в перечне присвоенных идентификаторов. Первичная идентификация пользователя должна проводиться один раз в момент установления личности физического лица, запрашивающего доступ к информационной системе.

Первичная идентификация пользователей должна завершаться регистрацией идентификационной информации и присвоенного пользователю уникального идентификатора доступа или отказом. Основанием для отказа в регистрации может быть несоответствие заявленных идентификационных данных требованиям к первичной идентификации, отрицательный результат, полученный в процессе их верификации.

Идентификационная информация, полученная в процессе первичной идентификации, должна обновляться при изменении идентификационных данных пользователей (например, при смене фамилии, при изменении номера мобильного телефона, если он используется для целей идентификации пользователя).

Вторичная идентификация должна включать проверку предъявленного пользователем идентификатора по списку зарегистрированных идентификаторов в информационной системе и опознавание пользователя. Вторичная идентификация является многократно повторяющимся процессом, осуществляющимся каждый раз при новом запросе пользователя на доступ к информационной системе и ресурсам (объектам защиты) информационной системы.

Первичная и вторичная идентификация пользователей осуществляется с учетом положений национальных стандартов ГОСТ Р 58833-2020 «Защита информации. Идентификация и аутентификация. Общие положения» и ГОСТ Р 70262.1-2022 «Защита информации. Идентификация и аутентификация. Уровни доверия идентификации».

В информационной системе должна быть обеспечена возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

В процессе сбора, передачи, обработки и хранения идентификационной и подтверждающей информации (в том числе персональных данных) должны быть реализованы меры по защите информации, обеспечивающие ее конфиденциальность, целостность и доступность.

В информационной системе должно быть реализовано управление идентификаторами, включающее:

определение работника оператора, ответственного за создание, присвоение и уничтожение идентификаторов пользователей;

формирование идентификатора, который однозначно идентифицирует пользователя;

присвоение идентификатора пользователю;

проверку личности пользователя при присвоении ему идентификатора;

предотвращение повторного использования идентификатора пользователя;

хранение и поддержание актуального состояния (обновление)

идентификационной информации пользователей;

блокирование идентификатора пользователя после установленного оператором времени неиспользования.

Идентификация пользователей обеспечивается применением входящих в состав информационной системы операционной системы, и (или) средств защиты информации от несанкционированного доступа, и (или) средствами защиты информации, обеспечивающими централизованное управление идентификаторами.

Требования к документированию: В эксплуатационной документации[10] на информационную систему должны быть определены:

перечень типов пользователей (пользователи, главный администратор, системные администраторы, администраторы безопасности, пользователи подрядных организаций, внешние пользователи и другие типы пользователей);

состав идентификационных данных для каждого типа пользователей, минимально необходимый для однозначной идентификации пользователей;

перечень разрешенных к применению средств, используемых для идентификации, в зависимости от ресурсов (объектов защиты) информационной системы, к которым пользователь получает доступ, и средств, с которых осуществляется доступ;

порядок верификации (проверки и подтверждения) идентификационной информации пользователей, порядок действий при выявлении несоответствий, правила проведения верификации;

правила формирования (создания) уникальных идентификаторов, их присвоения пользователям, регистрации идентификаторов в информационной системе;

порядок выдачи идентификаторов пользователям;

правила хранения, поддержания актуального состояния (обновления) идентификационной информации пользователей, периодичности обновления (актуализации) идентификационной информации пользователей и мест ее хранения, организации доступа к ней, отзыва идентификатора пользователя и удаления идентификационной и подтверждающей информации.

Требования к усилению:

1) в информационной системе должно быть реализовано централизованное управление идентификаторами.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1

[10] Национальный стандарт Российской Федерации ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

ИАФ.1	+	+	+
Усиление ИАФ.1		1	1

ИАФ.2 Идентификация устройств

Цель: Исключение подключения к информационным системам неидентифицированных устройств.

Требования к реализации: В информационной системе должен быть определен перечень типов сетевых устройств (в том числе серверы, автоматизированные рабочие места, телекоммуникационное оборудование, мобильные устройства, системы хранения данных), используемых в информационной системе.

Идентификации подлежат:

сетевые устройства, входящие в состав информационной системы (в том числе серверы, автоматизированные рабочие места, телекоммуникационное оборудование, системы хранения данных);

мобильные устройства внутренних пользователей информационной системы (при их подключении к информационной системе);

устройства, предназначенные для удаленного доступа работников подрядных организаций, иных государственных органов, организаций к информационным системам, содержащейся в них информации, и (или) передачи им информации.

Процесс идентификации должен осуществляться в два этапа – первичная идентификация и вторичная идентификация[11].

В ходе первичной идентификации в информационной системе должны быть определены уникальные признаки (атрибуты) каждого устройства (идентификационные данные). В качестве признаков (атрибутов) устройств могут использоваться логические имена (имя устройства и (или) ID), логические адреса (например, IP-адреса) и (или) физические адреса (например, MAC-адреса) устройств или их комбинации.

Каждому устройству информационной системы должен быть присвоен уникальный идентификатор или их комбинация для доступа в информационные системы.

Первичная идентификация устройств осуществляется единожды при регистрации каждого нового устройства.

Основанием для отказа в первичной идентификации является несоответствие заявленных идентификационных данных требованиям к первичной идентификации

[11] Национальный стандарт Российской Федерации ГОСТ Р 58833-2020 «Защита информации. Идентификация и аутентификация. Общие положения»

или невозможность их подтверждения в установленном порядке.

По результатам первичной идентификации у оператора должен быть сформирован перечень всех идентификаторов устройств, используемых в информационной системе.

В ходе вторичной идентификации выполняется проверка наличия у устройства, от имени которого осуществляется запрос доступа в информационную систему, идентификатора доступа.

При наличии предъявленного идентификатора доступа в перечне присвоенных идентификаторов процесс вторичной идентификации считается успешно пройденным, затем проводится аутентификация устройств в соответствии с мерой защиты информации ИАФ.4.

Вторичная идентификация проводится при каждом запросе на подключение устройства к информационной системе оператора (при начале информационного взаимодействия).

Идентификация устройств обеспечивается применением серверной операционной системы и (или) прошивкой сетевого устройства или иных средствам.

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены:

перечень типов устройств;

порядок верификации (проверки и подтверждения) идентификационной информации устройств, порядка действий при выявлении несоответствий, правил ее проведения;

порядок привязки идентификационной информации к устройству для каждой конкретной среды функционирования, условий эксплуатации и обслуживания;

состав идентификационных данных для каждого типа устройств минимально необходимый для однозначной идентификации устройств (объем, состав и уникальные признаки (атрибуты);

перечень исключений и порядок действий в случае, если объем идентификационных данных устройства недостаточен;

правила формирования (создания) уникальных идентификаторов, их присвоения устройствам, регистрации идентификаторов в информационной системе;

порядок действий оператора информационной системы по идентификации устройств.

Требования к усилению:

1) проведение инвентаризации идентификационных данных в информационной системе устройств не реже чем один раз в два года для информационных систем 1 класса защищенности;

2) проведение инвентаризации идентификационных данных

в информационной системе устройств не реже чем один раз в три года для информационных систем 2 и 3 классов защищенности;

3) применение вспомогательных атрибутов (электронных идентификаторов с уникальным машиночитаемым номером, встроенных модулей безопасности, средств доверенной загрузки);

4) реализация системы централизованного управления жизненным циклом цифровых сертификатов, электронных идентификаторов, встроенных модулей безопасности;

5) для информационных систем с доменной архитектурой:

наличие у оператора информационной системы центра сертификации, обеспечивающего регистрацию устройств, а также выпуск, обслуживание и валидацию машинных сертификатов (цифровых сертификатов доступа), доставку и установку выпущенных сертификатов в обслуживаемые устройства с использованием различных протоколов;

реализация (встроенная поддержка) протоколов аутентификации и работы с цифровыми сертификатами в устройстве (при наличии сетевых функций).

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ИАФ.2			
Усиление ИАФ.2			

ИАФ.3 Аутентификация пользователей

Цель: Исключение доступа к информационной системе пользователей, не прошедших процедуру аутентификации.

Требования к реализации: Аутентификация пользователей должна проводиться после их идентификации в информационной системе.

Пользователи информационной системы должны однозначно аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации в соответствии с мерой защиты информации УПД.9.

Аутентификация пользователей осуществляется с учетом положений национальных стандартов ГОСТ Р 58833-2020 «Защита информации. Идентификация и аутентификация. Общие положения» и ГОСТ Р 70262.2-2025 «Идентификация и аутентификация. Уровни доверия аутентификации».

Аутентификация для пользователя должна производиться при каждом запросе на доступ в информационную систему, а также к ресурсам (объектам защиты) информационной системы. Например, при входе в информационную систему пользователь проходит аутентификацию в операционной системе,

а затем аутентификацию при запросе на доступ к ресурсам информационной системы, под которыми понимаются системы управления базами данных, веб-порталы, системы электронного документооборота и иные ресурсы.При локальном доступе в информационную систему, а также к ресурсам (объектам защиты) информационной системы внутреннего непривилегированного пользователя должна как минимум осуществляться простая (парольная) аутентификация.

При использовании простой (парольной) аутентификации пользователей для доступа в информационную систему и к ресурсам (объектам защиты) информационной системы длина пароля должна быть не менее 12 символов. Алфавит паролей не менее 70 символов, максимальное количество неуспешных попыток ввода неправильного пароля до блокировки учетной записи пользователя – 5, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации на 15 минут, смена паролей не более чем через 90 дней. Запрещается повторно использовать пароль для доступа в информационную систему и к ресурсам (объектам защиты) информационной системы.

Защита обратной связи «система-пользователь» в процессе простой (парольной) аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками «*», «•» или иными знаками.

Усиленная аутентификация пользователей должна осуществляться при следующих условиях:

при удаленном доступе в информационную систему, а также к ресурсам (объектам защиты) информационной системы внутреннего непривилегированного пользователя;

при локальном доступе в информационную систему, а также к ресурсам (объектам защиты) информационной системы внутреннего привилегированного пользователя;

при удаленном доступе в информационную систему, а также к ресурсам (объектам защиты) информационной системы внутреннего привилегированного пользователя.

При доступе в информационную систему, а также к ресурсам (объектам защиты) информационной системы внешнего непривилегированного пользователя должна осуществляться простая (парольная) аутентификация.

При доступе в информационную систему, а также к ресурсам (объектам защиты) информационной системы внутреннего непривилегированного

пользователя с мобильных устройств, входящих в состав информационной системы, и с личных мобильных устройств должна осуществляться усиленная аутентификация.

Удаленный доступ в информационную систему, а также к ресурсам (объектам защиты) информационной системы внутренних привилегированных пользователей с личных мобильных устройств не допускается.

В таблице определены виды аутентификации, минимально необходимые для разных типов пользователей и условий доступа в информационную систему в зависимости от класса защищённости.

Тип пользователя	Тип доступа	Права доступа	Вид аутентификации		
			К3	К2	К1
Внутренний пользователь	Локальный	Непривилегированный	**П**	**У**	**У**
	Удалённый	Непривилегированный	**У**	**У**	**У**
Внутренний пользователь	Локальный	Привилегированный	**У**	**У**	**У**
	Удалённый	Привилегированный	**У**	**У**	**У**
Внутренний пользователь с мобильного устройства	Удаленный	Непривилегированный	**П**	**У**	**У**
Внешний пользователь	Удалённый	Непривилегированный	**П**	**У**	**У**

Принятые обозначения:

П – простая (парольная) аутентификация;

У – усиленная (двухфакторная) аутентификация.

Аутентификация внешних пользователей в целях предоставления государственных услуг осуществляется в том числе с использованием единой системы идентификации и аутентификации, созданной в соответствии с постановлением Правительства Российской Федерации от 28 ноября 2011 г. № 977.

В информационной системе должна обеспечиваться блокировка доступа к информационной системе для пользователей, не прошедших процедуру аутентификации.

В информационной системе должно быть реализовано управление аутентификаторами (аутентификационной информацией) пользователей, включающее:

изменение аутентификационной информации (аутентификаторов), заданной производителями и (или) используемых при внедрении системы

защиты информации информационной (автоматизированной) системы;

генерацию и выдачу аутентификационной информации;

блокирование (прекращение действия) и замену утерянных, скомпрометированных или поврежденных аутентификаторов;

обновление аутентификационной информации (замену аутентификаторов) с периодичностью, установленной оператором;

защиту аутентификационной информации от неправомерного доступа к ней и модификации.

Аутентификация пользователей обеспечивается применением входящих в состав информационной системы операционной системы, и (или) средств защиты информации от несанкционированного доступа, и (или) средств защиты информации, обеспечивающих управление аутентификационной информацией.

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены:

требования к аутентификации пользователей при осуществлении доступа в информационную систему и ресурсам (объектам защиты) информационной системы, включающие вид аутентификации для каждого типа пользователей, типа доступа, ресурсов (объектов защиты), к которым пользователь получает доступ;

состав аутентификационной информации для каждого типа пользователей;

правила формирования (создания) уникальных аутентификаторов, их присвоения пользователям, регистрации аутентификаторов в информационной системе;

порядок привязки аутентификационной информации к пользователю;

порядок аутентификации, порядок действий при выявлении несоответствий, правила ее проведения;

перечень исключений и порядок действий в случае, если объем аутентификационных данных недостаточен;

правила хранения, поддержания актуального состояния (обновления) аутентификационной информации пользователей, периодичности обновления (актуализации), места ее хранения, организации доступа к ней.

Требования к усилению:

1) при реализации усиленной аутентификации привилегированного пользователя при удаленном доступе требуется наличие у пользователя второго фактора аутентификации – одноразового пароля, создаваемого с применением устройства аутентификации, находящего во владении пользователя;

2) при реализации усиленной аутентификации привилегированного пользователя при удаленном доступе требуется наличие у пользователя второго фактора аутентификации – владения физическим (аппаратным) устройством, знание секрета, подтверждающего право владения (распоряжения) этим

устройством и (или) его биометрические данные;

3) при локальном доступе в информационную систему, а также к ресурсам (объектам защиты) информационной системы внутреннего непривилегированного пользователя должна осуществляться усиленная аутентификация;

4) при доступе в информационную систему, а также к ресурсам (объектам защиты) информационной системы внешнего пользователя должна осуществляться усиленная аутентификация;

5) при удаленном доступе в информационную систему, а также к ресурсам (объектам защиты) информационной системы внутреннего непривилегированного пользователя должна осуществляться строгая аутентификации;

6) при удаленном доступе в информационную систему, а также к ресурсам (объектам защиты) информационной системы внутреннего привилегированного пользователя должна осуществляться строгая аутентификация;

7) в информационной системе должны использоваться автоматизированные средства, обеспечивающие контроль правил генерации и смены паролей пользователей;

8) в информационной системе должны применяться средства централизованного управления аутентификаторами (аутентификационной информацией) пользователей;

9) устройства аутентификации не должны входить в состав объекта доступа (в том числе средство вычислительной техники, конечное устройство, мобильное устройство) и должны быть физически отделены от него;

10) при реализации строгой аутентификации требуется наличие у пользователя второго фактора аутентификации – владения физическим (аппаратным) устройством с поддержкой криптографии, неизвлекаемым закрытым ключом, энергонезависимой памятью для хранения цифровых сертификатов, а также знание секрета (ПИН-кода устройства). Срок действия цифровых сертификатов при использовании аппаратных средств аутентификации с неизвлекаемым закрытым ключом не должен превышать 3 лет, в остальных случаях – не более 1 года. Для реализации строгой аутентификации в информационной системе с доменной архитектурой должны быть развернуты корпоративный центр выпуска, обслуживания и валидации цифровых сертификатов доступа (центр сертификации), система централизованного управления жизненным циклом цифровых сертификатов и средств аутентификации. На клиентской стороне должна быть обеспечена поддержка необходимых криптографических протоколов аутентификации (например, Kerberos, TLS) с использованием цифровых сертификатов и средств

строгой аутентификации. При отсутствии (или невозможности) взаимодействия с центром сертификации, выполняющим функцию третьей доверенной стороны, информационная система может использовать списки действительных и аннулированных (отозванных) сертификатов или другие методы проверки аутентификационной информации. Для информационных систем, в состав которых входит менее 50 рабочих мест, в которых отсутствует домен безопасности и центр сертификации, для внутренних пользователей допускается применение усиленной аутентификации с использованием компенсирующих мер защиты информации, усиливающих привязку пользователя к используемому им физическому (аппаратному) средству аутентификации. Например, использование биометрии или мобильного телефона пользователя в качестве второго фактора с установленным приложением-генератором одноразовых паролей, получением SMS, push-уведомлений;

11) в информационной системе должны быть определены меры по исключению возможности использования пользователями их идентификаторов и аутентификационной информации в других информационных системах.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ИАФ.3	+	+	+
Усиление ИАФ.3			1

ИАФ.4 Аутентификация устройств

Цель: Исключение доступа к информационным системам и содержащейся в них информации устройствам (программно-аппаратных средствам), не прошедшим процедуру аутентификации.

Требования к реализации: Аутентификация устройства должна проводиться после идентификации устройства и его регистрации в информационной системе.

Аутентификация для каждого устройства должна производиться при каждом запросе на его подключение к информационной системе и до начала информационного взаимодействия с ней.

Подключение к информационной системе устройств, не прошедших процедуру аутентификации, не допускается.

В информационной системе должны быть определены способ аутентификации устройств и применяемые протоколы аутентификации. В процессе аутентификации устройств должны использоваться поддерживаемые

ими протоколы аутентификации (например, EAP, 802.1x, CMP, EST, ACME, MS-WSTEP, TLS, DTLS и другие протоколы аутентификации).

Аутентификация устройств обеспечивается применением входящих в состав информационной системы операционной системы, средств защиты информации от несанкционированного доступа. Реализация меры по аутентификации устройств достигается применением одного или совокупности программных, программно-аппаратных средств.

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены:

места размещения устройств, находящихся внутри информационной системы и за ее периметром;

способы аутентификации устройств;

действия администратора по настройке и контролю функционирования способов аутентификации устройств;

действия администратора в случае утери, поломки, вывода устройств из эксплуатации и (или) компрометации аутентификационной информации устройств;

правила и процедуры управления средствами аутентификации устройств;

порядок осуществления мероприятий по мониторингу и аудиту действий администраторов и пользователей, связанных с обслуживанием и жизненным циклом аутентификационной информации и средств аутентификации;

процедуры эксплуатации системы централизованного управления (при ее наличии).

Требования к усилению:

1) смена аутентификационных данных устройств не реже чем один раз в год;

2) реализация аутентификации устройств с использованием криптографических протоколов аутентификации;

3) реализация аутентификации с использованием третьей доверенной стороны (корпоративного центра сертификации);

4) использование системы централизованного управления жизненным циклом цифровых сертификатов, электронных идентификаторов, встроенных модулей безопасности.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ИАФ.4			
Усиление ИАФ.4			

4.2. Управление доступом (УПД)

УПД.1 Реализация модели управления доступом

Цель: Определение и реализация модели управления доступом субъектов к объектам доступа в информационной системе.

Требования к реализации: В информационной системе должна быть реализована модель управления доступом, формализующая методы управления доступом, типы доступа субъектов к объектам доступа и правила управления доступа субъектов доступа к объектам доступа, реализуемые в информационной системе.

Разработка модели управления доступом осуществляется с учетом положений национальных стандартов ГОСТ Р 59453.1-2021 «Защита информации. Формальная модель управления доступом. Часть 1. Общие положения», ГОСТ Р 59453.3-2025 «Защита информации. Формальная модель управления доступом. Часть 3. Рекомендации по разработке».

В информационной системе должны быть реализованы один или несколько методов управления доступом, к которым относятся:

дискреционный метод управления доступом;

ролевой метод управления доступом;

мандатный метод управления доступом;

атрибутный метод управления доступом.

В информационной системе в зависимости от реализуемых методов управления доступом необходимо определить несколько из указанных критериев:

типы субъектов и объектов доступа (например, пользователи, устройства, приложения (процессы), файлы и иные субъекты и объекты доступа);

типы учетных записей (ролей) субъектов доступа (внутреннего пользователя, внешнего пользователя; непривилегированная, привилегированная; постоянная, временная, гостевая и (или) иные типы учетных записей субъектов доступа);

типы доступа субъектов к объектам доступа (права доступа) (например, операции по чтению, записи, удалению, выполнению, администрированию, экспорту/импорту данных, созданию резервных копий, изменению политик безопасности и иные типы доступа субъектов доступа к объектам доступа);

правила разграничения доступа субъектов доступа к объектам доступа в информационной системе в соответствии с заданными методами управления доступом.

Модель управления доступом должна пересматриваться ежегодно или при внесении изменений в методы и типы субъектов и объектов доступа,

а также типы доступа субъектов к объектам доступа.

В информационной системе должна быть реализована модель управления доступом за счет применения в информационной системе операционных систем, систем управления базами данных, средств виртуализации, средств контейнеризации, средств доверенной загрузки, иных средств защиты информации.

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены:

используемые методы управления доступом;

перечни субъектов и объектов доступа;

правила управления доступом субъектов доступа к объектам доступа;

средства защиты информации, реализующие правила управления доступом.

Требования к усилению:

1) модель управления доступом должна быть согласована с моделями доступа, применяемыми в операционных системах, системах управления базами данных, средствах виртуализации, средствах контейнеризации, иных средствах защиты информации;

2) модель управления доступом должна обеспечивать реализацию управления доступом между субъектами и объектами доступа, являющимися устройствами и (или) приложениями;

3) модель управления доступом должна реализовываться на уровне сегментов информационной системы (микросегментов, информационных ресурсов, приложений) путем применения межсетевых экранов уровня приложений, многофункциональных межсетевых экранов уровня сети, средств виртуализации.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
УПД.1	+	+	+
Усиление УПД.1		1, 2	1, 2

УПД.2 Разграничение и контроль прав доступа

Цель: Реализация принципов минимизации прав доступа и разграничения прав доступа при реализации модели управления доступом субъектов к объектам доступа в информационной системе.

Требования к реализации: Разграничение и контроль прав доступа реализуются на основе модели управления доступом и должны обеспечивать управление доступом пользователей и запускаемых от их имени приложений при

доступе (входе) в информационную систему и различных типах последующего доступа в информационной системе:

к программно-аппаратным средствам, машинным носителям информации и устройствам;

к объектам файловых систем;

к запускаемым и исполняемым файлам приложений;

к информации в системах управления базами данных;

к параметрам настройки средств защиты информации;

к системным журналам, журналам приложений, журналам событий безопасности;

к доступным пользователям, устройствам и приложениям, API-интерфейсам;

к средствам удаленного администрирования;

к объектам доступа в виртуальной инфраструктуре (например, образам виртуальных машин, средствам виртуализации, запущенным виртуальным машинам);

к объектам доступа в контейнерной инфраструктуре (например, образам контейнеров, средствам контейнеризации (оркестраторам), запущенным контейнерам);

к иным определенным в информационной системе субъектам и объектам доступа.

В информационной системе должны быть обеспечены:

разграничение прав доступа непривилегированных и привилегированных пользователей, в том числе администраторов, администраторов безопасности, обеспечивающих функционирование информационной системы технических специалистов;

минимизация прав доступа субъектов доступа к объектам доступа.

В информационной системе должен быть установлен запрет использования пользователями информационной системы групповых (общих) учетных записей и учетных записей, заданных по умолчанию, посредством отключения (удаления) данных учетных записей в информационной системе.

В информационной системе должны быть пересмотрены ограничения и запреты действий для пользователей с целью актуализации правил разграничения и минимизации прав доступа ежегодно или при внесении изменений в методы и типы субъектов и объектов доступа, а также типы доступа субъектов к объектам доступа, или при существенном изменении числа и состава групп субъектов и объектов доступа.

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены:

обязанности (функции) пользователей (ролей) информационной системы;

права доступа, минимально необходимые для выполнения обязанностей (функций) пользователей (ролей) информационной системы;

права доступа, минимально необходимые для функционирования устройств и приложений в информационной системе;

принципы разграничения прав доступа непривилегированных и привилегированных пользователей (ролей), в том числе администраторов, администраторов безопасности, обеспечивающих функционирование информационной системы технических специалистов;

ограничения и запреты для каждого субъекта (роли) и объекта доступа, используемых в информационной системе.

Требования к усилению:

1) в информационной системе должна быть обеспечена реализация ограничений и запретов совмещения одним пользователем информационной системы непривилегированных обязанностей по обработке информации и привилегированных обязанностей по администрированию, обеспечению безопасности, обеспечению функционирования информационной системы;

2) в информационной системе должна быть обеспечена минимизация прав субъектов и объектов доступа, являющихся устройствами и приложениями, в том числе средствами защиты информации, а также техническими компонентами информационной системы, такими как средства управления базами данных, конвейеры разработки, тестирования и доставки программного обеспечения, хранилища секретов, элементы сетевой инфраструктуры, облачные сервисы и средства администрирования, в том числе на уровне типов доступа к файлам и процессам приложений в операционной системе;

3) в информационной системе должен быть определен привилегированный пользователь (главный администратор), имеющий права по передаче полномочий по администрированию информационной системы и системы защиты информации другим лицам и осуществляющий контроль за использованием переданных полномочий.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
УПД.2	+	+	+
Усиление УПД.2		1	1, 2

УПД.3 Управление учетными записями

Цель: Управление жизненным циклом учетных записей субъектов доступа в информационной системе.

Требования к реализации: Управление учетными записями субъектов доступа в информационной системе должно обеспечивать:

создание, назначение, активацию, блокирование и удаление учетных записей;

учет учетных записей;

верификацию пользователей (проверку личности пользователя, его функциональных обязанностей) при заведении учетной записи;

верификацию компонентов информационной системы, таких как устройства, приложения, для которых создается (технологическая) учетная запись;

назначение, изменение, удаление правил доступа учетных записей;

объединение учетных записей в группы учетных записей (при необходимости);

пересмотр правил доступа учетных записей и групп учетных записей;

регистрацию событий безопасности, связанных с управлением учетными записями.

В информационной системе должны использоваться средства управления учетными записями пользователей.

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены:

порядок верификации и активации учетных записей пользователей, устройств, приложений при создании учетной записи в информационной системе;

порядок создания, активации, блокирования, удаления, назначения, пересмотра, изменения видов, типов и правил доступа учетных записей;

порядок ведения журнала реализации функций (административных действий) заведения, активации, блокирования и удаления привилегированных учетных записей;

порядок уведомления администраторов, отвечающих за управление и контроль над учетными записями пользователей, о реализации функций по управлению учетными записями;

процедуры анализа журналов безопасности для выявления нарушений и событий безопасности и процедуры реагирования на них;

требования к договорным документам и соглашениям об информационном взаимодействии при подключении внешних пользователей, устройств, приложений к информационной системе.

Требования к усилению:

1) в информационной системе должно быть реализовано централизованное управление учетными записями пользователей с использованием программного обеспечения централизованного управления учетными записями;

2) в информационной системе должно быть реализовано централизованное управление учетными записями устройств, приложений с использованием программного обеспечения централизованного управления учетными записями.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
УПД.3	+	+	+
Усиление УПД.3		1	1, 2

УПД.4 Ограничение неуспешных и нерегламентированных попыток доступа в информационную систему

Цель: Защита информационной системы посредством ограничений прав доступа субъектов доступа, превысивших число неуспешных попыток доступа в информационную систему либо осуществляющих попытки доступа в информационную систему в нерегламентированное (нештатное) время.

Требования к реализации: В информационной системе должно быть обеспечено ограничение права доступа субъектов доступа, превысивших число неуспешных попыток доступа в информационную систему за установленный в информационной системе период времени.

Ограничение прав доступа должно реализовываться в отношении:

субъектов доступа, являющихся пользователями и устройствами информационной системы;

субъектов доступа (нарушителей), осуществляющих попытки получения несанкционированного доступа к информационной системе с использованием взаимодействующих с информационной системой устройств и приложений.

Ограничение прав доступа в информационную систему должно выполняться посредством автоматического анализа событий попыток доступа в информационную систему в соответствии с мерами защиты информации ИАФ.1 – ИАФ.4.

Ограничение прав доступа должно выполняться посредством блокирования учетной записи пользователя, устройства или приложения в информационной системе, а также посредством блокирования доступа на основе совпадения технических признаков (например, IP-адрес, сигнатуры

сведений о пользовательском агенте).

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены:

установленное в информационной системе значение допустимого числа неуспешных попыток входа;

период времени, в течение которого учитываются попытки входа;

типы объектов блокирования (учетные записи, устройства, характеризуемые техническими признаками приложения);

периоды времени существования различных типов временных учетных записей;

периоды допустимого времени неактивности различных типов учетных записей;

регламентированное (штатное) время входа и (или) конкретные типы доступа субъектов доступа к объектам доступа;

порядок блокирования субъектов доступа;

условия разблокирования учетной записи или устройства, например, интервалы времени автоматического разблокирования, разблокирование в результате подтверждения привилегированным пользователем (администратором).

Требования к усилению:

1) в информационной системе должна быть обеспечена реализация автоматического блокирования и (или) удаления временных и неиспользуемых учетных записей, а также оповещение о данном событии привилегированного пользователя (администратора), отвечающего за управление и контроль над учетными записями пользователей;

2) разблокирование доступа привилегированных субъектов доступа, превысивших число неуспешных попыток доступа в информационную систему, может выполняться только главным администратором.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
УПД.4	+	+	+
Усиление УПД.4		1, 2	1, 2

УПД.5 Предупреждение пользователя при его доступе к информационной системе

Цель: Информирование пользователей о реализации мер защиты информации и обязательности соблюдения установленных правил работы с информацией при доступе к информационной системе.

Требования к реализации: В информационной системе должно быть обеспечено предупреждение пользователя до момента выполнения идентификации и аутентификации в соответствии с мерами защиты информации ИАФ.1 – ИАФ.4 в виде сообщения («окна») о том, что в информационной системе реализованы меры защиты информации, а также о том, что пользователем должны быть соблюдены установленные в информационной системе правила и ограничения на работу с информацией.

Доступ пользователя в информационную систему осуществляется только после подтверждения пользователем ознакомления с предупреждением.

Требования к документированию: Не предъявляются.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
УПД.5			
Усиление УПД.5			

УПД.6 Оповещение пользователя о предыдущем входе в информационную систему

Цель: Оповещение пользователя о попытках входа в информационную систему, осуществленных ранее от имени его учетной записи.

Требования к реализации: В информационной системе должно быть обеспечено оповещение пользователя о последнем успешном входе в информационную систему, осуществленном ранее от имени его учетной записи, после успешного выполнения пользователем входа в информационную систему в соответствии с мерами защиты информации ИАФ.1 – ИАФ.4.

Оповещение должно содержать информацию как минимум о дате и времени предыдущего входа в информационную систему от имени учетной записи пользователя, а также иную информацию, определенную в информационной системе.

Пользователь информационной системы, установивший на основании оповещения факт несанкционированного доступа в информационную систему от имени его учетной записи, должен незамедлительно проинформировать привилегированного пользователя (администратора безопасности).

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены:

объем сведений о факте предыдущего входа от имени учетной записи пользователя в информационную систему, например, дата, время, регион, IP-адрес, устройство;

используемые каналы и адреса основного и альтернативного оповещения пользователя, например, окно браузера, e-mail, SMS, push-уведомление;

порядок настройки и подтверждения пользователем контактных данных, используемых для оповещения;

порядок информирования привилегированного пользователя (администратора безопасности) о фактах несанкционированного доступа в информационную систему от имени учетной записи пользователя.

Требования к усилению:

1) после успешного выполнения пользователем входа в информационную систему должно обеспечиваться оповещение пользователя о числе неуспешных попыток входа в информационную систему от имени его учетной записи, зафиксированных с момента последнего успешного входа пользователя в информационную систему;

2) после успешного выполнения пользователем входа в информационную систему должно обеспечиваться оповещение пользователя о числе всех попыток входа в информационную систему от имени его учетной записи, зафиксированных в нештатное (нерегламентированное) время;

3) после успешного выполнения пользователем входа в информационную систему должно обеспечиваться оповещение пользователя о числе всех попыток входа в информационную систему от имени его учетной записи, зафиксированных за период времени не менее 7 дней;

4) после успешного выполнения пользователем входа в информационную систему должно обеспечиваться оповещение пользователя об изменении сведений, относящихся к учетной записи пользователя (в том числе повышении прав доступа), произведенных за период времени не менее, чем с момента предыдущего успешного входа в информационную систему;

5) объем сведений о фактах попыток входа от имени учетной записи пользователя в информационную систему должен включать информацию о том, откуда (например, регион или IP-адрес) и с какого устройства или приложения (например, сигнатуры сведений о пользовательском агенте) осуществлялась попытка входа;

6) пользователь должен получать уведомления о критически важных событиях (изменение пароля, вход из нового региона/устройства) по альтернативным каналам связи.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
УПД.6			
Усиление УПД.6			

УПД.7 Ограничение числа параллельных сеансов доступа

Цель: Ограничение числа параллельных сеансов доступа от имени учетной записи к информационной системе.

Требования к реализации: В информационной системе должны обеспечиваться:

возможность задавать ограничения на число параллельных сеансов доступа, основываясь на идентификаторах учетных записей;

автоматический учет активных сеансов доступа для каждой учетной записи пользователей, устройств и приложений информационной системы;

автоматическое ограничение числа параллельных сеансов доступа для каждой учетной записи пользователей, устройств и приложений информационной системы;

уведомление пользователя при превышении числа параллельных сеансов от имени его учетной записи либо администрируемых или контролируемых пользователем устройств и приложений.

В информационной системе в случае попытки входа от имени учетных записей непривилегированных или привилегированных пользователей, для которых достигнуто максимальное значение допустимых параллельных сеансов, при успешной аутентификации пользователя или администратора должно выдаваться сообщение о превышении числа параллельных сеансов доступа, месте (местах) их предыдущего входа (предыдущих входов) с активными сессиями и предложением отключения этой сессии (этих сессий).

В информационной системе число параллельных сеансов доступа может быть задано для информационной системы в целом, для отдельных сегментов информационной системы, для групп пользователей, отдельных пользователей или их комбинаций.

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены:

значения максимально допустимого числа параллельных сеансов доступа для различных типов учетных записей;

порядок учета и регистрации активных сеансов доступа для каждой учетной записи;

порядок автоматического учета активных сеансов и реализации заданных ограничений;

порядок уведомления пользователя при превышении числа параллельных сеансов;

порядок оповещения администраторов о превышении лимитов активных сеансов учетных записей;

объем сведений в оповещающем сообщении, например, дата, время, место

и устройство предыдущих входов, предложение завершить активные сессии.

Требования к усилению:

1) в информационной системе для учетных записей привилегированных пользователей (администраторов, администраторов безопасности) количество параллельных (одновременных) сеансов (сессий) не должно превышать следующих значений:

а) не более 2;

б) не более 1.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
УПД.7		+	+
Усиление УПД.7			1а

УПД.8 Блокирование сеанса доступа пользователя при неактивности

Цель: Обеспечение защиты информационной системы от несанкционированного доступа в случаях, когда субъект доступа оставляет активный сеанс (сессию) без контроля.

Требования к реализации: В информационной системе должно обеспечиваться блокирование сеанса доступа субъекта доступа (пользователя, устройства, приложения) после установленного в информационной системе времени его бездействия (неактивности), а также по запросу субъекта доступа или оператора.

Для заблокированного сеанса должно осуществляться блокирование любых действий по доступу к информации и (или) устройствам отображения, кроме необходимых для разблокирования сеанса.

Разблокирование сеанса доступа субъекта доступа в информационную систему должно осуществляться после повторной аутентификации в соответствии с мерой защиты информации ИАФ.3.

В информационной системе на устройстве отображения (мониторе) после блокирования сеанса не должна отображаться информация сеанса субъекта доступа.

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены:

значения допустимого времени бездействия для различных категорий пользователей;

порядок реализации автоматического блокирования сеанса при превышении допустимого времени бездействия;

порядок восстановления работы субъекта доступа после блокирования сеанса;

порядок регистрации событий превышения установленного оператором допустимого числа неуспешных попыток разблокирования доступа.

Требования к усилению:

1) в информационной системе должно осуществляться завершение сеанса доступа после превышения установленного оператором времени бездействия (неактивности) субъекта доступа;

2) в информационной системе должно осуществляться завершение сеанса доступа после превышения установленного оператором числа неуспешных попыток разблокирования сеанса доступа.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
УПД.8	+	+	+
Усиление УПД.8			

УПД.9 Контроль действий субъектов доступа до идентификации и аутентификации

Цель: Обеспечение контроля и ограничения действий субъекта доступа в информационной системе до прохождения процедур идентификации и аутентификации.

Требования к реализации: В информационной системе должен быть установлен перечень действий субъектов доступа, разрешенных до прохождения ими процедур идентификации и аутентификации в соответствии с мерами защиты информации ИАФ.1 – ИАФ.4, и запрет действий субъектов доступа, не включенных в перечень разрешенных действий, до прохождения ими процедур идентификации и аутентификации.

В информационной системе должен быть определен перечень действий привилегированных субъектов доступа (администраторов, администраторов безопасности, технических специалистов), осуществление которых допускается в обход установленных процедур идентификации и аутентификации, необходимых для восстановления функционирования информационной системы в случае сбоев в работе или выхода из строя отдельных технических средств (устройств).

Все действия, выполняемые без прохождения процедуры идентификации и аутентификации, должны регистрироваться в журналах регистрации событий безопасности, за исключением доступа к общедоступным сведениям, подлежащим опубликованию в открытом доступе на компонентах информационной системы.

Перечень действий субъектов доступа, разрешенных до идентификации и аутентификации, должен пересматриваться не реже 1 раза в год и после изменений модели доступа в информационной системе.

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены:

перечень ресурсов и компонентов информационной системы, доступ к которым предоставляется субъектам доступа до идентификации и аутентификации;

перечень действий пользователей, разрешенных до прохождения процедур идентификации и аутентификации;

описание порядка регистрации действий, выполняемых без прохождения процедур идентификации и аутентификации.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
УПД.9	+	+	+
Усиление УПД.9			

4.3. Регистрация событий безопасности (РСБ)

РСБ.1 Определение событий безопасности и данных о них, подлежащих регистрации

Цель: Определить состав и содержание информации о событиях, связанных с возможным нарушением безопасности информации, нарушением функционирования информационных систем, реализацией угроз безопасности информации (далее – события безопасности), подлежащих регистрации в информационной системе.

Требования к реализации: В информационной системе должен быть определен перечень программных, программно-аппаратных средств, средств защиты информации, которые обеспечивают возможность регистрации событий безопасности.

Регистрация событий безопасности информации должна проводиться:

в средствах защиты информации, установленных в информационной системе;

в программно-аппаратных средствах (серверах и автоматизированных рабочих местах, в системах хранения данных, средствах защиты информации, телекоммуникационном оборудовании), находящихся на периметре информационной системы и (или) информационно-телекоммуникационной инфраструктуры, на базе которой функционирует информационная система;

в программных, программно-аппаратных средствах информационной системы (сегментах информационной системы), предназначенных для обработки информации, которая отнесена к информации ограниченного доступа;

в программных, программно-аппаратных средствах информационной системы (сегментах информационной системы), предназначенных для реализации значимых функций информационной системы;

на средствах, обеспечивающих удаленное подключение пользователей к информационной системе.

Состав и содержание событий безопасности, а также типы событий безопасности, подлежащие регистрации в информационной системе, определяются оператором информационной системы в соответствии с национальным стандартом ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результата события безопасности (успешно или неуспешно), субъекта доступа (пользователя и (или) процесса), связанного с данным событием безопасности.

В информационной системе как минимум подлежат регистрации следующие события:

вход (выход), а также попытки входа субъектов доступа в информационную систему;

подключение машинных носителей информации и вывод информации на носители информации;

запуск (завершение) программ и процессов, связанных с обработкой защищаемой информации;

попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, каталогам, файлам, записям, полям записей) и иным объектам доступа;

попытки удаленного доступа;

события, регистрируемые средствами защиты информации.

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены требования к определению событий безопасности и данных о них, подлежащих регистрации в информационной системе, предусматривающие определение:

программных, программно-аппаратных средств, с которых осуществляется регистрация и сбор событий безопасности;

состава и содержания информации о событиях безопасности, подлежащих регистрации;

типов событий безопасности, подлежащих регистрации в информационной системе.

Требования к усилению:

1) в информационной системе обеспечивается запись дополнительной информации о событиях безопасности, включающая запись привилегированных команд (команд, управляющих системными функциями);

2) в информационной системе обеспечивается централизованный мониторинг событий безопасности в рамках сегментов информационной системы, определяемых оператором, и (или) информационной системы в целом;

3) в информационной системе обеспечивается регистрация информации о месте (в частности сетевой адрес, географическая привязка и (или) другая информация), с которого осуществляется удаленный доступ в информационную систему;

4) зарегистрированная информация о событиях безопасности должна передаваться в средства управления событий информационной безопасности.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
РСБ.1	+	+	+
Усиление РСБ.1	1	1, 2	1, 2, 3

РСБ.2 Анализ событий безопасности и реагирование на них

Цель: Своевременное выявление признаков компьютерных атак и инцидентов безопасности.

Требования к реализации: Анализ записей регистрации должен проводиться для всех событий, подлежащих регистрации в соответствии с мерой защиты информации РСБ.1, с периодичностью, установленной оператором и обеспечивающей своевременное выявление признаков компьютерных атак и инцидентов безопасности.

В случае выявления признаков компьютерных атак и инцидентов безопасности в информационной системе осуществляется проведение мероприятий по реагированию на выявленные компьютерные атаки и инциденты безопасности.

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены периодичность проведения анализа событий безопасности, а также порядок реагирования на выявленные признаки компьютерных атак и инциденты безопасности.

Требования к усилению:

1) в информационной системе должны обеспечиваться сбор результатов анализа записей регистрации из разных источников (журналов, хранилищ информации о событиях безопасности) и их корреляция с целью выявления инцидентов безопасности и реагирования на них;

2) в информационной системе должна обеспечиваться интеграция процессов анализа результатов регистрации событий безопасности с результатами анализа уязвимостей и результатами обнаружения вторжений с целью усиления возможностей по выявлению признаков инцидентов безопасности;

3) в информационной системе должен обеспечиваться полнотекстовый анализ привилегированных команд;

4) оператором должен обеспечиваться анализ записанных сетевых потоков (дампов);

5) реагирование на компьютерные инциденты должно осуществляться с учетом ГОСТ Р 59712-2022 «Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты».

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
РСБ.2	+	+	+
Усиление РСБ.2			

РСБ.3 Генерация временных меток при регистрации событий безопасности

Цель: Формирование надежных меток времени и (или) синхронизация системного времени.

Требования к реализации: В информационной системе должно обеспечиваться получение меток времени, включающих дату и время, используемых при генерации записей регистрации событий безопасности.

В информационной системе должен быть определен источник надежных меток времени и должна выполняться синхронизация системного времени с периодичностью, определенной оператором.

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены требования к генерации надежных меток времени при регистрации событий безопасности, предусматривающие определение правил и процедур генерации надежных меток времени.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
РСБ.3	+	+	+
Усиление РСБ.3			

РСБ.4 Требования к сбору, хранению и защите данных о событиях безопасности

Цель: Обеспечение хранения и защиты данных о событиях безопасности от несанкционированного доступа.

Требования к реализации: В информационной системе должны осуществляться сбор, запись и хранение информации о событиях безопасности в течение установленного оператором времени хранения информации о событиях безопасности.

Сбор, запись и хранение информации о событиях безопасности должны предусматривать:

возможность выбора администратором безопасности событий безопасности, подлежащих регистрации в текущий момент времени, из перечня типов событий безопасности, определенных в соответствии с мерой защиты информации РСБ.1;

формирование (сбор, запись) записей типов событий безопасности, подлежащих регистрации;

хранение информации о событиях безопасности в течение времени, установленного оператором информационной системы.

Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, состава и содержания информации о событиях безопасности, подлежащих регистрации, а также срока хранения информации о зарегистрированных событиях безопасности.

В информационной системе должна обеспечиваться защита информации о событиях безопасности, регистрируемых в информационной системе в соответствии с настоящим методическим документом.

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены:

типы событий безопасности, подлежащие регистрации в заданный момент времени, из перечня типов событий безопасности, определенных в соответствии с мерой защиты информации РСБ.1;

порядок хранения сведений о событиях безопасности, в том числе требования к местам хранения сведений о событиях безопасности и периоду времени хранения информации о событиях безопасности.

Требования к усилению:

1) в информационной системе должно быть обеспечено централизованное автоматизированное управление сбором, записью и хранением информации о событиях безопасности;

2) в информационной системе должно быть обеспечено объединение информации из записей регистрации событий безопасности, полученной от разных технических средств (устройств), программного обеспечения информационной системы, в единый логический или физический журнал аудита с корреляцией информации по времени для своевременного выявления инцидентов и реагирования на них;

3) в информационной системе должно быть обеспечено хранение копий записей системных журналов и записей о событиях безопасности в обособленном хранилище, физически отделенном от иных технических средств, входящих в состав информационной системы;

4) в информационной системе должно быть обеспечено резервное копирование записей регистрации (аудита);

5) в информационной системе для обеспечения целостности информации о зарегистрированных событиях безопасности должны применяться в соответствии с законодательством Российской Федерации криптографические методы.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
РСБ.4	+	+	+
Усиление РСБ.4			

РСБ.5 Реагирование на сбои при регистрации событий безопасности

Цель: Осуществление реагирования 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.

Требования к реализации: Реагирование на сбои при регистрации событий безопасности должно предусматривать:

предупреждение (сигнализация, индикация) администраторов о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;

реагирование на сбои при регистрации событий безопасности путем изменения администраторами параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов информационной системы, запись поверх

устаревших хранимых записей событий безопасности.

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены требования к правилам и процедурам реагирования на сбои при регистрации событий безопасности.

Требования к усилению:

1) в информационной системе должна обеспечиваться выдача предупреждения администратору в масштабе времени, близком к реальному, при наступлении критичных сбоев в механизмах сбора информации, определенных в информационной системе;

2) в информационной системе должен обеспечиваться запрет обработки информации в случае аппаратных или программных ошибок, сбоев в механизмах сбора информации или достижения предела или переполнения объема (емкости) памяти.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
РСБ.5	+	+	+
Усиление РСБ.5			

4.4. Защита виртуализации и облачных вычислений (ЗСВ)

ЗСВ.1 Доверенная загрузка средств виртуализации и виртуальных машин

Цель: Контроль целостности средств виртуализации и виртуальных машин на этапе их загрузки.

Требования к реализации: При применении средств виртуализации должны обеспечиваться:

доверенная загрузка хостовой операционной системы (при ее наличии) и средства виртуализации;

выявление загрузки виртуальных машин, состав и настройки виртуального оборудования которых содержат несанкционированные изменения.

Указанные меры защиты информации реализуются за счет применения в информационной системе встроенных в базовые системы ввода-вывода механизмов безопасности, и (или) средств доверенной загрузки, и (или) встроенных в хостовые операционные системы механизмов безопасности, и (или) встроенных в средства виртуализации механизмов безопасности.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должна обеспечиваться блокировка загрузки виртуальной машины,

в которой исполняемые файлы или конфигурация компонентов, участвующих в загрузке гостевой операционной системы, содержат несанкционированные изменения;

2) должна обеспечиваться блокировка загрузки виртуальной машины, если загружаемая версия гостевой операционной системы содержит критические уязвимости и (или) запрещена для использования в информационной системе;

3) должна обеспечиваться блокировка загрузки виртуальной машины, если исполняемые файлы или конфигурация компонентов, участвующих в загрузке гостевой операционной системы, не прошли аутентификацию с использованием свидетельств подлинности модулей (в том числе цифровых сигнатур производителя или иных свидетельств подлинности модулей);

4) должна обеспечиваться блокировка загрузки виртуальной машины, если исполняемые файлы или конфигурация компонентов, участвующих в загрузке гостевой операционной системы, не прошли аутентификацию с использованием свидетельств подлинности модулей в виде цифровых сигнатур оператора информационной системы.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗСВ.1	+	+	+
Усиление ЗСВ.1		1	1, 2

ЗСВ.2 Контроль целостности средств виртуализации и виртуальных машин

Цель: Контроль целостности средств виртуализации и виртуальных машин на этапе их функционирования.

Требования к реализации: При применении средств виртуализации должен обеспечиваться еженедельный или с меньшей периодичностью, устанавливаемой в информационной системе, контроль отсутствия несанкционированных изменений в составе и настройках виртуального оборудования выполняющихся виртуальных машин.

Указанные меры защиты информации реализуются за счет применения в информационной системе встроенных в средства виртуализации механизмов безопасности.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должен обеспечиваться еженедельный или с меньшей периодичностью, устанавливаемой в информационной системе, контроль отсутствия несанкционированных изменений в исполняемых файлах программного

обеспечения хостовой операционной системы и средства виртуализации;

2) должен обеспечиваться еженедельный или с меньшей периодичностью, устанавливаемой в информационной системе, контроль отсутствия несанкционированных изменений в параметрах настройки хостовой операционной системы и средства виртуализации;

3) должен обеспечиваться еженедельный или с меньшей периодичностью, устанавливаемой в информационной системе, контроль отсутствия несанкционированных изменений в файлах виртуальной базовой системы ввода-вывода (первичного загрузчика виртуальной машины);

4) должен обеспечиваться еженедельный или с меньшей периодичностью, устанавливаемой в информационной системе, контроль отсутствия несанкционированных изменений в исполняемых файлах программного обеспечения гостевой операционной системы.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗСВ.2	+	+	+
Усиление ЗСВ.2		1, 2	1, 2

ЗСВ.3 Регистрация событий безопасности в среде виртуализации

Цель: Определить состав и содержание информации о событиях безопасности, подлежащих регистрации в среде виртуализации.

Требования к реализации: При применении средств виртуализации должна обеспечиваться в соответствии с мерами защиты информации РСБ.1 – РСБ.5 регистрация следующих событий безопасности:

успешные и неуспешные попытки аутентификации пользователей средств виртуализации;

доступ пользователей средств виртуализации к виртуальным машинам посредством интерфейса средства виртуализации (терминальный доступ, виртуальный рабочий стол);

создание и удаление виртуальных машин;

запуск и остановка средства виртуализации с указанием причины остановки;

запуск и остановка виртуальных машин с указанием причины остановки;

изменение назначения ролей;

изменение конфигурации средства виртуализации;

изменение конфигураций виртуальных машин;

факты нарушения целостности объектов контроля;

факты перемещения виртуальных машин.

Указанные меры защиты информации реализуются за счет применения

в информационной системе встроенных в средства виртуализации механизмов защиты и (или) средств управления событиями безопасности.

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены требования к сбору, регистрации и анализу событий безопасности.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗСВ.3	+	+	+
Усиление ЗСВ.3			

ЗСВ.4 Управление доступом в среде виртуализации

Цель: Исключение несанкционированного доступа к объектам защиты в среде виртуализации.

Требования к реализации: Должны обеспечиваться меры по управлению доступом пользователей в среде виртуализации в соответствии с мерами защиты информации УПД.1 – УПД.4, а также:

управление правами доступа пользователей средств виртуализации к виртуальным машинам;

управление доступом виртуальных машин к физическому и виртуальному оборудованию;

управление квотами доступа виртуальных машин к физическому и виртуальному оборудованию.

Указанные меры защиты информации реализуются за счет применения в информационной системе встроенных в средства виртуализации механизмов безопасности.

Требования к документированию: В эксплуатационной документации на информационную систему должна быть определена модель управления доступом в среде виртуализации.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗСВ.4	+	+	+
Усиление ЗСВ.4			

ЗСВ.5 Резервное копирование в среде виртуализации

Цель: Обеспечение возможности восстановления средств виртуализации и виртуальных машин.

Требования к реализации: При применении средств виртуализации должно обеспечиваться резервное копирование:

образов виртуальных машин, определенных оператором;

параметров настройки средств виртуализации.

Указанные меры защиты информации реализуются за счет применения в информационной системе встроенных в средства виртуализации механизмов безопасности, и (или) встроенных в хостовые операционные системы механизмов безопасности, и (или) средств резервного копирования.

Требования к документированию: В эксплуатационной документации на информационную систему должен быть определен порядок реализации резервного копирования.

Требования к усилению:

1) должно обеспечиваться резервное копирование конфигураций виртуального оборудования виртуальных машин;

2) должно обеспечиваться резервное копирование сведений о событиях безопасности в среде виртуализации.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗСВ.5	+	+	+
Усиление ЗСВ.5			

ЗСВ.6 Ограничение программной среды в среде виртуализации

Цель: Блокирование несанкционированного запуска программного обеспечения в среде виртуализации.

Требования к реализации: Должно обеспечиваться выявление запуска компонентов программного обеспечения хостовой операционной системы и средства виртуализации, не включенных в перечень компонентов, разрешенных для запуска.

Указанные меры защиты информации реализуются за счет применения в информационной системе встроенных в средства виртуализации и (или) хостовые операционные системы механизмов безопасности.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должна обеспечиваться блокировка запуска компонентов программного

обеспечения хостовой операционной системы и (или) средства виртуализации, не включенных в перечень программного обеспечения, разрешенного для запуска в среде виртуализации.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗСВ.6	+	+	+
Усиление ЗСВ.6			1

ЗСВ.7 Защита памяти в среде виртуализации

Цель: Защита оперативной и постоянной памяти информационной системы при применении средств виртуализации.

Требования к реализации: При применении средств виртуализации должны обеспечиваться:

изоляция областей памяти, относящихся к различным виртуальным машинам;

очистка остаточной информации в памяти средств вычислительной техники, используемой для хранения данных виртуальных машин, при ее освобождении или перераспределении.

Указанные меры защиты информации реализуются за счет применения в информационной системе встроенных в средства виртуализации и (или) хостовые операционные системы механизмов безопасности.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должно обеспечиваться удаление объектов файловой системы, используемых средством виртуализации, путем многократной перезаписи уничтожаемых (стираемых) объектов файловой системы специальными битовыми последовательностями;

2) должна обеспечиваться изоляция области памяти виртуальных машин путем применения механизмов управления памятью аппаратной платформы;

3) должен обеспечиваться контроль целостности областей памяти виртуальных машин по запросу гостевой операционной системы.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗСВ.7	+	+	+
Усиление ЗСВ.7			

ЗСВ.8 Идентификация и аутентификация в среде виртуализации

Цель: Исключение несанкционированного доступа субъектов доступа, не прошедших идентификацию и аутентификацию, к объектам доступа в среде виртуализации.

Требования к реализации: Должна обеспечиваться идентификация и аутентификация субъектов доступа в среде виртуализации в соответствии с мерами защиты информации ИАФ.1, ИАФ.3, в том числе:

разработчиков виртуальных машин;

администраторов безопасности средств виртуализации;

администраторов средств виртуализации;

администраторов виртуальных машин;

администраторов хостовых операционных систем;

администраторов средств вычислительной техники, с использованием которых обеспечивается функционирование среды виртуализации.

Указанные меры защиты информации реализуются за счет применения в информационной системе встроенных в средства виртуализации и (или) хостовые операционные системы механизмов безопасности.

Требования к документированию: В эксплуатационной документации на информационную систему должен быть определен порядок идентификации и аутентификации субъектов доступа в среде виртуализации.

Требования к усилению:

1) должна обеспечиваться идентификация объектов доступа среды виртуализации:

виртуальных машин;

средств виртуализации;

средств вычислительной техники, входящих в состав виртуальной инфраструктуры.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗСВ.8	+	+	+
Усиление ЗСВ.8			

ЗСВ.9 Управление виртуальными машинами

Цель: Обеспечение централизованного управления образами виртуальных машин и виртуальными машинами.

Требования к реализации: При применении средств виртуализации должны обеспечиваться управление размещением и перемещением:

файлов-образов виртуальных машин между носителями (системами хранения данных);

исполняемых виртуальных машин между серверами виртуализации;

данных, обрабатываемых с использованием виртуальных машин, между носителями (системами хранения данных).

При применении средств виртуализации должен обеспечиваться контроль за перемещением виртуальных машин за пределы информационной системы (сегментов информационной системы) и (или) информационно-телекоммуникационной инфраструктуры, на базе которой они функционируют.

Управление перемещением виртуальных машин и обрабатываемых на них данных должно обеспечиваться только с применением технических средств, входящих в состав информационной системы.

Указанные меры защиты информации реализуются за счет применения в информационной системе встроенных в средства виртуализации и (или) хостовые операционные системы механизмов безопасности.

Требования к документированию: Не предъявляются.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗСВ.9		+	+
Усиление ЗСВ.9			

4.5. Защита технологий контейнерных сред и их оркестрации (ЗКО)

ЗКО.1 Контроль целостности в контейнерных средах

Цель: Обеспечение целостности средства контейнеризации, контейнеров и их образов.

Требования к реализации: При применении средств контейнеризации должен обеспечиваться еженедельный или с меньшей периодичностью, устанавливаемой в информационной системе, контроль отсутствия несанкционированных изменений в образах контейнеров и в исполняемых файлах контейнеров.

Указанная мера защиты информации реализуется за счет применения в информационной системе встроенных в средства контейнеризации и хостовые операционные системы механизмов безопасности.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должен обеспечиваться еженедельный или с меньшей периодичностью,

устанавливаемой в информационной системе, контроль отсутствия несанкционированных изменений в исполняемых файлах программного обеспечения хостовой операционной системы и средства контейнеризации;

2) должен обеспечиваться еженедельный или с меньшей периодичностью, устанавливаемой в информационной системе, контроль отсутствия несанкционированных изменений в параметрах настройки хостовой операционной системы и средства контейнеризации;

3) должно обеспечиваться выявление запуска компонентов программного обеспечения хостовой операционной системы и средства контейнеризации, целостность которых нарушена;

4) должен обеспечиваться контроль отсутствия несанкционированных изменений в образах контейнеров с использованием свидетельств подлинности (в том числе цифровых сигнатур производителя или иных свидетельств подлинности модулей) при установке образов контейнера в информационной системе;

5) должен обеспечиваться еженедельный или с меньшей периодичностью, устанавливаемой в информационной системе, контроль отсутствия несанкционированных изменений в образах контейнеров и в параметрах настройки средства контейнеризации с использованием свидетельств подлинности (в том числе цифровых сигнатур производителя или иных свидетельств подлинности модулей);

6) должно обеспечиваться выявление образа контейнера, целостность которого нарушена;

7) должна обеспечиваться блокировка запуска образа контейнера, целостность которого нарушена, и компонентов программного обеспечения хостовой операционной системы и средства контейнеризации, целостность которых нарушена.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКО.1	+	+	+
Усиление ЗКО.1		1, 2	1, 2, 3, 4, 5, 6

ЗКО.2 Регистрация событий безопасности в контейнерных средах

Цель: Определение состава и содержания информации о событиях безопасности, подлежащих регистрации в контейнерных средах.

Требования к реализации: При применении контейнерных сред должна обеспечиваться в соответствии с мерами защиты информации РСБ.1 – РСБ.5 регистрация следующих событий безопасности:

попытки осуществления несанкционированного доступа к средству контейнеризации;

попытки аутентификации пользователей средств контейнеризации;

создание, модификация и удаление образов контейнеров;

получение доступа к образам контейнеров;

запуск и остановка средства контейнеризации с указанием причины остановки;

запуск и остановка контейнеров с указанием причины остановки;

изменение назначения ролей;

модификация запускаемых контейнеров;

выявление известных уязвимостей в образах контейнеров и некорректности их конфигурации;

факты нарушения целостности объектов контроля.

Кроме того, должна обеспечиваться регистрация событий безопасности, относящихся к функционированию контейнера, с указанием идентификатора контейнера.

Указанные меры защиты информации реализуются за счет применения в информационной системе встроенных в средства контейнеризации и хостовые операционные системы механизмов безопасности.

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены требования к регистрации событий безопасности при применении контейнерных сред.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКО.2	+	+	+
Усиление ЗКО.2			

ЗКО.3 Управление доступом в контейнерных средах

Цель: Исключение несанкционированного доступа к объектам защиты в контейнерных средах.

Требования к реализации: При применении контейнерных сред должно обеспечиваться в соответствии с мерами защиты информации УПД.1 – УПД.4 управление доступом пользователей средства контейнеризации, а также иных субъектов доступа к контейнерам и их образам.

Указанные меры защиты информации реализуются за счет применения в информационной системе встроенных в средства контейнеризации и хостовые операционные системы механизмов безопасности.

Требования к документированию: В эксплуатационной документации

на информационную систему должны быть определены модели управления доступом в контейнерных средах, применяемых в информационной системе.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКО.3	+	+	+
Усиление ЗКО.3			

ЗКО.4 Резервное копирование в контейнерных средах

Цель: Обеспечение возможности восстановления функционирования контейнерной среды информационной системы.

Требования к реализации: При применении контейнерной среды должно обеспечиваться резервное копирование образов контейнеров.

Указанная мера защиты информации реализуются за счет применения в информационной системе средств резервного копирования.

Требования к документированию: В эксплуатационной документации на информационную систему должен быть определен порядок резервного копирования контейнерной среды.

Требования к усилению:

1) должно обеспечиваться резервное копирование параметров настройки средств контейнеризации;

2) должно обеспечиваться резервное копирование сведений о событиях безопасности в среде контейнеризации.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКО.4	+	+	+
Усиление ЗКО.4			

ЗКО.5 Изоляция контейнеров в контейнерной среде

Цель: Предотвращение несанкционированного доступа из одного контейнера к ресурсам других контейнеров и хостовой операционной системы.

Требования к реализации: В контейнерной среде должны обеспечиваться:

изоляция областей памяти, относящихся к различным контейнерам;

недоступность записи в корневую файловую систему хостовой операционной системы для программного обеспечения, выполняемого внутри контейнера;

ограничение прав программного обеспечения, выполняемого внутри

контейнера, на использование периферийных устройств, устройств хранения данных и съемных машинных носителей информации (блочных устройств), входящих в состав информационной системы;

ограничение прав программного обеспечения, выполняемого внутри контейнера, на использование вычислительных ресурсов (оперативной памяти, операций ввода-вывода за период времени) хостовой операционной системы.

Указанные меры защиты информации реализуются за счет применения в информационной системе встроенных в средства контейнеризации и хостовые операционные системы механизмов безопасности.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должна обеспечиваться:

изоляция пространств идентификаторов процессов контейнеров;

изоляция пространств имен для межпроцессного взаимодействия контейнеров;

изоляция пространств имен для пользователей и групп контейнеров;

изоляция пространств имен хостов и доменов контейнеров;

изоляция сетевых пространств имен контейнеров;

изоляция пространств имен для иерархии каталогов контейнеров.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКО.5	+	+	+
Усиление ЗКО.5		1	1

ЗКО.6 Идентификация и аутентификация в контейнерной среде

Цель: Исключение несанкционированного доступа субъектов доступа, не прошедших идентификацию и аутентификацию, к объектам доступа в контейнерной среде.

Требования к реализации: Должна обеспечиваться в соответствии с мерами защиты информации ИАФ.1, ИАФ.3 идентификация и аутентификация пользователей, реализующих следующие роли в контейнерной среде:

разработчик образов контейнеров;

администратор безопасности средств контейнеризации;

администратор средств контейнеризации;

администратор хостовой операционной системы.

Указанная мера защиты информации реализуется за счет применения в информационной системе встроенных в средства контейнеризации и хостовые операционные системы механизмов безопасности.

Требования к документированию: В эксплуатационной документации на информационную систему должен быть определен порядок идентификации и аутентификации субъектов доступа в контейнерной среде.

Требования к усилению:

1) должна обеспечиваться идентификация в контейнерной среде следующих объектов доступа:

образы контейнеров;

контейнеры;

средства контейнеризации.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКО.6	+	+	+
Усиление ЗКО.6			

ЗКО.7 Управление контейнерами и их образами (оркестрация)

Цель: Обеспечение централизованного управления контейнерами и их образами в контейнерной среде.

Требования к реализации: В контейнерной среде должны обеспечиваться:

создание, модификация, хранение, получение и удаление образов контейнеров;

инвентаризация контейнеров и их образов;

управление размещением и перемещением файлов-образов контейнеров между носителями (системами хранения данных);

управление размещением и перемещением исполняемых контейнеров между серверами контейнеризации;

управление размещением и перемещением данных, обрабатываемых с использованием контейнеров, между носителями (системами хранения данных).

В контейнерной среде должен обеспечиваться контроль за перемещением исполняемых контейнеров за пределы информационной системы (сегментов информационной системы) и (или) информационно-телекоммуникационной инфраструктуры, на базе которой они функционируют.

Управление образами контейнеров должно обеспечивать размещение образов контейнеров, запускаемых в рамках информационной системы, только на ресурсах технических средств, входящих в состав информационной системы.

Указанные меры защиты информации реализуются за счет применения в информационной системе встроенных в средства контейнеризации и хостовые операционные системы механизмов безопасности.

Требования к документированию: Не предъявляются.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКО.7	+	+	+
Усиление ЗКО.7			

ЗКО.8 Выявление и устранение уязвимостей в контейнерной среде

Цель: Предотвращение несанкционированного доступа к контейнерной среде за счет эксплуатации уязвимостей образов контейнеров.

Требования к реализации: При применении средств контейнеризации должны обеспечиваться:

выявление известных уязвимостей при создании, установке в информационную систему и хранении образов контейнеров во взаимодействии со средством контроля и анализа защищенности на основе сведений, содержащихся в банке данных угроз безопасности информации ФСТЭК России, а также в иных источниках, содержащих сведения об известных уязвимостях;

оповещение о выявленных уязвимостях администратора безопасности информационной системы.

устранение выявленных уязвимостей образов контейнеров.

Выявление известных уязвимостей в образах контейнеров должно осуществляться не реже одного раза в месяц.

Требования к документированию: В эксплуатационной документации на информационную систему должен быть определен порядок выявления и устранения уязвимостей в образах контейнеров.

Требования к усилению:

1) выявление известных уязвимостей в образах контейнеров должно осуществляться не реже одного раза в неделю;

2) должно быть запрещено создание образов контейнеров, содержащих известные уязвимости критического и высокого уровня опасности, или, в случае невозможности устранения уязвимостей, в их отношении должны быть приняты меры, предотвращающие их эксплуатацию.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКО.8	+	+	+
Усиление ЗКО.8		1, 2	1, 2

4.6. Защита сервисов электронной почты (ЗЭП)

ЗЭП.1 Защита ящиков и сообщений электронной почты

Цель: Исключение возможности несанкционированного доступа к объектам электронной почты (ящикам и сообщениям электронной почты) информационной системы (информационной инфраструктуры оператора).

Требования к реализации: Должны быть реализованы следующие меры защиты информации для обеспечения защиты ящиков и сообщений электронной почты:

периодический анализ (аудит) ящиков электронной почты на наличие ящиков, подлежащих удалению;

регистрация событий безопасности, связанных с действиями пользователей сервисов электронной почты в соответствии с мерами защиты информации РСБ.1 – РСБ.5.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должно обеспечиваться автоматическое блокирование доступа к ящикам электронной почты после установленного времени их неиспользования (неактивности);

2) должно быть обеспечено периодическое резервное копирование содержимого ящиков электронной почты.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗЭП.1	+	+	+
Усиление ЗЭП.1			

ЗЭП.2 Управление доступом пользователей

Цель: Исключение несанкционированного доступа к объектам электронной почты (ящикам и сообщениям электронной почты) информационной системы (информационной инфраструктуры оператора).

Требования к реализации: Должны быть реализованы следующие меры защиты информации для обеспечения защиты ящиков электронной почты и сообщений электронной почты:

доступ пользователей к ящикам электронной почты должен осуществляться после прохождения процедуры идентификации и аутентификации;

идентификация и аутентификация пользователей при доступе к ящикам

электронной почты в соответствии с мерами защиты информации ИАФ.1, ИАФ.3.

Доступ субъектов доступа к общим (групповым) ящикам электронной почты и группам рассылки должен осуществляться по согласованию с владельцем группы ящиков электронной почты (рассылок).

Требования к документированию: Не предъявляются.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗЭП.2	+	+	+
Усиление ЗЭП.2			

ЗЭП.3 Защита от вредоносных вложений

Цель: Обеспечение антивирусной защиты объектов электронной почты (ящиков и сообщений электронной почты), включающее:

обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, сокрытия присутствия другого вредоносного программного обеспечения в информационной системе, сокрытия свидетельств несанкционированного доступа к любым ресурсам информационной системы;

обеспечение реагирования на обнаружение вредоносного программного обеспечения.

Требования к реализации: Должна обеспечиваться антивирусная защита в соответствии с мерой защиты информации АВЗ.2.

Должен обеспечиваться контроль вложений и ссылок в составе сообщений электронной почты с использованием индикаторов компрометации, содержащих информацию об объектах и (или) действиях, которая свидетельствует о реализованных вредоносных действиях (операциях).

Должно быть обеспечено блокирование сообщений электронной почты, содержащих вложения, имеющие неразрешенные форматы файлов (вложений).

Должна обеспечиваться возможность проведения ретроспективного анализа вложений и ссылок ранее поступивших сообщений электронной почты на наличие вредоносного программного обеспечения.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) контроль вложений, поступающих пользователям информационной

системы в составе сообщений электронной почты, должен осуществляться с использованием замкнутой системы (среды) предварительного выполнения программ («песочницы»);

2) должно обеспечиваться блокирование возможности использования заархивированных с использованием паролей вложений до их проверки на наличие компьютерных вирусов.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗЭП.3	+	+	+
Усиление ЗЭП.3			

ЗЭП.4 Защита от фишинга

Цель: Обеспечение выявления и блокирования сообщений электронной почты, содержащих поддельные данные и фишинговые элементы, направленные на компрометацию учетных записей, или иное несанкционированное воздействие на информационную систему (информационную инфраструктуру оператора).

Требования к реализации: Должен обеспечиваться контроль текста сообщения (контента), содержащегося в сообщении электронной почты, и ссылок, ведущих на сторонние информационные ресурсы, на наличие вредоносных и фишинговых элементов.

Должны обеспечиваться:

фильтрация сообщений электронной почты на основе информации об отправителе сообщения (IP-адреса, доменные имена), в том числе с использованием «черных» списков (запрещенные отправители) и (или) «белых» списков (разрешенные отправители);

фильтрация сообщений электронной почты по содержимому с использованием критериев, позволяющих относить сообщения к фишинговым.

Должна обеспечиваться возможность проведения ретроспективного анализа сообщений электронной почты на наличие поддельных данных и (или) фишинговых элементов.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должно осуществляться блокирование сообщений электронной почты, содержащих поддельные данные и (или) фишинговые элементы, или помещение их в карантин;

2) должна осуществляться фильтрация сообщений электронной почты

на основе репутационной информации об отправителе сообщения;

3) контроль сообщений электронной почты на наличие фишинговых элементов должен осуществляться с использованием замкнутой системы (среды) предварительного выполнения программ («песочницы»);

4) должны обеспечиваться контроль адресов электронной почты, с которых было отправлено сообщение электронной почты с целью верификации адресов электронной почты, а также обнаружение фактов подделки электронных писем от легитимных отправителей.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗЭП.4	+	+	+
Усиление ЗЭП.4		1	1

ЗЭП.5 Защита от спама

Цель: Предотвращение поступления незапрашиваемых сообщений электронной почты (спама) пользователям информационной системы.

Требования к реализации: Должен обеспечиваться контроль поступающих сообщений электронной почты, позволяющий обнаруживать незапрашиваемые сообщения.

Контроль поступающих сообщений электронной почты должен осуществляться за счет:

фильтрации сообщений электронной почты на основе информации об отправителе сообщения (IP-адреса, доменные имена), в том числе с использованием «черных» списков (запрещенные отправители) и (или) «белых» списков (разрешенные отправители);

фильтрации сообщений электронной почты по содержимому с использованием критериев, позволяющих относить сообщения к спаму.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должна осуществляться фильтрация сообщений электронной почты на основе репутационной информации об отправителе сообщения;

2) должно быть установлено ограничение на количество сообщений электронной почты, поступающих от одного отправителя за период времени, при превышении которого последующие сообщения электронной почты должны блокироваться;

3) должны применяться технологии, позволяющие однозначно верифицировать адреса электронной почты, от имени которых были отправлены сообщения.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗЭП.5	+	+	+
Усиление ЗЭП.5			

ЗЭП.6 Защита метаданных и иной технической информации сервисов электронной почты

Цель: Обеспечение защиты метаданных и иной технической информации, связанной с функционированием сервисов электронной почты, для предотвращения их несанкционированного использования.

Требования к реализации: Информационное взаимодействие между пользователями ящиков электронной почты и сервером электронной почты должно осуществляться с использованием технологий и сетевых протоколов, обеспечивающих сокрытие метаданных и иной технической информации, связанной с функционированием сервисов электронной почты.

Должно обеспечиваться сокрытие метаданных и иной технической информации, связанной с функционированием сервисов электронной почты, а именно:

служебные заголовки сообщений электронной почты, содержащие информацию об инфраструктуре информационной системы, а также программном обеспечении, с использованием которого отправлено сообщение электронной почты (например, X-Mailer, User-Agent);

служебные заголовки сообщений электронной почты, содержащие информацию о маршруте передачи сообщения (например, X-Originating-IP, Message-ID).

Сокрытие информации, содержащейся в служебных заголовках, должно осуществляться одним из следующих способов:

настройка параметров сервера электронной почты, при которой обеспечивается запрет записи информации в служебные заголовки отправляемых сообщений электронной почты;

использование промежуточного сервера (SMTP-шлюз или прокси-сервер), позволяющего подменять или удалять информацию, содержащуюся в служебных заголовках.

Должна быть исключена возможность получения информации о существующих ящиках электронной почты, содержащихся на сервере электронной почты, с использованием:

запрета использования на почтовом сервере команд VRFY/EXPN;

средства защиты информации, позволяющего блокировать запросы

на получение информации о существующих ящиках электронной почты, содержащихся на сервере электронной почты.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) сервер электронной почты, доступный из сети «Интернет», не должен поддерживать прием и передачу почтового сетевого трафика, предназначенного для других информационных систем (доменов).

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗЭП.6	+	+	+
Усиление ЗЭП.6			

4.7. Защита веб-технологий (ЗВТ)

ЗВТ.1 Защита пользовательских данных

Цель: Обеспечение защиты пользовательских данных, передаваемых, обрабатываемых и хранящихся в составе веб-приложения.

Требования к реализации: Сетевое информационное взаимодействие между субъектами доступа и объектами доступа (пользователями и приложениями) должно осуществляться посредством программного интерфейса приложений, защита данных в котором обеспечивается в соответствии с мерой защиты информации ЗПИ.1.

Доступ субъектов доступа к пользовательским данным, хранящимся в веб-приложении, а также доступ к функциям веб-приложения должен осуществляться в соответствии с мерой защиты информации УПД.2.

Сетевое взаимодействие между субъектами и объектами доступа (пользователями и приложениями) должно осуществляться с учетом мер защиты информации ЗКС.1 – ЗКС.5.

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены:

объекты доступа, содержащиеся в веб-приложении;

перечень типов пользователей веб-приложения.

Требования к усилению:

1) в информационной системе должно быть исключено кэширование пользовательских данных, определяемых оператором, в веб-браузере (например, путем использования соответствующих директив заголовков Cache-Control, Pragma протокола передачи гипертекста);

2) в информационной системе должны быть отключены функции автоматического заполнения форм (например, путем установления соответствующего значения атрибута Autocomplete протокола передачи гипертекста) для полей, предназначенных для ввода пользовательских данных, определяемых оператором;

3) в информационной системе должна обеспечиваться защита пользовательских данных от компрометации посредством межсайтового скриптинга путем настойки соответствующих заголовков безопасности протокола передачи гипертекста;

4) в информационной системе должна обеспечиваться защита пользовательских данных от компрометации посредством подмены (перекрытия) элементов графического интерфейса путем контроля вложенности контекстов отображения.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗВТ.1	+	+	+
Усиление ЗВТ.1			

ЗВТ.2 Управление доступом пользователей

Цель: Исключение несанкционированного доступа к объектам доступа, содержащимся в веб-приложении информационной системы (информационной инфраструктуры оператора).

Требования к реализации: В информационной системе должны быть обеспечены:

идентификация и аутентификация пользователей веб-приложения, системы управления контентом веб-приложения в соответствии с мерами защиты информации ИАФ.1, ИАФ.3;

управление доступом пользователей к функциям и данным, хранящимся в веб-приложении, а также в системе управления контентом веб-приложения, в соответствии с мерами защиты информации УПД.1 – УПД.6;

ограничение числа параллельных сеансов доступа к веб-приложению в соответствии с мерой защиты информации УПД.7;

автоматическое завершение сеансов доступа к веб-приложению при неактивности в соответствии с мерой защиты информации УПД.8;

проверка прав доступа субъектов доступа при каждом обращении (запросе) к функциям или данным веб-приложения, включая обработку запросов на чтение и модификацию данных, вызов API-методов, загрузку файлов, за исключением

определенных общедоступных ресурсов в соответствии с мерой защиты информации УПД.9.

Возможность идентификации и аутентификации пользователя только на стороне пользователя веб-приложения (например, проверка доступа на уровне JavaScript-кода в веб-браузере) должна быть исключена.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) идентификация и аутентификация привилегированных пользователей (администраторов, администраторов безопасности) веб-приложения должны осуществляться с использованием ввода второго фактора при использовании многофакторной аутентификации в составе информационной системы в соответствии с мерами защиты информации ИАФ.1, ИАФ.3.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗВТ.2	+	+	+
Усиление ЗВТ.2		1	1

ЗВТ.3 Контроль и фильтрация трафика веб-приложений

Цель: Обеспечение контроля и фильтрации сетевого трафика веб-приложений.

Требования к реализации: В информационной системе должна быть обеспечена возможность автоматического контроля и фильтрации сетевого трафика веб-приложения, поступающего по сетевому интерфейсу программного взаимодействия с веб-приложением, в соответствии с мерой защиты информации ЗПИ.3.

Контроль и фильтрация данных пользовательских запросов должны быть направлены на обнаружение, как минимум, следующих событий:

нарушение содержащимися в запросе пользователя данными установленных в информационной системе ограничений по типу, размеру, формату и допустимому содержимому (схемы запроса);

включение в состав запроса управляющих символов и конструкций, способных изменить логику обработки веб-приложением пользовательских запросов (например, SQL-запросы, JavaScript-код, системные команды);

включение в состав запроса аутентификаторов доступа или иной чувствительной информации в открытом виде;

формирование запросов автоматизированными инструментальными средствами поиска и эксплуатации уязвимостей веб-приложений;

формирование запросов автоматизированными инструментальными средствами перебора (подбора) аутентификационной информации.

Контроль и фильтрация сетевого трафика веб-приложения должны обеспечиваться на основе как минимум следующих атрибутов пользовательского запроса протокола передачи гипертекста:

унифицированный идентификатор запрошенного информационного ресурса;

веб-метод запроса;

значения заголовков запроса;

наименования и значения параметров запроса;

идентификатор веб-клиента (набор значений заголовков атрибутов веб-клиента).

Контроль и фильтрация сетевого трафика веб-приложений, использующих расширения протокола передачи гипертекста и иные версии прикладных протоколов (например, протокол WebSocket), должны обеспечиваться на основе атрибутов, описанных во внутреннем стандарте, содержащем требования к типовым конфигурациям и настройкам программных, программно-аппаратных средств.

Для веб-приложений, доступных из сети «Интернет», указанные меры защиты информации должны быть реализованы с использованием межсетевого экрана уровня веб-сервера, или многофункционального межсетевого экрана уровня сети.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) в информационной системе контроль и фильтрация трафика веб-приложений должны осуществляться в том числе методом анализа вложений (полезной нагрузки) пользовательских запросов;

2) в информационной системе должны выявляться события, связанные с нарушениями в пользовательских запросах спецификации протокола передачи гипертекста и ограничений на структуру пользовательского запроса.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗВТ.3	+	+	+
Усиление ЗВТ.3			1

ЗВТ.4 Регистрация событий безопасности в веб-приложениях и реагирование на них

Цель: Определение состава и содержания информации о событиях безопасности, подлежащих регистрации в веб-приложениях.

Требования к реализации: В информационной системе в соответствии с мерами защиты информации РСБ.1 – РСБ.5 должна быть обеспечена регистрация событий безопасности, связанных с попытками доступа субъектов доступа к объектам доступа веб-приложения в соответствии с мерами защиты информации УПД.1 – УПД.9.

В информационной системе должна быть обеспечена регистрация событий безопасности на уровне межсетевого экрана уровня веб-сервера и (или) многофункционального межсетевого экрана уровня сети, обеспечивающего контроль и фильтрацию сетевого трафика веб-приложения.

На уровне веб-приложения дополнительно должна осуществляться регистрация следующих типов событий безопасности:

события безопасности, связанные с идентификацией и аутентификацией пользователей веб-приложений;

события безопасности, связанные с управлением учетными записями пользователей веб-приложения (для веб-приложений, допускающих такие изменения);

события безопасности, связанные с изменением типов субъектов доступа, типов объектов доступа (для веб-приложений, допускающих такие изменения);

события безопасности, связанные с изменением типов доступа субъектов доступа к объектам доступа, в том числе к функциям веб-приложений (для веб-приложений, допускающих такие изменения);

события безопасности, связанные с ограничением числа параллельных сеансов доступа к веб-приложению;

события безопасности, связанные с автоматическим завершением сеансов доступа к веб-приложению при неактивности;

события безопасности, связанные с изменениями параметров настроек веб-приложения.

На уровне межсетевого экрана уровня веб-сервера и (или) многофункционального межсетевого экрана уровня сети, обеспечивающего контроль и фильтрацию сетевого трафика веб-приложения, должна осуществляться регистрация следующих типов событий безопасности:

события безопасности, связанные с фильтрацией сетевого трафика;

события безопасности, связанные с обнаружением признаков вредоносного воздействия на веб-приложение.

В информационной системе должна обеспечиваться передача зарегистрированных событий безопасности в систему управления событиями безопасности информации, функционирующую в информационной системе.

В информационной системе по результатам анализа событий безопасности должно обеспечиваться автоматическое реагирование на них посредством:

блокирования сетевого сеанса взаимодействия с веб-приложением для событий безопасности, определенных оператором;

уведомления администратора (администратора безопасности) информационной системы о факте и причинах блокирования сетевого сеанса.

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены:

перечень веб-приложений, для которых должна быть настроена регистрация событий безопасности;

перечень средств защиты информации, осуществляющих регистрацию событий безопасности, связанных с веб-приложением;

минимальный перечень событий безопасности, подлежащих регистрации.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗВТ.4	+	+	+
Усиление ЗВТ.4			

ЗВТ.5 Проверка файлов, передаваемых веб-приложениями, на вредоносное программное обеспечение

Цель: Обеспечение антивирусной защиты веб-приложений информационной системы, включающее:

обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, сокрытия присутствия другого вредоносного программного обеспечения в информационной системе, сокрытия свидетельств несанкционированного доступа к любым ресурсам информационной системы;

обеспечение реагирования на обнаружение вредоносного программного обеспечения.

Требования к реализации: Должна обеспечиваться проверка всех файлов, передаваемых веб-приложениями, на вредоносное программное обеспечение в соответствии с мерой защиты информации АВЗ.1.

Проверка должна включать анализ всех передаваемых в теле запроса файлов, а также составляющих тело запроса скриптов и данных, поступающих в веб-приложение.

Должен быть исключен автоматический запуск переданных файлов в операционной системе на стороне веб-приложения или пользователя (например, путем осуществления фильтрации исполняемых файлов, определения соответствия типа файла его содержимому, предотвращения маскирования исполняемых файлов под иные форматы).

Требования к документированию: Не предъявляются.

Требования к усилению:

1) в информационной системе должна обеспечиваться возможность проведения ретроспективного анализа файлов.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗВТ.5	+	+	+
Усиление ЗВТ.5			

4.8. Защита программных интерфейсов взаимодействия приложений (API) (ЗПИ)

ЗПИ.1 Защита данных API

Цель: Исключение несанкционированного доступа к информационной системе при использовании программных интерфейсов взаимодействия приложений (API).

Требования к реализации: При организации сетевого взаимодействия между субъектами доступа (пользователями и приложениями) и объектами доступа посредством API должна обеспечиваться минимизация объема информации, раскрывающей структуру информационной системы, или иной информации, передаваемой посредством API.

В информационной системе должна обеспечиваться минимизация состава информации, возвращаемой в сообщениях об ошибках взаимодействия с API, раскрывающей структуру и особенности функционирования информационной системы или иную конфиденциальную информацию.

Должна обеспечиваться минимизация состава информации, содержащейся в аутентификаторах доступа к API путем исключения данных, раскрывающих структуру информационной системы или иные конфиденциальные сведения.

При сетевом информационном взаимодействии внешних субъектов доступа с API через сеть «Интернет» должна обеспечиваться с учетом мер защиты информации ЗКС.1 – ЗКС.5.

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены:

перечни API, предоставляемых внешним и внутренним пользователям информационной системой;

требования к режимам и настройкам программного обеспечения, обеспечивающим конфиденциальность информации и служебных данных, передаваемых при получении доступа и взаимодействии с API.

Требования к усилению:

1) должен осуществляться ежегодный пересмотр режимов и настроек программного обеспечения, реализующего API, с целью выявления уязвимостей его конфигурации.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗПИ.1	+	+	+
Усиление ЗПИ.1		1	1

ЗПИ.2 Управление доступом пользователей и приложений

Цель: Исключение несанкционированного доступа к информационной системе субъектов доступа (пользователей и приложений), взаимодействующих с программным обеспечением информационной системы посредством API, не прошедших процедуру аутентификации.

Требования к реализации: В информационной системе должны быть осуществлены:

определение перечня API, для которых требуется контроль доступа пользователей и приложений;

обеспечение идентификации и аутентификации пользователей, взаимодействующих с программным обеспечением информационной системы посредством API в соответствии с мерами защиты информации ИАФ.1, ИАФ.3;

управление доступом пользователей и приложений, получающих доступ к информационной системе посредством входящих в перечень API, соответствии с мерами защиты информации УПД.1 – УПД.6;

ограничение числа параллельных сеансов доступа к API в соответствии с мерой защиты информации УПД.7;

автоматическое завершение сеансов доступа к API при неактивности в соответствии с мерой защиты информации УПД.8;

проверка прав доступа субъектов доступа при каждом обращении (запросе) к API, за исключением определенных общедоступных ресурсов, в соответствии с мерой защиты информации УПД.9;

установлены ограничения на частоту и объем обращений к программным интерфейсам (API), а также порядок автоматического выявления и пресечения попыток подбора средств аутентификации.

Требования к документированию: Не предъявляются.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗПИ.2	+	+	+
Усиление ЗПИ.2			

ЗПИ.3 Проверка на соответствие спецификации API

Цель: Обеспечение контроля запросов к интерфейсам взаимодействия приложений с целью выявления и блокирования запросов, не соответствующих утвержденной спецификации API.

Требования к реализации: При организации сетевого информационного взаимодействия между субъектами доступа (пользователями и приложениями) и объектами доступа в информационной системе посредством API в информационной системе должна быть определена спецификация API.

В информационной системе должна быть обеспечена возможность автоматической проверки запросов на предмет соответствия формату, структуре и ограничениям, предусмотренным разработанной спецификацией API. В информационной системе должно быть определено множество правил, описывающих виды запросов, не соответствующих спецификации API, подлежащие автоматическому блокированию средствами защиты информации до момента оказания запросом воздействия на приложение, доступное посредством API.

В информационной системе должен быть осуществлен пересмотр перечня и спецификации API на предмет выявления недокументированных, устаревших и неиспользуемых API и ресурсов, доступных внешним пользователям информационной системы посредством данных API, ежегодно или при изменении API.

В информационной системе должна осуществляться проверка поступающих к API запросов на соответствие формату, структуре и ограничениям, и блокировка запросов, не соответствующих спецификации API.

Требования к документированию: Не предъявляется.

Требования к усилению:

1) в информационной системе должен быть осуществлен пересмотр перечня и спецификации API при изменении кода или конфигурации приложений, реализующих данные API;

2) должен обеспечиваться автоматический анализ трафика сетевого информационного взаимодействия между внешними субъектами доступа и внешними API информационной системы на предмет выявления недокументированных, устаревших и неиспользуемых API и ресурсов, доступных внешним пользователям информационной системы посредством данных API.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗПИ.3	+	+	+
Усиление ЗПИ.3			1

4.9. Защита конечных устройств (ЗКУ)

ЗКУ.1 Управление доступом к конечным устройствам

Цель: Исключение несанкционированного доступа к конечным устройствам.

Требования к реализации: В информационной системе при защите конечных устройств должны обеспечиваться:

идентификация и аутентификация пользователей конечных устройств в соответствии с мерами защиты информации ИАФ.1, ИАФ.3;

управление доступом пользователей к конечным устройствам в соответствии с мерами защиты информации УПД.1 – УПД.9.

При предоставлении пользователям доступа к конечным устройствам должен применяться принцип наименьших привилегий.

Должен осуществляться контроль доступа пользователей к интерфейсам ввода-вывода конечных устройств.

Указанные меры защиты информации реализуются путем применения механизмов безопасности операционных систем и (или) средствами идентификации и аутентификации.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) на конечных устройствах должны применяться доверенные средства сетевого взаимодействия (в том числе, доверенные аппаратные сетевые интерфейсы);

2) в составе конечного устройства должны применяться аппаратные средства гарантированного отключения незадействованных компонентов регистрации акустических (микрофоны) или оптических (веб-камеры) сигналов (в случае применения в конечном устройстве таких компонентов);

3) должна выполняться фильтрация команд, обеспечивающая передачу на устройства ввода и (или) вывода в информационной системе, в том числе на многофункциональные устройства и принтеры, только разрешенных команд с целью исключения несанкционированного доступа к информации;

4) в составе конечного устройства, предназначенного для подключения к нескольким информационным системам информационной инфраструктуры оператора, должны применяться компоненты, обеспечивающие гарантированное (физическое) разделение информационных систем (сегментов, контуров) и невозможность сохранения созданных данных в энергонезависимую память;

5) должна осуществляться идентификация конечных устройств пользователей.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКУ.1	+	+	+
Усиление ЗКУ.1			

ЗКУ.2 Обеспечение целостности программного обеспечения конечного устройства

Цель: Исключение несанкционированного изменения программного обеспечения конечного устройства.

Требования к реализации: В информационной системе должна обеспечиваться целостность следующего программного обеспечения конечных устройств:

операционные системы;

программное обеспечение средств защиты информации;

иное программное обеспечение, определяемое в информационной системе.

На конечных устройствах должен быть обеспечен запрет на установку и запуск (инсталляцию) неразрешенного к использованию программного обеспечения.

Обеспечение целостности программного обеспечения конечных устройств реализуется путем применения механизмов безопасности операционных систем и иных средств защиты информации.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должна обеспечиваться доверенная загрузка операционных систем автоматизированных рабочих мест пользователей, на которых осуществляется обработка информации ограниченного доступа и (или) выполнение значимых функций оператора;

2) должна обеспечиваться доверенная загрузка операционных систем серверов, на которых осуществляется обработка информации ограниченного доступа и (или) выполнение значимых функций оператора;

3) должна обеспечиваться доверенная загрузка сетевых средств защиты информации;

4) должна обеспечиваться доверенная загрузка программного обеспечения телекоммуникационного оборудования;

5) должна обеспечиваться блокировка запуска программного обеспечения и (или) блокировка конечного устройства в случае обнаружения фактов нарушения целостности;

6) должен обеспечиваться контроль целостности базовой системы ввода-вывода конечных устройств;

7) должен обеспечиваться контроль целостности микропрограммного обеспечения и аппаратных компонентов конечных устройств;

8) должен обеспечиваться запрет применения функций разработки и отладки программ на конечных устройствах. При необходимости применения функций разработки и отладки программ должно обеспечиваться выполнение процедур контроля целостности программного обеспечения после завершения каждого процесса функционирования средств разработки и отладки программ.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКУ.2	+	+	+
Усиление ЗКУ.2			

ЗКУ.3 Антивирусная защита и обнаружение и предотвращение вторжений на конечных устройствах

Цель: Обнаружение вторжений (компьютерных атак), вредоносного программного обеспечения и их нейтрализация на конечных устройствах.

Требования к реализации: Должна обеспечиваться антивирусная защита конечных устройств информационной системы в соответствии с мерой защиты информации АВЗ.1.

На конечных устройствах, где отсутствует техническая возможность применения средств антивирусной защиты (телекоммуникационное оборудование, принтеры, многофункциональные устройства и иные конечные устройства), должны приниматься меры, обеспечивающие невозможность реализации угроз, связанных с вредоносным программным обеспечением.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) на конечных устройствах информационной системы, имеющей доступ к ресурсам сети «Интернет», должны обеспечиваться обнаружение вторжений (компьютерных атак) и реагирование на них с использованием систем обнаружения вторжений уровня узла и (или) средств обнаружения и реагирования на уровне узла;

2) должен обеспечиваться периодический ретроспективный анализ событий безопасности средств обнаружения и реагирования на уровне узла на наличие признаков вторжений (компьютерных атак);

3) должно обеспечиваться взаимодействие с репутационной базой угроз для обогащения информацией о признаках вторжений (компьютерных атак);

4) должно обеспечиваться применение репутационной базы угроз для проверки файловых объектов, сетевых и прикладных артефактов (IP-адресов, доменов, URL) в масштабе, близком к реальному времени;

5) должна обеспечиваться передача файловых объектов (исполняемых файлов, архивов) от применяемых на узлах информационной системы средств обнаружения и реагирования на уровне узла в замкнутую систему (среду) предварительного выполнения программ («песочницу») для динамического анализа в автоматическом режиме.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКУ.3	+	+	+
Усиление ЗКУ.3		1	1

ЗКУ.4 Мониторинг процессов и состояния устройства

Цель: Выявление несанкционированных действий пользователей и выполняемых процессов на конечных устройствах пользователей и серверов.

Требования к реализации: Должен обеспечиваться мониторинг процессов и состояния конечных устройств пользователей и серверов в соответствии с мерами защиты информации РСБ.1 – РСБ.5.

При мониторинге процессов и состояний рекомендуется отслеживать:

запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;

выполнение процессов с высоким уровнем привилегий, скрытых процессов и системных служб;

выполнение процессов, инициированных средствами защиты информации конечных устройств;

выполнение команд в интерпретаторе командной строки;

попытки доступа к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей и иным объектам доступа);

попытки идентификации и аутентификации пользователей конечных устройств;

попытки удаленного доступа;

подключение внешних устройств с использованием интерфейсов ввода-вывода;

попытки осуществления беспроводного доступа;

изменение программной конфигурации конечного устройства.

Указанные меры защиты информации реализуются путем применения механизмов безопасности операционных систем, и (или) средств обнаружения и реагирования на уровне узла, и (или) иных средств защиты информации.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) при осуществлении мониторинга процессов и состояния конечных устройств должны выявляться аномалии в действиях пользователей и выполнении процессов конечных устройств;

2) должна обеспечиваться интеграция результатов мониторинга процессов и состояния конечных устройств, полученных по результатам отслеживания разных процессов, и их корреляция с целью выявления инцидентов безопасности и реагирования на них.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКУ.4	+	+	+
Усиление ЗКУ.4			

ЗКУ.5 Контроль и фильтрация трафика на конечном устройстве

Цель: Обеспечение безопасности сетевого взаимодействия конечных устройств.

Требования к реализации: Должен обеспечиваться контроль сетевого трафика конечного устройства, включающий контроль:

доступа к внешним ресурсам информационной системы;

доступа к внутренним ресурсам информационной системы.

Должна осуществляться фильтрация сетевого трафика конечного устройства по определенным правилам фильтрации (по IP-адресам, портам, протоколам, по содержимому и иным правилам межсетевых экранов, многофункциональных межсетевых экранов уровня сети).

Указанные меры защиты информации реализуются путем применения механизмов безопасности операционных систем, и (или) средств обнаружения и реагирования на уровне узла, и (или) иных средств защиты информации.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должен обеспечиваться контроль сетевого трафика конечного устройства по времени доступа к определенным ресурсам;

2) должен выполняться анализ сетевого трафика конечного устройства, включающий определение потоков данных, информацию об отправителях и получателях, используемых сетевых протоколах и портах, статусах сетевых соединений (открытое, закрытое);

3) на конечных устройствах должны применяться аппаратные средства сетевого взаимодействия (в том числе, доверенные аппаратные сетевые интерфейсы), обеспечивающие фильтрацию входящего и (или) исходящего сетевого трафика узла по сетевым (IP) и (или) физическим (MAC) адресам;

4) в составе конечного устройства должны применяться аппаратные средства гарантированной блокировки линий обмена данными по команде и (или) по расписанию.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКУ.5			
Усиление ЗКУ.5			

ЗКУ.6 Анализ и реагирование на события безопасности

Цель: Исключение несанкционированного доступа к конечным устройствам путем анализа событий безопасности и реагирования на них.

Требования к реализации: Должен выполняться анализ зарегистрированных событий безопасности, по результатам анализа должно осуществляться реагирование на выявленные компьютерные инциденты.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) реагирование на выявленные признаки компьютерных инцидентов должно включать отправку уведомлений администратору безопасности информационной системы;

2) должен обеспечиваться анализ зарегистрированных на конечном устройстве событий безопасности системой управления событиями безопасности информации;

3) должно обеспечиваться реагирование на обнаружение компьютерных инцидентов средствами управления инцидентами информационной безопасности (в случае применения средства обнаружения и реагирования на уровне узла с учетом меры защиты информации ЗКУ.3 и наличия в информационной системе системы управления событиями безопасности информации);

4) должны обеспечиваться блокирование и (или) изоляция конечного устройства, на котором выявлены компьютерные инциденты.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКУ.6	+	+	+
Усиление ЗКУ.6		1	1

4.10 Защита мобильных устройств (ЗМУ)

ЗМУ.1 Идентификация и аутентификация пользователей

Цель: Исключение доступа к информационной системе пользователей мобильных устройств, не прошедших процедуру идентификации и аутентификации.

Требования к реализации: При применении пользователями мобильных устройств для доступа к информационной системе, а также при предоставлении доступа пользователям к информации, содержащейся в информационной системе, в целях выполнения своих служебных обязанностей (функций) должна быть реализована идентификация и аутентификация пользователей в соответствии с мерами защиты информации ИАФ.1 – ИАФ.4.

При аутентификации пользователя на мобильном устройстве используется простая (парольная) аутентификация. Длина пароля должна быть не менее 6 символов. Максимальное количество неуспешных попыток ввода неправильного пароля до блокировки учетной записи пользователя – 5, блокировка мобильного устройства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации на 15 минут, смена паролей не более чем через 30 дней. Запрещается повторно использовать 12 последних паролей для доступа к мобильному устройству.

Указанные меры реализуются за счет применения в информационной системе операционных систем и (или) средствами идентификации и аутентификации.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) длина пароля для входа пользователя в мобильное устройство должна быть не менее 10 символов.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗМУ.1	+	+	+
Усиление ЗМУ.1		1	1

ЗМУ.2 Управление доступом пользователей к мобильным устройствам

Цель: Исключение несанкционированного доступа пользователей к мобильным устройствам.

Требования к реализации: Должны обеспечиваться меры по управлению доступом пользователей к мобильным устройствам в соответствии с мерами защиты информации УПД.1 – УПД.9, а также по управлению правами доступа пользователей к приложениям, установленным на мобильных устройствах, к информации, содержащейся в мобильном устройстве, и иным объектам доступа.

При применении пользователями мобильных устройств для доступа к информационной системе, а также при предоставлении доступа пользователям к информации, содержащейся в мобильных устройствах, должен применяться принцип наименьших привилегий.

Указанные меры защиты информации реализуются путем применения операционных систем, и (или) средств идентификации и аутентификации, и (или) систем управления мобильными устройствами.

Требования к документированию: Не предъявляются.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗМУ.2	+	+	+
Усиление ЗМУ.2			

ЗМУ.3 Обеспечение целостности

Цель: Обеспечение целостности программной среды мобильных устройств.

Требования к реализации: В информационной системе должен осуществляться контроль целостности следующего программного обеспечения мобильных устройств:

операционные системы;

программное обеспечение средств защиты информации;

прикладное программное обеспечение (приложения).

Контроль целостности программного обеспечения мобильных устройств реализуется за счет применения операционных систем, и (или) систем управления мобильными устройствами, и (или) иных средств защиты информации.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должен обеспечиваться запрет применения функций разработки и отладки программ на мобильных устройствах. При необходимости применения функций разработки и отладки программ должно обеспечиваться выполнение

процедур контроля целостности программного обеспечения после завершения каждого процесса функционирования средств разработки и отладки программ;

2) должна обеспечиваться блокировка запуска программного обеспечения и (или) блокировка мобильного устройства в случае обнаружения фактов нарушения целостности;

3) должна обеспечиваться доверенная загрузка мобильных операционных систем, на которых осуществляется обработка информации ограниченного доступа и (или) выполнение значимых функций.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗМУ.3	+	+	+
Усиление ЗМУ.3		1	1, 2

ЗМУ.4 Защита данных

Цель: Обеспечение защиты данных информационной системы, обрабатываемых на мобильных устройствах и передаваемых между информационной системой и мобильными устройствами.

Требования к реализации: Программное обеспечение на мобильных устройствах, используемое для доступа к информационной системе, не должно сохранять данные в общедоступные каталоги мобильного устройства.

Программное обеспечение мобильных устройств должно сохранять данные информационной системы только в изолированную область памяти, к которой имеет доступ только указанное программное обеспечение.

Создание резервных копий данных информационной системы в общедоступных облачных сервисах в сети «Интернет» с помощью мобильных устройств или установленного на них программного обеспечения должно быть заблокировано.

Указанные меры защиты информации реализуются путем применения операционных систем и (или) систем управления мобильными устройствами.

Обмен данными между информационной системой и мобильными устройствами посредством сети «Интернет» должен осуществляться с учетом реализации меры защиты информации ЗКС.1.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должно осуществляться удаление информации на мобильном устройстве (сброс к заводским настройкам) при превышении допустимого числа неуспешных попыток разблокировки мобильного устройства более чем в два раза;

2) должна быть исключена возможность сохранения информации из программного обеспечения на мобильном устройстве, используемом для доступа к информационной системе, с помощью снимков экрана;

3) должна проводиться очистка памяти мобильного устройства и переустановка программного обеспечения при передаче мобильного устройства от одного пользователя другому.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗМУ.4	+	+	+
Усиление ЗМУ.4			1

ЗМУ.5 Антивирусная защита

Цель: Противодействие внедрению и распространению вредоносного программного обеспечения на мобильных устройствах.

Требования к реализации: Должна обеспечиваться антивирусная защита мобильных устройств информационной системы в соответствии с мерой защиты информации АВЗ.1.

Антивирусная защита мобильных устройств реализуется путем применения средств антивирусной защиты.

Требования к документированию: Не предъявляются.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗМУ.5	+	+	+
Усиление ЗМУ.5			

ЗМУ.6 Контроль приложений

Цель: Обеспечение управления установкой, запуском и функционированием программного обеспечения мобильного устройства (приложениями).

Требования к реализации: По отношению к мобильному устройству должны осуществляться:

контроль установки, запуска, функционирования и обновления приложений;

запрет на установку и запуск неразрешенных к использованию приложений;

запуск и функционирование приложений с минимальными правами, необходимыми для работы приложения.

Должно обеспечиваться управление правами доступа приложений, установленных на мобильных устройствах, к интерфейсам мобильного устройства и ресурсам мобильной операционной системы (например, оперативной памяти, доступу к сети «Интернет», к другим приложениям).

Должен быть реализован запрет использования функций удаленного управления мобильным устройством сторонними приложениями, не входящими в состав и не являющимися средствами защиты информации.

Указанные меры защиты информации реализуются за счет применения операционных систем и (или) систем управления мобильными устройствами.

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены состав программного обеспечения, подлежащего установке на мобильных устройствах (приложений).

Требования к усилению:

1) должно осуществляться централизованное управление параметрами настройки и правами приложений, включая программные компоненты средств защиты информации, установленных на мобильном устройстве;

2) для учета используемых мобильных устройств должны применяться автоматизированные средства инвентаризации.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗМУ.6	+	+	+
Усиление ЗМУ.6			

ЗМУ.7 Ограничение и контроль функциональности

Цель: Ограничение возможностей нарушителя по получению доступа к мобильным устройствам через их интерфейсы.

Требования к реализации: При ограничении и контроле функциональности в мобильном устройстве должны быть:

определены беспроводные каналы передачи данных, допустимые к использованию на мобильных устройствах;

определены интерфейсы ввода-вывода, допустимые к использованию на мобильных устройствах;

реализован запрет на использование беспроводных каналов передачи данных и интерфейсов ввода-вывода, недопустимых к использованию на мобильных устройствах.

Указанные меры защиты информации реализуются за счет применения

операционных систем и (или) систем управления мобильными устройствами.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должна быть реализована взаимная аутентификация мобильных устройств и точек беспроводного доступа, используемых для подключения пользователей мобильных устройств к информационным системам;

2) должны быть аппаратно отключены (заблокированы) неиспользуемые интерфейсы мобильных устройств.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗМУ.7	+	+	+
Усиление ЗМУ.7			

ЗМУ.8 Определение и контроль геопозиции

Цель: Обеспечение получения, регистрации и контроля фактического местоположения мобильных устройств, подключенных к информационной системе.

Требования к реализации: Должна обеспечиваться регистрация информации о местоположении мобильного устройства, с которого осуществляется доступ к информационной системе.

Должны регистрироваться факты невозможности определения геопозиции мобильного устройства (например, вследствие недоступности сигналов спутников, сигналов сотовых вышек или других беспроводных точек, по информации о которых делается вывод о геопозиции мобильного устройства).

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должно быть реализовано ограничение доступа к информационной системе в зависимости от геопозиции мобильного устройства;

2) для определения геопозиции по сигналам сотовых вышек или других беспроводных точек должны использоваться серверы, которые расположены на территории Российской Федерации.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗМУ.8			
Усиление ЗМУ.8			

ЗМУ.9 Регистрация, анализ и реагирование на события безопасности

Цель: Определение состава и содержания информации о событиях безопасности, подлежащих регистрации в мобильных устройствах.

Требования к реализации: Должна обеспечиваться регистрация событий безопасности в операционной системе мобильного устройства в соответствии с мерами защиты информации РСБ.1 – РСБ.5.

Должен выполняться анализ зарегистрированных событий безопасности, по результатам анализа должно осуществляться реагирование на выявленные компьютерные инциденты.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) реагирование на выявленные признаки компьютерных инцидентов должно включать отправку уведомлений администратору безопасности информационной системы;

2) должны обеспечиваться блокирование и (или) изоляция мобильного устройства, на котором выявлены компьютерные инциденты.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗМУ.9	+	+	+
Усиление ЗМУ.9		1	1

4.11. Защита технологий «интернета вещей» (ЗИВ)

ЗИВ.1 Идентификация и аутентификация

Цель: Исключение доступа к информационной системе устройств «интернета вещей», не прошедших процедуру идентификации и аутентификации.

Требования к реализации: Должна обеспечиваться идентификация устройств «интернета вещей» в соответствии с мерой защиты информации ИАФ.2.

Идентификация устройств «интернета вещей» должна обеспечиваться по логическим именам (имя устройства и (или) идентификатор), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, MAC-адресам) или по комбинации имени, логического и (или) физического адресов устройств «интернета вещей».

Аутентификация устройств «интернета вещей» должна обеспечиваться с использованием протоколов аутентификации.

Не допускается осуществлять аутентификацию устройств «интернета вещей» с использованием паролей, установленных по умолчанию.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должна быть обеспечена идентификация устройств «интернета вещей» на основе приватных идентификаторов (псевдонимов), не отражающих реальные наименования и назначение устройств;

2) аутентификация устройств «интернета вещей» должна осуществляться с использованием сертификатов безопасности;

3) должна обеспечиваться взаимная аутентификация устройства «интернета вещей» и другого взаимодействующего устройства до начала их информационного взаимодействия;

4) должна обеспечиваться аутентификация устройств «интернета вещей» по уникальным встроенным средствам аутентификации.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗИВ.1	+	+	+
Усиление ЗИВ.1			

ЗИВ.2 Управление доступом

Цель: Исключение несанкционированного доступа к устройствам «интернета вещей».

Требования к реализации: При реализации управления доступом к устройствам «интернета вещей» должны быть установлены:

методы управления доступом к устройствам «интернета вещей» (например, метод ролевого управления доступом, метод управления доступом, основанный на атрибутах устройств «интернета вещей», метод управления доступом, основанный на списках управления доступом) в соответствии с мерами защиты информации УПД.1 – УПД.9;

виды устройств «интернета вещей», разрешенные для применения в информационной системе;

виды доступа (беспроводной, проводной (коммутируемый) и иные виды доступа), разрешенные для доступа к объектам доступа информационной системы с использованием устройств «интернета вещей»;

протоколы взаимодействия устройств «интернета вещей», разрешенные для применения в информационной системе.

При предоставлении доступа к устройствам «интернета вещей» должен применяться принцип наименьших привилегий.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должно обеспечиваться централизованное управление доступом устройств «интернета вещей»;

2) должны обеспечиваться мониторинг и контроль доступа устройств «интернета вещей» на предмет выявления установления несанкционированных соединений устройств «интернета вещей» с информационной системой;

3) должен быть реализован контроль за несанкционированными изменениями настроек устройств «интернета вещей»;

4) должно обеспечиваться определение местонахождения устройств «интернета вещей»;

5) должно обеспечиваться блокирование доступа с несанкционированного устройства «интернета вещей» в информационную систему;

6) должны использоваться фильтры сообщений (команд), обеспечивающие передачу от устройств «интернета вещей» (датчиков), а также к устройствам «интернета вещей» (исполнительным механизмам и датчикам) только разрешенных сообщений (команд);

7) должна быть обеспечена безопасность передаваемых данных в вычислительной сети «интернета вещей» с использованием, в соответствии с законодательством Российской Федерации, криптографических методов защиты информации;

8) должен быть обеспечен запрет применения беспроводных каналов связи для передачи информации устройством «интернета вещей»;

9) устройства «интернета вещей» и вычислительной сети устройств «интернета вещей» в целом, используемые в информационных системах в целях выполнения ими своих функций, должны быть изолированы от сетей связи, предназначенных для доступа к сети «Интернет» и (или) иной общедоступной сети связи.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗИВ.2	+	+	+
Усиление ЗИВ.2			

ЗИВ.3 Защита данных

Цель: Предотвращение утечек, несанкционированного изменения или ограничения доступа к данным устройств «интернета вещей».

Требования к реализации: При реализации мер по защите данных устройств «интернета вещей» должны обеспечиваться:

инвентаризация устройств «интернета вещей» с целью выявления неиспользуемых устройств, а также устройств, не предусмотренных к использованию;

возможность подключения только к разрешенным устройствам «интернета вещей» для выполнения установленных функций;

ограничение формата данных (команд), вводимых в устройства «интернета вещей»;

отключение в устройствах «интернета вещей» неиспользуемых средств (протоколов) подключения (коммуникации) между устройствами «интернета вещей» в вычислительной сети устройств «интернета вещей»;

выделение сетей устройств «интернета вещей» в отдельные сегменты информационной системы;

защита данных устройств «интернета вещей» от раскрытия, модификации и навязывания (ввода ложной информации) при их передаче по каналам связи, имеющим выход за пределы контролируемой зоны;

отключение неиспользуемых функциональных возможностей устройств «интернета вещей».

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должно обеспечиваться исключение возможности ввода данных (команд) в устройства «интернета вещей» посредством реализации ограничительных интерфейсов по вводу информации;

2) должен обеспечиваться анализ сетевого трафика сетей устройств «интернета вещей» с целью выявления признаков реализации компьютерных атак.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗИВ.3	+	+	+
Усиление ЗИВ.3		1	1

ЗИВ.4 Контроль целостности

Цель: Обеспечение целостности устройств «интернета вещей».

Требования к реализации: При реализации мер по контролю целостности устройств «интернета вещей» должен обеспечиваться контроль:

целостности аппаратной части компонентов устройств «интернета вещей», а также выявления фактов несанкционированного добавления новых устройств «интернета вещей»;

состава программного обеспечения устройств «интернета вещей», а также выявления фактов несанкционированного добавления нового программного обеспечения устройств «Интернета вещей»;

целостности обновлений программного обеспечения вычислительной сети устройств «интернета вещей»;

целостности файлов, содержащих параметры настройки (конфигурацию) программного обеспечения устройств «интернета вещей».

Должен выполняться анализ уязвимостей прошивок устройств «интернета вещей». В случае выявления уязвимостей должно выполняться обновление версий прошивок устройств «интернета вещей» на версии (при их наличии), не содержащие известные уязвимости.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должен осуществляться контроль целостности микропрограммного обеспечения устройств «интернета вещей» путем верификации сертификата безопасности и (или) контрольных сумм;

2) должен осуществляться еженедельный или с меньшей периодичностью, устанавливаемой в информационной системе, контроль отсутствия несанкционированных изменений в параметрах настройки устройств «интернета вещей»;

3) должны обеспечиваться выявление и блокировка запуска программного обеспечения устройств «интернета вещей», целостность которого нарушена.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗИВ.4	+	+	+
Усиление ЗИВ.4			

ЗИВ.5 Регистрация, анализ и реагирование на события безопасности

Цель: Определение состава и содержания информации о событиях безопасности, подлежащих регистрации в устройствах «интернета вещей».

Требования к реализации: Должна обеспечиваться регистрация событий безопасности в устройствах «интернета вещей» в соответствии с мерами защиты информации РСБ.1 – РСБ.5.

Должен выполняться анализ зарегистрированных событий безопасности, по результатам анализа должно осуществляться реагирование на выявленные

компьютерные инциденты.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) реагирование на выявленные признаки компьютерных инцидентов должно включать отправку уведомлений администратору безопасности информационной системы;

2) должны обеспечиваться блокирование и (или) изоляция устройств «интернета вещей», на которых выявлены компьютерные инциденты.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗИВ.5	+	+	+
Усиление ЗИВ.5		1	1

4.12 Защита точек беспроводного доступа (ЗБД)

ЗБД.1 Идентификация и аутентификация

Цель: Исключение доступа объектов и субъектов беспроводного доступа к информационной системе, не прошедших процедуру идентификации и аутентификации.

Требования к реализации: Должны обеспечиваться:

идентификация и аутентификация пользователей, запрашивающих доступ к беспроводной локальной вычислительной сети (внутренних пользователей, привилегированных пользователей, администраторов), в соответствии с мерами защиты информации ИАФ.1, ИАФ.3;

идентификация устройств, запрашивающих доступ к беспроводной локальной вычислительной сети, в соответствии с мерой защиты информации ИАФ.2;

идентификация точек беспроводного доступа беспроводной локальной вычислительной сети.

Идентификация точек беспроводного доступа должна обеспечиваться по логическим именам (например, символьному названию беспроводной точки доступа SSID), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, MAC-адресам) или по комбинации имени, логического и (или) физического адресов точки беспроводного доступа.

Идентификация устройств при подключении к точкам беспроводного доступа в информационной системе обеспечивается по логическим именам (имя устройства и (или) ID), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, MAC-адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства.

Не допускается осуществлять аутентификацию точек беспроводного доступа с использованием паролей, установленных по умолчанию.

Указанные меры защиты информации реализуются за счет применения в информационной системе средств идентификации и аутентификации, реализованных и (или) применяемых в точках беспроводного доступа, ином оборудовании беспроводной локальной вычислительной сети, устройствах пользователей.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должно обеспечиваться сокрытие имени сети (SSID) в списке доступных сетей;

2) для управления учетными записями и учетными данными субъектов беспроводного доступа в беспроводной локальной вычислительной сети должны использоваться системы (средства) управления учетными записями;

3) символьное название беспроводной точки доступа, служащее для идентификации ее пользователями и устройствами пользователей, точкой доступа не должно транслироваться широковещательно и, соответственно, не должно отражаться в списке видимых точек доступа на устройствах пользователей и иных субъектов доступа;

4) аутентификация устройств при подключении к точкам беспроводного доступа в информационной системе обеспечивается с использованием протоколов аутентификации.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗБД.1	+	+	+
Усиление ЗБД.1			1

ЗБД.2 Управление доступом

Цель: Исключение несанкционированного доступа к точкам беспроводного доступа.

Требования к реализации: Должны обеспечиваться меры по управлению доступом субъектов к точкам беспроводного доступа в информационной системе в соответствии с мерами защиты информации УПД.1 – УПД.9, а также обеспечиваться:

фильтрация устройств пользователей, используемых для беспроводного доступа, (например, по физическим адресам (MAC-адресам) для управления разрешениями по доступу к беспроводной локальной вычислительной сети;

предоставление доступа к параметрам (изменению параметров) настройки

точек беспроводного доступа только администраторам информационной системы;

предоставление доступа к беспроводной локальной вычислительной сети (к точкам беспроводного доступа, хранимой информации, услугам (сервисам) и приложениям) только пользователям, прошедшим идентификацию и аутентификацию.

Указанные меры защиты информации реализуются за счет применения в информационной системе средств управления доступом, реализованных и (или) применяемых в точках беспроводного доступа, ином оборудовании беспроводной локальной вычислительной сети, устройствах пользователей.

При предоставлении пользователям доступа к точкам беспроводного доступа должен применяться принцип наименьших привилегий.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должна быть исключена возможность несанкционированных изменений настроек точек беспроводного доступа;

2) должно обеспечиваться ограничение времени сессии доступа пользователей и автоматическое завершение соединений при превышении заданного времени доступа;

3) должны применяться системы управления беспроводными сетями;

4) должны применяться системы контроля (управления) доступом устройств при подключении к беспроводной локальной вычислительной сети.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗБД.2	+	+	+
Усиление ЗБД.2			

ЗБД.3 Защита пользовательских данных

Цель: Предотвращение утечек, перехвата и модификации пользовательских данных при подключении к точкам беспроводного доступа.

Требования к реализации: При подключении пользователей к точкам беспроводного доступа в информационной системе должны обеспечиваться:

выделение беспроводных локальных вычислительных сетей в отдельные сегменты информационной системы;

инвентаризация точек беспроводного доступа;

подключение только к разрешенным точкам беспроводного доступа для выполнения установленных обязанностей (функций);

обеспечение возможности реализации соединений с точками

беспроводного доступа только через контролируемые интерфейсы точек беспроводного доступа и устройств пользователей (в том числе, путем применения средств защиты информации);

контроль подключения устройств пользователей к точкам беспроводного доступа пользователей в информационной системе до начала информационного взаимодействия с информационной системой.

На точках беспроводного доступа неиспользуемые функциональные возможности должны быть отключены (заблокированы).

Должен выполняться анализ уязвимостей прошивок и программного обеспечения точек беспроводного доступа. В случае выявления уязвимостей должно выполняться обновление версий прошивок и программного обеспечения точек беспроводного доступа (при их наличии) на версии, не содержащие уязвимости.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должен обеспечиваться анализ сетевого трафика сетей беспроводного доступа с целью выявления признаков реализации компьютерных атак;

2) должна проводиться инвентаризация точек беспроводного доступа с целью выявления неиспользуемых устройств, а также устройств, не предусмотренных к использованию;

3) должно обеспечиваться отключение функциональной возможности автоматического подключения устройств пользователей к точкам беспроводного доступа;

4) должен обеспечиваться анализ сетевого трафика беспроводной локальной вычислительной сети с целью выявления несанкционированных подключений;

5) должны применяться механизмы фильтрации (ограничения доступа) при подключении к точкам беспроводного доступа по физическим и (или) логическим адресам.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗБД.3	+	+	+
Усиление ЗБД.3			

ЗБД.4 Контроль целостности

Цель: Обеспечение целостности точек беспроводного доступа.

Требования к реализации: Должны обеспечиваться следующие меры по контролю целостности точек беспроводного доступа в информационной системе:

контроль целостности программного обеспечения точек беспроводного доступа, в том числе версий микропрограммного обеспечения;

контроль состава аппаратных компонентов точек беспроводного доступа;

отключение неиспользуемых интерфейсов;

размещение точек беспроводного доступа в пределах контролируемой зоны;

установка актуальных обновлений для точек беспроводного доступа и устранение уязвимостей, связанных с безопасностью беспроводных соединений.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должен осуществляться еженедельный или с меньшей периодичностью, устанавливаемой в информационной системе, контроль отсутствия несанкционированных изменений в настройках в точках беспроводного доступа;

2) должен осуществляться контроль целостности микропрограммного обеспечения точек беспроводного доступа путем верификации цифровой подписи или контрольных сумм;

3) должно обеспечиваться исключение возможности изменения пользователем подключаемого устройства настроек точек беспроводного доступа;

4) должен обеспечиваться контроль целостности конфигурации и параметров настройки точек беспроводного доступа.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗБД.4	+	+	+
Усиление ЗБД.4			

ЗБД.5 Ограничение уровней сигналов

Цель: Обеспечение невозможности (затруднения) доступа к точкам беспроводного доступа из-за пределов контролируемой зоны.

Требования к реализации: Должны применяться точки беспроводного доступа, имеющие возможность настройки уровня мощности сигнала.

Должно обеспечиваться ограничение уровней сигналов точек беспроводного доступа. Значения уровней сигналов точек беспроводного доступа должны устанавливаться с учетом физических границ информационной системы (сегментов информационной системы) с целью обеспечения минимального уровня сигнала на физических границах.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должен осуществляться мониторинг уровней сигналов точек беспроводного доступа;

2) должна быть составлена карта покрытия сигналами точек беспроводного доступа помещений информационной системы (сегментов информационной системы), размещение точек беспроводного доступа и уровень мощности их сигналов должны быть определены с учетом карты покрытия;

3) должна осуществляться фильтрация частотного диапазона передачи данных точки беспроводного доступа для исключения несанкционированного доступа к информации, передаваемой по беспроводному каналу.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗБД.5	+	+	+
Усиление ЗБД.5			

ЗБД.6 Регистрация, анализ и реагирование на события безопасности

Цель: Определение состава и содержания информации о событиях безопасности, подлежащих регистрации в беспроводных локальных вычислительных сетях.

Требования к реализации: Должна обеспечиваться регистрация событий безопасности в сетях беспроводного доступа в соответствии с мерами защиты информации РСБ.1 – РСБ.5.

Должен выполняться анализ зарегистрированных событий безопасности, по результатам анализа должно осуществляться реагирование на выявленные компьютерные инциденты.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) реагирование на выявленные признаки компьютерных инцидентов должно включать отправку уведомлений администратору безопасности информационной системы;

2) должны обеспечиваться блокирование и (или) изоляция точек беспроводного доступа, на которых выявлены компьютерные инциденты.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗБД.6	+	+	+
Усиление ЗБД.6		1	1

4.13. Антивирусная защита (АВЗ)

АВЗ.1 Антивирусная защита устройств

Цель: Обеспечение антивирусной защиты информационной системы на устройствах, включающее:

обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, сокрытия присутствия другого вредоносного программного обеспечения в информационной системе, сокрытия свидетельств несанкционированного доступа к любым ресурсам информационной системы;

обеспечение реагирования на обнаружение вредоносного программного обеспечения.

Требования к реализации: Реализация антивирусной защиты устройств должна предусматривать:

определение физических и виртуальных устройств, входящих в состав информационной системы, на которых необходимо применение средств антивирусной защиты;

установку, конфигурирование и управление средствами антивирусной защиты;

предоставление прав доступа средствам антивирусной защиты к объектам информационной системы, которые должны быть подвергнуты проверке средством антивирусной защиты;

настройку средств антивирусной защиты, обеспечивающую проведение периодических проверок устройств на наличие вредоносного программного обеспечения;

настройку средств антивирусной защиты на устройствах информационной системы, через которые в нее может быть внедрено вредоносное программное обеспечение, обеспечивающую проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных

носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников);

выявление вредоносного программного обеспечения и реагирование на его обнаружение на устройствах и серверах средством антивирусной защиты при подключении съемных машинных носителей информации, а также периодически или по команде в процессе функционирования устройств и серверов в соответствии с эксплуатационной документацией;

определение и выполнение действий по реагированию на обнаружение в информационной системе объектов, подвергшихся заражению вредоносным программным обеспечением;

обновление баз данных признаков вредоносных компьютерных программ (вирусов) в соответствии с информацией, поступающей от разработчика средства антивирусной защиты, в порядке, установленном в эксплуатационной документации;

проверку устройств на наличие вредоносного программного обеспечения после обновления баз данных признаков вредоносных компьютерных программ (вирусов).

Указанные меры защиты информации реализуются за счет применения средств антивирусной защиты.

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены:

порядок учета устройств, на которых необходимо применение средств антивирусной защиты;

порядок и правила проведения периодических проверок устройств и серверов на наличие компьютерных вирусов;

действия по реагированию на обнаружение в информационной системе объектов, подвергшихся заражению вредоносным программным обеспечением;

порядок и правила обновления баз данных признаков вредоносных компьютерных программ (вирусов).

Требования к усилению:

1) в информационной системе должно обеспечиваться выявление вредоносного программного обеспечения и реагирование на его обнаружение на устройствах средством антивирусной защиты до загрузки операционных систем;

2) в информационной системе должно обеспечиваться централизованное управление антивирусной защитой за счет применения средств, обеспечивающих централизованное управление средствами антивирусной защиты;

3) в информационной системе должна обеспечиваться настройка средств антивирусной защиты на устройствах информационной системы, через которые в нее может быть внедрено вредоносное программное обеспечение,

обеспечивающая проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников при загрузке, открытии или исполнении таких файлов.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
АВЗ.1	+	+	+
Усиление АВЗ.1			

АВЗ.2 Антивирусная защита электронной почты

Цель: Обеспечение антивирусной защиты электронной почты, включающее:

обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, сокрытия присутствия другого вредоносного программного обеспечения в информационной системе, сокрытия свидетельств несанкционированного доступа к любым ресурсам информационной системы;

обеспечение реагирования на обнаружение вредоносного программного обеспечения.

Требования к реализации: Реализация антивирусной защиты электронной почты должна предусматривать:

обнаружение в сообщениях электронной почты вредоносного программного обеспечения;

реагирование на обнаружение угроз безопасности информации путем блокирования (удаления) вредоносного программного обеспечения из сообщений электронной почты, информирования об обнаруженных угрозах безопасности информации, оповещения о выполненных действиях (удалении сообщений электронной почты или вложений, помещении в карантин).

Указанные меры защиты информации реализуются за счет применения средств антивирусной защиты электронной почты.

Требования к документированию: В эксплуатационной документации на информационную систему должен быть определен порядок осуществления антивирусной защиты электронной почты.

Требования к усилению:

1) в информационной системе должно обеспечиваться обнаружение компьютерных вирусов во вложениях сообщений электронной почты, содержащих данные, инкапсулированные в преобразованном (кодированном)

виде, и архивированные файлы.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
АВЗ.2	+	+	+
Усиление АВЗ.2			

АВЗ.3 Антивирусная проверка сетевого трафика

Цель: Обеспечение антивирусной защиты сетевого трафика, включающее:

обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, сокрытия присутствия другого вредоносного программного обеспечения в информационной системе, сокрытия свидетельств несанкционированного доступа к любым ресурсам информационной системы;

обеспечение реагирования на обнаружение вредоносного программного обеспечения.

Требования к реализации: Реализация антивирусной защиты сетевого трафика должна предусматривать:

антивирусную проверку файлов, извлекаемых из сетевого трафика;

анализ файлов, извлекаемых из сетевого трафика, на предмет наличия вредоносного программного обеспечения в масштабе времени, близком к реальному;

анализ файлов, извлекаемых из сетевого трафика, на предмет наличия вредоносного программного обеспечения с использованием сигнатурного метода обнаружения, хэш-сумм и других индикаторов;

реагирование по результатам антивирусной проверки файлов, извлекаемых из сетевого трафика, в соответствии с порядком, установленным в эксплуатационной документации.

Указанные меры защиты информации реализуются за счет применения средств антивирусной защиты и (или) многофункциональных межсетевых экранов уровня сети, и (или) иных средств защиты информации.

Требования к документированию: В эксплуатационной документации на информационную систему должен быть определен порядок осуществления антивирусной защиты сетевого трафика.

Требования к усилению:

1) в информационной системе должен обеспечиваться анализ файлов, извлекаемых из сетевого трафика, на предмет наличия вредоносного программного обеспечения с использованием эвристических методов обнаружения;

2) в информационной системе должен обеспечиваться анализ файлов, извлекаемых из сетевого трафика, на предмет наличия вредоносного программного обеспечения на прикладном уровне для установленных в эксплуатационной документации приложений (веб-приложений, клиентов файловых хранилищ, мессенджеров и иных приложений);

3) в информационной системе должен осуществляться анализ извлекаемых из сетевых пакетов данных, инкапсулированных в преобразованном (кодированном) виде, на предмет наличия вредоносного программного обеспечения.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
АВЗ.3	+	+	+
Усиление АВЗ.3			

АВЗ.4 Применение замкнутой системы (среды) предварительного выполнения программ («песочницы»)

Цель: Выявление в информационной системе вредоносного программного обеспечения путем запуска потенциально вредоносных объектов в замкнутой программной среде исполнения («песочнице») и анализа поведения указанных объектов.

Требования к реализации: В случае выявления в информационной системе потенциального вредоносного объекта контроля и (или) потенциального вредоносного поведения объекта контроля должны обеспечиваться:

возможность передачи копии потенциально вредоносного объекта в замкнутую систему (среду) предварительного выполнения программ («песочницу») в целях его динамического анализа;

динамический анализ потенциально вредоносного объекта в замкнутой системе (среде) предварительного выполнения программ («песочнице»);

получение результатов динамического анализа потенциально вредоносного объекта в замкнутой системе (среде) предварительного выполнения программ («песочнице»).

Требования к документированию: Не предъявляются.

Требования к усилению:

1) в информационной системе должна применяться замкнутая система (среда) предварительного выполнения программ («песочница»), позволяющая обеспечивать возможность имитации пользовательских действий с подозрительными объектами;

2) в информационной системе должна применяться замкнутая система (среда) предварительного выполнения программ («песочница»), обеспечивающая возможность загрузки образов виртуальных машин, входящих в состав информационной системы.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
АВЗ.4			
Усиление АВЗ.4			

4.14. Обнаружение и предотвращение вторжений на сетевом уровне (СОВ)

СОВ.1 Обнаружение и предотвращение вторжений на периметре

Цель: Обнаружение и предотвращение вторжений (компьютерных атак) со стороны внешних нарушителей на периметре информационных систем.

Требования к реализации: При обнаружении и предотвращении вторжений на периметре должны обеспечиваться:

получение сетевого трафика (копии сетевого трафика) для анализа;

обнаружение (предотвращение) вторжений (компьютерных атак) на периметре информационной системы;

реагирование на компьютерные атаки (например, уведомление администратора безопасности, блокирование трафика) в соответствии с эксплуатационной документацией;

автоматизированное получение и обновление баз решающих правил и индикаторов атак средств защиты информации с ресурсов разработчика средства и (или) с настраиваемых локальных ресурсов по расписанию и (или) по требованию.

Указанные меры защиты информации реализуются за счет применения систем обнаружения вторжений уровня сети, и (или) многофункциональных межсетевых экранов уровня сети, и (или) иных средств защиты информации.

Требования к документированию: В эксплуатационной документации на информационную систему должен быть определен порядок обнаружения и предотвращения вторжений на периметре.

Требования к усилению:

1) в информационной системе должны разрабатываться (модернизироваться) решающие правила с целью предотвращения компьютерных атак, специфичных для информационной системы, а также новых компьютерных атак, информация о которых была получена из открытых или иных источников;

2) должно осуществляться обнаружение вторжений на прикладном уровне;

3) должна обеспечиваться возможность анализа извлекаемых из сетевых пакетов данных, инкапсулированных в преобразованном (кодированном) виде, на предмет обнаружения вторжений (компьютерных атак);

3) должна обеспечиваться возможность хранения фрагментов собранного сетевого трафика;

5) должна обеспечиваться возможность ретроспективного анализа сетевого трафика;

6) должна обеспечиваться возможность выявления аномалий сетевого трафика;

7) должна обеспечиваться возможность анализа вложений и объектов, извлекаемых из сетевого трафика (исполняемых файлов, ссылок, архивов и других объектов), с возможностью их передачи в замкнутую программную среду исполнения («песочницу») для динамического анализа в автоматическом режиме;

8) должны применяться средства защиты информации, обладающие комплексными функциональными возможностями по обнаружению вторжений, анализу сетевого трафика на предмет наличия вредоносного программного обеспечения, в том числе с использованием замкнутой программной среды исполнения («песочницы»);

9) должно обеспечиваться использование репутационной базы угроз для проверки сетевых и прикладных артефактов (IP-адресов, доменов, URL) в масштабе, близком к реальному времени;

10) должны применяться пассивные (энергонезависимые) технические средства однонаправленного ответвления сетевого трафика для получения копии сетевого трафика системами обнаружения вторжений уровня сети для анализа.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
СОВ.1	+	+	+
Усиление СОВ.1		1	1

СОВ.2 Обнаружение и предотвращение вторжений в сегментах информационной системы

Цель: Обнаружение и предотвращение вторжений (компьютерных атак) со стороны внешних и внутренних нарушителей в сегментах информационной системы.

Требования к реализации: Должно обеспечиваться обнаружение (предотвращение) вторжений (компьютерных атак) в сегментах (на границах сегментов) информационной системы.

В качестве таких сегментов рассматриваются:

сетевые сегменты (например, внутренняя сеть информационной системы, сеть гостевого доступа);

функциональные сегменты (например, сеть для обработки финансовых данных, сеть для пользовательских интерфейсов);

сегменты с различным уровнем значимости информации;

сегменты с различными классами защищенности;

сегменты с различными типами устройств (например, автоматизированные рабочие места, серверы, телекоммуникационное оборудование).

Должен обеспечиваться анализ сетевого трафика между сегментами на наличие вторжений (компьютерных атак).

Должно обеспечиваться автоматизированное получение и обновление баз решающих правил и индикаторов атак средств защиты информации с ресурсов разработчика средства и (или) с настраиваемых локальных ресурсов по расписанию и (или) по требованию.

Указанные меры защиты информации реализуются за счет применения систем обнаружения вторжений уровня сети, и (или) многофункциональных межсетевых экранов уровня сети, и (или) иных средств защиты информации.

Требования к документированию: В эксплуатационной документации на информационную систему должен быть определен порядок обнаружения и предотвращения вторжений (компьютерных атак) в сегментах информационной системы.

Требования к усилению:

1) должно обеспечиваться блокирование сетевого трафика или изоляция сегмента, в котором обнаружены компьютерные атаки;

2) должно обеспечиваться централизованное управление (администрирование) компонентами системы обнаружения вторжений, установленными в различных сегментах информационной системы.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
СОВ.2	+	+	+
Усиление СОВ.2			

4.15. Сегментация и межсетевое экранирование (МСЭ)

МСЭ.1. Сегментация сети

Цель: Обеспечение изоляции сегментов информационной системы друг от друга.

Требования к реализации: В информационной системе должна быть реализована сегментация информационной системы. Сегментация информационной системы проводится путем выделения:

сетевых сегментов (например, внутренняя сеть информационной системы, сеть гостевого доступа);

функциональных сегментов (например, сеть для обработки финансовых данных, сеть для пользовательских интерфейсов);

сегментов с различным уровнем значимости информации;

сегментов с различными классами защищенности;

сегментов с различными типами устройств (например, автоматизированные рабочие места, серверы, телекоммуникационное оборудование);

сегментов виртуальной среды;

сегментов контейнерной среды.

При сегментации информационной системы должны обеспечиваться контроль и фильтрация сетевого трафика на границах сегментов.

При сегментации информационной системы должна проводиться проверка корректности сегментации информационной системы в соответствии с эксплуатационной документацией, но не реже одного раза в год.

Должен быть обеспечен принцип минимальных привилегий при взаимодействии между сегментами, при предоставлении доступа субъектов доступа в сегменты информационной системы.

Указанные меры защиты информации реализуются за счет применения в информационной системе межсетевых экранов, и (или) многофункциональных межсетевых экранов уровня сети, и (или) средств однонаправленной передачи информации, а также (при необходимости) за счет физической изоляции отдельных сегментов информационной системы, определяемых оператором.

Требования к документированию: В эксплуатационной документации

на информационную систему должен быть определен порядок сегментации информационной системы.

Требования к усилению:

1) должна быть реализована микросегментация на уровне сегментов информационной системы, обеспечивающая их разделение на изолированные сегменты;

2) должна быть реализована возможность предоставления доступа внешних пользователей к приложениям (сервисам) информационной системы без предоставления доступа к иным сегментам информационной системы;

3) должна быть реализована автоматизация управления правилами фильтрации в сегментах информационной системы для обеспечения согласованности правил на различных межсетевых экранах;

4) должны централизовано регистрироваться события блокировки попыток доступа в обход определяемых оператором правил межсетевого экранирования с применением средств мониторинга информационной безопасности.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
МСЭ.1	+	+	+
Усиление МСЭ.1			1

МСЭ.2. Организация демилитаризованной зоны

Цель: Создание контролируемого буферного сегмента информационной системы для безопасного взаимодействия с внешними информационными системами и сетями.

Требования к реализации: В информационной системе должна быть реализована демилитаризованная зона для размещения компонентов информационной системы, обеспечивающих взаимодействие с внешними информационными системами и сетями, включая сеть «Интернет».

Демилитаризованная зона должна быть изолирована от внутренних сегментов информационной системы, обрабатывающих информацию ограниченного доступа, с применением межсетевых экранов, и (или) многофункциональных межсетевых экранов уровня сети, и (или) средств однонаправленной передачи информации.

Все сетевые соединения между демилитаризованной зоной, внешними информационными системами, сетями и внутренними сегментами должны проходить через средства межсетевого экранирования и (или) многофункциональные межсетевые экраны уровня сети.

Требования к документированию: В эксплуатационной документации на информационную систему должен быть определен порядок организации демилитаризованной зоны.

Требования к усилению:

1) должна обеспечиваться защита компонентов информационной системы, находящихся в демилитаризованной зоне, с применением средств межсетевого экранирования уровня веб-сервера;

2) должны использоваться обратные прокси-серверы для организации доступа к компонентам информационной системы, находящимся в демилитаризованной зоне;

3) аппаратная платформа средств защиты информации (в том числе многофункциональных межсетевых экранов уровня сети), используемых в демилитаризованной зоне для безопасного взаимодействия с внешними информационными системами и сетями, должна ограничивать доступ через сетевые интерфейсы к оперативной памяти указанных средств защиты информации только в разрешенном диапазоне адресов и исключать возможность доступа (как на чтение, так и на запись) к остальной части оперативной памяти со стороны сетевого интерфейса.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
МСЭ.2	+	+	+
Усиление МСЭ.2			

МСЭ.3. Контроль сетевого доступа и фильтрация трафика

Цель: Обеспечение безопасного сетевого взаимодействия между сегментами информационной системы, а также внешними информационными системами и сетями.

Требования к реализации: В информационной системе должен быть реализован контроль сетевого доступа и фильтрация всего трафика на границах между сегментами информационной системы, а также на границе с внешними информационными системами и сетями, включая сеть «Интернет».

Контроль должен осуществляться с применением правил фильтрации трафика, разработанных с учетом актуальных угроз, и (или) с применением средств однонаправленной передачи информации.

В информационной системе должны быть определены правила контроля и фильтрации сетевого трафика. Фильтрации подлежат входящие и исходящие сетевые соединения. В информационной системе должны регистрироваться события безопасности, связанные с нарушением правил сетевого

взаимодействия, определяемых оператором.

Должно обеспечиваться резервное копирование перечня правил межсетевого экранирования

Указанные меры защиты информации реализуются за счет применения в информационной системе межсетевых экранов, и (или) многофункциональных межсетевых экранов уровня сети, и (или) средств однонаправленной передачи информации, а также (при необходимости) за счет физической изоляции отдельных сегментов информационной системы, определяемых оператором.

Требования к документированию: В эксплуатационной документации на информационную систему должен быть определен порядок контроля и фильтрации сетевого трафика.

Требования к усилению:

1) на аппаратном уровне должна быть реализована пакетная фильтрация на основе физических и (или) сетевых адресов отправителей, и (или) получателей сетевого трафика с применением межсетевых экранов, и (или) многофункциональных межсетевых экранов уровня сети.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
МСЭ.3	+	+	+
Усиление МСЭ.3			

МСЭ.4. Маскирование системы

Цель: Затруднение проведения анализа информационной системы и получения сведений о ее конфигурации и особенностях функционирования внешними нарушителями безопасности информации.

Требования к реализации: В информационной системе должны быть определены компоненты информационной системы, расположенные на границе с внешними системами и сетями, включая сеть «Интернет», подлежащие маскированию.

При маскировании должна быть исключена возможность несанкционированного определения сетевых адресов, наименований узлов, типов и версий программного обеспечения информационной системы.

Ответы на сетевые запросы к компонентам информационной системы, подлежащим маскированию, не должны раскрывать сведения о информационной системе (например, сетевых адресов, наименований узлов, типов и версий программного обеспечения).

Реализация маскирования не должна нарушать штатные процессы функционирования информационной системы.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должны применяться технологии сокрытия сетевых адресов сервисов для управления доступом к административным сервисам;

2) должны использоваться системы замедления сетевого сканирования;

3) должно быть обеспечено игнорирование запросов с внешних источников;

4) должны применяться средства маскирования атрибутов сетевого трафика для затруднения анализа.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
МСЭ.4			
Усиление МСЭ.4			

МСЭ.5. Создание ложных систем

Цель: Выявление попыток несанкционированного доступа нарушителей в информационной системе с использованием специально созданных (эмулированных) ложных информационных систем и (или) их компонентов.

Требования к реализации: В информационной системе должны применяться специально созданные (эмулированные) ложные информационные системы и (или) ложные компоненты информационной системы, предназначенные для обнаружения, регистрации и анализа действий нарушителей безопасности информации в процессе реализации угроз безопасности информации.

Ложные информационные системы или их компоненты должны:

имитировать функционирование реальной информационной системы или ее компонентов (сегментов);

обнаруживать и регистрировать действия нарушителей безопасности информации по реализации компьютерной атаки;

передавать собранную информацию в системы мониторинга информационной безопасности.

Ложные информационные системы должны быть изолированы от информационной системы, обладать признаками функционирующих сервисов и не должны содержать информацию ограниченного доступа.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) на компонентах информационной системы должны создаваться ложные данные. Например, могут создаваться следующие типы ложных данных:

формат текстовых файлов и таблиц doc, docx, odt, xls, xlsx;

ложные данные, размещаемые в системных компонентах операционных систем;

ложные данные, размещаемые в прикладном программном обеспечении операционных систем;

2) ложные информационные системы или их компоненты должны предоставлять возможность однозначного определения их как существующей информационной системы, без возможности определения компонента как элемента информационной системы.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
МСЭ.5			
Усиление МСЭ.5			

4.16. Защита от компьютерных атак, направленных на отказ в обслуживании (ЗОО)

ЗОО.1 Защита от компьютерных атак, направленных на отказ в обслуживании, при доступе внешних пользователей к прикладным сервисам, предоставляемым информационной системой

Цель: Обеспечение доступности информационной системы, в том числе входящих ее состав объектов защиты информации (прикладных сервисов, сетевых сервисов) при реализации нарушителем компьютерных атак, направленных на отказ в обслуживании.

Требования к реализации: В информационной системе должны быть реализованы следующие меры:

серверы, обеспечивающие и предоставляющие прикладные сервисы информационной системы внешним пользователям информационной системы, должны размещаться в демилитаризованной зоне, соответствующей мере защиты информации МСЭ.2;

на границе демилитаризованной зоны или до поступления в демилитаризованную зону сетевой трафик из внешней сети должен подвергаться фильтрации и очистке от составляющих, связанных с компьютерными атаками, направленными на отказ в обслуживании, с использованием средств защиты информации от воздействий, направленных на

отказ в обслуживании информационных (автоматизированных) на стороне оператора информационной системы, и (или) на стороне провайдера, и (или) организации, предоставляющей услуги связи, и (или) организации, оказывающей услуги по контролю, фильтрации и блокированию сетевых запросов, обладающих признаками компьютерных атак, направленных на отказ в обслуживании.

Требования к документированию: Не предъявляются.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗОО.1	+	+	+
Усиление ЗОО.1			

ЗОО.2 Контроль и фильтрация входящего трафика

Цель: Исключение нелегитимных потоков входящего трафика сервисов информационной системы.

Требования к реализации: При реализации контроля и фильтрации входящего трафика в информационной системе должно быть обеспечено:

применение правил фильтрации входящего трафика в момент после обнаружения компьютерной атаки, направленной на отказ в обслуживании;

применение правил фильтрации входящего трафика на сетевом и транспортном уровнях информационных систем;

применение правил фильтрации на основе матрицы коммуникаций информационных систем с сетью «Интернет» на транспортном уровне информационных систем и поддержание ее в актуальном состоянии;

определение сетевых адресов, с которыми должно быть обеспечено взаимодействие информационной системы, и применение списков разрешенных сетевых адресов;

фильтрация данных информационной системы за счет определения страновой принадлежности сетевых адресов центра мониторинга и управления сетями связи общего пользования (GeoIP) путем исключения трафика, не относящегося к IP-адресам Российской Федерации, в условиях реализации компьютерных атак, направленных на отказ в обслуживании, при которых не удается обеспечить должный уровень фильтрации (обеспечить доступность информационной системы) на основе матрицы коммуникаций информационных систем.

Для защиты информационных систем и фильтрации трафика компьютерных атак, направленных на отказ в обслуживании, на прикладном

уровне в том числе должны использоваться специализированные программные, программно-аппаратные средства и (или) услуги провайдеров хостинга или организаций, предоставляющих услуги связи, и (или) организаций, оказывающих услуги по контролю, фильтрации и блокированию входящего трафика, способных работать на прикладном уровне информационных систем.

Требования к документированию: В эксплуатационной документации на систему защиты информации должны быть определены:

перечень интерфейсов и сервисов информационных систем, которые должны быть постоянно доступны из сети «Интернет» и подлежат защите от компьютерных атак, направленных на отказ в обслуживании;

состав подразделений (работников), участвующих в предоставлении (открытии) доступа пользователям из сети «Интернет» интерфейсов и сервисов информационных систем, подлежащих защите от компьютерных атак, направленных на отказ в обслуживании, их функции и полномочия, порядок взаимодействия при проведении мероприятий;

требование о хранении в течении трех лет информации о фактах реализации компьютерных атак, направленных на отказ в обслуживании: дата и время начала и окончания реализации атак, тип атаки (на сетевом, транспортном и прикладном уровнях), объем (Гбит/с, сетевых пакетов/с, в случае атак прикладного уровня - запросов в секунду), перечень сетевых адресов, являющихся источником атак (за исключением случаев подмены IP-адресов), и сетевых адресов, подверженных атакам.

Требования к усилению:

1) в информационной системе должно быть обеспечено применение правил фильтрации входящего трафика на постоянной основе;

2) в информационной системе должно быть обеспечено наличие возможности анализа TLS-трафика путем его раскрытия или информации о нем, получаемой в виде журналов событий доступа к объектам информационной системы.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗОО.2	+	+	+
Усиление ЗОО.2			1

ЗОО.3 Мониторинг состояния сервисов и интерфейсов

Цель: Обеспечение непрерывного контроля состояния доступности информационных систем и ключевых показателей производительности сервисов и средств, используемых для защиты от компьютерных атак, направленных

на отказ в обслуживании.

Требования к реализации: При выполнении мониторинга состояния сервисов и интерфейсов в информационной системе должен быть обеспечен мониторинг:

показателей загрузки центрального процессора, оперативной памяти, сетевых интерфейсов (бит/с и пакетов/с) серверов, виртуальных машин, сетевого оборудования, а также находящихся на периметре средств защиты информации;

показателей количества одновременно установленных сетевых соединений для средств (балансировщиков нагрузки, межсетевых экранов уровня сети, межсетевых экранов уровня веб-сервера и других средств), реализующих сетевые функции с контролем состояния соединений;

количества запросов на прикладном уровне информационных систем для средств и сервисов, функционирующих на прикладном уровне;

количества и типов ошибок, отдаваемых в ответах приложениями и сервисами информационной системы.

В информационной системе должна быть обеспечена непрерывность регистрации событий о недоступности сервисов и интерфейсов информационной системы.

Требования к документированию: В эксплуатационной документации на информационную систему должны быть определены:

ключевые показатели производительности сервисов и средств, используемых для мониторинга;

порядок реагирования на события, связанные с недоступностью сервисов и интерфейсов информационной системы.

Требования к усилению:

1) в случае использования услуг провайдеров хостинга, и (или) организаций, предоставляющих услуги связи, и (или) организаций, оказывающих услуги по контролю, фильтрации и блокированию входящего трафика, в информационной системе должен быть обеспечен мониторинг состояния основных метрик работы сервиса и его эффективности;

2) в информационной системе должен быть обеспечен мониторинг доступности информационной системы на прикладном уровне информационных систем, используя инструменты контроля, расположенные в сети «Интернет».

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗОО.3	+	+	+
Усиление ЗОО.3			

ЗОО.4 Балансировка нагрузки

Цель: Повышение уровня отказоустойчивости сервисов информационной системы в условиях реализации компьютерных атак, направленных на отказ в обслуживании.

Требования к реализации: При обеспечении балансировки нагрузки в информационной системе необходимо обеспечить подключение информационной системы по независимым физическим каналам связи к нескольким провайдерам услуги доступа к сети «Интернет» и обеспечить возможность одновременного приема входящего трафика по нескольким каналам.

В случае использования услуг провайдеров хостинга, и (или) организаций, предоставляющих услуги связи, и (или) организаций, оказывающих услуги по контролю, фильтрации и блокированию входящего трафика, в информационной системе необходимо обеспечить выбор провайдера, удовлетворяющего указанному выше требованию.

В информационной системе должна быть обеспечена возможность вертикального масштабирования прикладных сервисов информационной системы в условиях реализации компьютерных атак, направленных на отказ в обслуживании.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) в информационной системе должна быть обеспечена возможность горизонтального масштабирования прикладных сервисов информационной системы и распределения нагрузки между узлами в условиях реализации компьютерных атак, направленных на отказ в обслуживании;

2) в информационной системе должна быть обеспечена возможность распределения нагрузки одновременно по двум географически распределенным площадкам, в которых располагается информационная система при условии, что информационная инфраструктура информационной системы предполагает такой принцип работы.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗОО.4			
Усиление ЗОО.4			

ЗОО.5 Ограничение нагрузки

Цель: Ограничение возможности создания условий для исчерпания ресурсов информационной системы.

Требования к реализации: При реализации меры по ограничению нагрузки в информационной системе необходимо установить ограничение:

по максимальному числу одновременно установленных TCP-соединений с одного IP-адреса (максимальное число соединений определяется по методике и исходным данным оператора для различных типов прикладных сервисов, типов пользователей и (или) API-клиентов);

по скорости ответа от системы доменных имен (DNS-сервера);

по максимальному числу одновременно выполняемых запросов в секунду на прикладном уровне с одного IP-адреса (максимальное число запросов определяется по методике и исходным данным оператора для запросов, поступающих от веб-интерфейсов, мобильных приложений, API-интерфейсов, интерфейсов администрирования).

При реализации меры по ограничению скорости в информационной системе необходимо обеспечить мониторинг трафика в информационной системе и выявление аномального поведения.

Требования к документированию: Не предъявляются.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗОО.5	+	+	+
Усиление ЗОО.5			

ЗОО.6 Поддержка резерва достаточной пропускной способности и расширение ресурсов при сбоях

Цель: Обеспечение резерва ресурсов пропускной способности, позволяющего обрабатывать входящий трафик в условиях реализации компьютерных атак, направленных на отказ в обслуживании.

Требования к реализации: В информационной системе должны быть обеспечены не менее чем:

двукратный резерв полосы пропускания на каналах провайдера услуг доступа к сети «Интернет» (резерв определяется по методике и исходным данным оператора);

двукратный резерв по возможности обработки трафика на определяемых оператором элементах информационной системы (резерв определяется по методике и исходным данным оператора).

Требования к документированию: Не предъявляются.

Требования к усилению:

1) двукратный резерв полосы пропускания внутри информационной системы

на всем пути следования трафика от точки сопряжения с сетью «Интернет» до прикладного сервиса. Резерв рассчитывается от пика полосы легитимного трафика в условиях реализации компьютерных атак, направленных на отказ в обслуживании;

2) должны использоваться доверенные аппаратные средства сетевого взаимодействия, в том числе встроенные в средства, используемые для защиты от компьютерных атак, направленных на отказ в обслуживании, поддерживающие технологии высокопроизводительной обработки сетевых пакетов, позволяющие преодолеть ограничения производительности обработки сетевых пакетов стандартным сетевым стеком ядра операционной системы (например, DPDK, XDP, PF_RING или иные).

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗОО.6		+	+
Усиление ЗОО.6			

4.17. Защита каналов связи и сетевого взаимодействия (ЗКС)

ЗКС.1. Защита данных при передаче по каналам связи

Цель: Обеспечение конфиденциальности и целостности информации при передаче по каналам связи за пределы контролируемой зоны.

Требования к реализации: При передаче информации по каналам связи, выходящим за пределы контролируемой зоны, должна обеспечиваться:

защита передачи информации ограниченного доступа;

защита удаленного доступа пользователей к информационной системе;

защита сетевого взаимодействия пользователей, приложений, сетевых сервисов, находящихся в разных сегментах информационной системы с учетом мер защиты информации МСЭ.1, МСЭ.3;

защита сетевого взаимодействия пользователей, приложений, сетевых сервисов информационной системы с другими информационными системами с учетом мер защиты информации МСЭ.2, МСЭ.3.

В информационной системе должна быть обеспечена защита каналов передачи данных, выходящих за пределы контролируемой зоны, которая включает:

контроль всех сетевых взаимодействий на портах и интерфейсах приложений и сетевых сервисов, доступных из сети «Интернет»;

формирование и поддержание в актуальном состоянии правил межсетевого экранирования с учетом меры защиты информации МСЭ.3;

ограничение доступа пользователей, приложений и сетевых сервисов к неиспользуемым портам, сетевым службам и сервисам;

отключение небезопасных версий протоколов и сетевых служб.

Реализация указанной меры защиты информации обеспечивается за счет применения межсетевых экранов, и (или) многофункциональных межсетевых экранов уровня сети, и (или) средств однонаправленной передачи информации, а также с использованием шифровальных (криптографических) средств защиты информации в соответствии с законодательством Российской Федерации.

Требования к документированию: В эксплуатационной документации на информационную систему должен быть определен перечень внешних информационных систем, приложений и сервисов.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКС.1	+	+	+
Усиление ЗКС.1			

ЗКС.2. Контроль атрибутов безопасности при сетевом взаимодействии

Цель: Обеспечение доверенного сетевого взаимодействия на основе контроля уникальных признаков (атрибутов безопасности) субъектов доступа.

Требования к реализации: В информационной системе должен быть определен перечень атрибутов безопасности, в соответствии с которыми осуществляется контроль информации, получаемой и передаваемой за пределы контролируемой зоны. Атрибуты безопасности должны включать характеристики, позволяющие однозначно идентифицировать субъект доступа.

В информационной системе должны быть обеспечены:

формирование перечня атрибутов безопасности отправителей и получателей, включающих атрибуты сетевых соединений;

проверка соответствия атрибутов безопасности отправителя, получателя перед разрешением передачи данных;

проверка соответствия атрибутов безопасности отправителя, получателя перед приемом данных;

применение правил межсетевого экранирования на межсетевых экранах, учитывающих атрибуты безопасности с учетом меры защиты информации МСЭ.3.

Операции с атрибутами должны регистрироваться с учетом мер защиты информации РСБ.1 – РСБ.5.

Реализация указанных мер защиты информации обеспечивается за счет

применения межсетевых экранов и (или) многофункциональных межсетевых экранов.

Требования к документированию: Не предъявляются.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКС.2	+	+	+
Усиление ЗКС.2			

ЗКС.3. Контроль доступа к внешним ресурсам

Цель: Исключение несанкционированного доступа внутренних пользователей к внешним информационным ресурсам (системам).

Требования к реализации: В информационной системе должны быть:

сформирован и поддерживаться в актуальном состоянии список внешних ресурсов, необходимых для выполнения функциональных задач (список разрешенных и (или) запрещенных ресурсов);

реализован контроль доступа пользователей, приложений и сетевых сервисов информационной системы к ресурсам внешних сетей, включая сеть «Интернет», в соответствии со списком разрешенных и (или) запрещенных ресурсов;

заблокированы попытки доступа к неразрешенным ресурсам внешних сетей, включая сеть «Интернет»;

определен список разрешенных в информационной системе используемых сетевых протоколов, сетевых приложений и сервисов.

Требования к документированию: В эксплуатационной документации на систему защиты информации должен быть определен порядок ведения списка разрешенных и (или) запрещенных ресурсов.

Требования к усилению:

1) должен проводиться морфологический анализ запрашиваемых веб-ресурсов перед их открытием;

2) должна использоваться категоризация веб-ресурсов.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКС.3	+	+	+
Усиление ЗКС.3			

ЗКС.4. Контекстная проверка исходящего трафика

Цель: Предотвращение утечки информации ограниченного доступа и выявление несанкционированного обмена данными путем анализа исходящего сетевого трафика.

Требования к реализации: В информационной системе должна быть реализована контекстная проверка исходящего сетевого трафика, направляемого за пределы контролируемой зоны, включая сеть «Интернет».

Проверка должна включать:

анализ содержания, метаданных и поведенческих характеристик передаваемых данных;

выявление аномальной активности в сетевом трафике.

Должны быть определены и контролироваться сетевые порты, приложения и сервисы, используемые для передачи данных за пределы контролируемой зоны, включая сеть «Интернет».

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должны применяться системы глубокого анализа пакетов для выявления аномалий в сетевом трафике;

2) должны использоваться механизмы поведенческого анализа активности пользователей;

3) должны использоваться специализированные компоненты (агенты) на конечных устройствах пользователей с целью анализа исходящего трафика;

4) должны реализовываться механизмы выявления и блокировки попыток маскировки данных;

5) должны использоваться системы контроля использования облачных сервисов;

6) должны внедряться механизмы классификации данных на основе анализа содержимого.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКС.4			
Усиление ЗКС.4			

Приложение № 1
к методическому документу

Термины и определения, применяемые для целей настоящего методического документа

Атрибутный метод управления доступом – метод, предусматривающий управление доступом субъектов доступа к объектам доступа на основе совокупности атрибутов, присущих субъектам, объектам и контексту доступа. Атрибутами субъекта могут являться должность, роль, подразделение, уровень доверия, статус аутентификации, используемое устройство, местоположение и иные характеристики; атрибутами объекта – метки безопасности, категория данных, тип информации, уровень критичности; атрибутами окружения (контекста) – время суток, канал/сеть доступа, географическое расположение, состояние информационной (автоматизированной) системы и иные параметры. Решение о предоставлении или отказе в доступе принимается на основе политик сопоставления атрибутов субъектов, объектов и контекста, установленных оператором.

Атрибуты безопасности – метаданные, присоединяемые к сетевым пакетам или ассоциированные с сессиями связи, которые содержат структурированную информацию о субъектах доступа, объектах доступа (передаваемой информации) и контексте взаимодействия. Эти характеристики используются системами контроля доступа (включая межсетевые экраны и шлюзы безопасности) для принятия решений о разрешении или запрете сетевого обмена в рамках реализации политики безопасности.

База решающих правил – составная часть системы обнаружения вторжений, содержащая информацию о вторжениях (сигнатурах), на основе которой система обнаружения вторжений принимает решение о наличии вторжения (атаки).

Белый список – перечень ресурсов (IP-адресов, доменных имен, приложений), доступ к которым разрешен; весь остальной трафик блокируется.

Беспроводная локальная вычислительная сеть – группа узлов в пределах ограниченного пространства, для которых обеспечена возможность осуществлять взаимодействие и обмен данными с использованием технологий радиосвязи.

Беспроводный доступ – технология, с помощью которой пользователи и устройства обмениваются данными по беспроводному каналу с помощью радиоволн или иных типов электромагнитного излучения.

Беспроводный канал передачи данных – совокупность технических средств, среды передачи и способа передачи данных между узлами без использования физических кабелей на основе радиоволн или иных типов электромагнитного излучения.

Виртуальная инфраструктура – совокупность виртуальных машин и виртуального оборудования, средств виртуализации, реализующих их эмуляцию, а также аппаратных средств вычислительной техники и хостовых операционных систем, составляющих среду функционирования этих средств виртуализации.

Виртуальная машина – программная эмуляция средства вычислительной техники, предназначенная для организации изолированных вычислений. Изоляция вычислений может использоваться для организации независимых вычислений на ресурсах одного аппаратного средства вычислительной техники, для формирования среды функционирования, независимой от хостовой операционной системы, или для обеспечения переносимости вычислений между различными аппаратными средствами вычислительной техники.

Виртуальное оборудование – оборудование, эмулируемое средством виртуализации, как составная часть виртуальной машины или механизмов взаимодействия виртуальных машин.

Вредоносное программное обеспечение – программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы.

Вторжение (атака) – действие, целью которого является осуществление несанкционированного доступа к информационным ресурсам.

Глубокий анализ пакетов – технология анализа сетевого трафика, которая позволяет проверять не только заголовки пакетов, но и их содержимое (данные), что позволяет блокировать угрозы безопасности информации, контролировать использования сетевых ресурсов и выявлять нежелательные приложения.

Гостевая операционная система – операционная система, управляющая виртуальной машиной.

Демилитаризованная зона – обособленный сегмент информационной системы, расположенный между сетью связи общего пользования (внешними информационными системами) и внутренней инфраструктурой информационной системы.

Дискреционный метод управления доступом – метод, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа.

Зона радиопокрытия – область пространства, в которой обеспечивается возможность подключения и использования услуг беспроводной локальной вычислительной сети.

Интернет вещей – концепция вычислительной сети, соединяющей вещи (физические предметы, устройства), оснащенные встроенными информационными технологиями для взаимодействия друг с другом или внешней средой.

Карта покрытия сигналами точек беспроводного доступа – визуальное представление зоны радиопокрытия и уровня сигнала точек беспроводного доступа в пределах контролируемой зоны.

Категоризация веб-ресурсов – процесс классификации веб-сайтов по тематическим категориям (например, социальные сети, развлечения, бизнес) и уровню риска для применения политик фильтрации.

Компонент информационной системы – программные, программно-аппаратные средства, обеспечивающие выполнение заданной задачи в информационной системе, взаимодействуя с другими элементами системы (например, почтовый сервис, веб-сайт, сетевой сервис).

Конечное устройство – физическое и виртуальное устройство информационной системы, в том числе имеющее доступ к ресурсам сети «Интернет».

Контейнер – среда исполнения программного обеспечения, изолированная средством контейнеризации от других контейнеров и хостовой операционной системы.

Контейнерная среда – средства контейнеризации, контейнеры и их образы, применяемые в информационной системе.

Контекстная проверка трафика – комплексный анализ сетевого трафика с учетом содержания данных, метаинформации, атрибутов безопасности и поведенческих характеристик.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено пребывание лиц, которым не предоставлен доступ к объектам защиты информационной системы и (или) информационно-телекоммуникационной инфраструктуры, на которой размещается информационная система.

Контроль доступа – совокупность мер и средств, предназначенных для регулирования доступа субъектов к объектам информационной системы.

Контроль доступа на основе атрибутов – модель контроля доступа, при которой решение о предоставлении доступа принимается на основе оценки атрибутов субъекта, объекта, действий и контекста.

Личное мобильное устройство – мобильное устройство, которое работник использует в личных целях, а также для доступа к информационной системе. Применение личных мобильных устройств допустимо в информационных системах, в которых не обрабатывается информация ограниченного доступа.

Ложные системы – специально созданные компоненты информационной системы, имитирующие реальные сервисы и ресурсы с целью обнаружения и изучения попыток несанкционированного доступа нарушителей безопасности информации.

Мандатный метод управления доступом – метод, предусматривающий управление доступом субъектов доступа к объектам доступа на основе сопоставления классификационных меток каждого субъекта доступа и каждого объекта доступа, отражающих классификационные уровни субъектов доступа и объектов доступа, являющиеся комбинациями иерархических и неиерархических категорий.

Маркировка информации – процесс присвоения информации меток (атрибутов), определяющих ее уровень конфиденциальности, целостности и другие свойства безопасности.

Маскирование системы – комплекс мер по сокрытию реальных характеристик и конфигурации информационной системы для затруднения проведения разведки потенциальным нарушителем безопасности информации.

Межсетевой экран – средство защиты информации, осуществляющее контроль и фильтрацию сетевого трафика на основе заданных правил.

Метки целостности данных – атрибуты, указывающие на требования к неизменности информации и позволяющие контролировать ее модификацию.

Микросегментация – метод защиты информации, заключающийся в логическом разделении информационной системы на изолированные сегменты на уровне отдельных компонентов (рабочих нагрузок, приложений, сервисов).

Многофункциональный межсетевой экран – средство защиты информации, сочетающее функции межсетевого экранирования с дополнительными возможностями, такими как контроль приложений, предотвращение вторжений и фильтрация контента.

Мобильное устройство – смартфон и планшетный компьютер под управлением мобильной операционной системы, обеспечивающей управление его аппаратными ресурсами и исполнение программного обеспечения (приложений) в рамках специализированной мобильной модели управления приложениями, включая механизмы жизненного цикла приложений, изоляции и управления энергопотреблением. К мобильным операционным системам не относятся операционные системы общего назначения, адаптированные для использования на мобильных устройствах.

Мониторинг аномалий – процесс непрерывного наблюдения за сетевым трафиком с целью выявления отклонений от нормальных паттернов поведения.

Морфологический анализ – метод анализа структуры и содержания веб-ресурсов (URL, доменные имена) для выявления подозрительных или запрещенных паттернов.

Непривилегированные пользователи – пользователи информационной системы, выполняющие задачи по обработке информации в информационной системе, не являющиеся привилегированными пользователями.

Образ контейнера – пакет программного обеспечения, необходимого для развертывания контейнера. Как правило, образ контейнера включает в себя все зависимости, необходимые для функционирования прикладного программного обеспечения, за исключением системных вызовов ядра хостовой операционной системы или средства контейнеризации.

Операционная система – программное обеспечение, предназначенное для управления аппаратными ресурсами средства вычислительной техники и формирования среды функционирования прикладных программ.

Поведенческий анализ – метод оценки действий пользователей и систем для выявления отклонений от нормальных, санкционированных паттернов поведения.

Подлинность сетевых соединений – свойство сетевого взаимодействия, гарантирующее, что соединение установлено с заявленным, доверенным узлом или сервисом.

Привилегированные пользователи – пользователи информационной системы, выполняющие задачи по администрированию, обеспечению функционирования, обеспечению безопасности информационной системы.

Программный интерфейс взаимодействия приложений (API) – прикладной программный интерфейс, описание способов (набор классов, процедур, функций, структур или констант), которыми одна компьютерная программа может взаимодействовать с другими программами).

Ретроспективный анализ данных – исследование исторических данных и событий безопасности для выявления ранее не обнаруженных инцидентов и скрытых взаимосвязей.

Ролевой метод управления доступом – метод, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа (совокупность действий и обязанностей, связанных с определенным видом деятельности).

Сегмент информационной системы – совокупность нескольких компонентов информационной системы, использующих общую (в том числе разделяемую) среду передачи и объединенных для единства решения функциональных задач.

Сервер виртуализации – средство вычислительной техники, на котором функционирует средство виртуализации.

Сигнатура – характерные признаки вторжения (атаки), используемые для его (её) обнаружения.

Система искусственного интеллекта – информационная система или совокупность информационных систем и технических средств, использующая одну или несколько технологий искусственного интеллекта**.**

Система обнаружения вторжений – программное или программно-техническое средство, реализующее функции автоматизированного обнаружения действий в информационной системе, направленных на преднамеренный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней.

Система хранения данных – программный или программно-аппаратный комплекс, предоставляющий сервис хранения данных. Доступ к сервису предоставляется как правило при помощи блочного, файлового или объектного интерфейсов. Пользователи блочного интерфейса получают доступ к виртуальным дискам, которые рассматриваются операционной системой как обычные локальные диски. Для этого используются такие протоколы как iSCSI, Fibre Channel, SAS/SATA, FC-NVMe. Пользователи файлового интерфейса получают доступ к сетевым файловым системам таким как NFS или SMB/CIFS. Пользователи объектного интерфейса получают доступ к хранению отдельных элементов данных (объектов) при помощи таких протоколов как S3 или Swift.

Системы управления контентом (CMS) – компьютерная программа, используемая для обеспечения и организации совместного процесса создания, редактирования и управления содержимым, иначе – контентом.

Служебные данные – данные, содержащиеся в запросах и ответах, предаваемых совместно с защищаемой информацией с использованием программного интерфейса взаимодействия приложений (API). К служебной информации относятся поля структур протоколов, разметка представления информации, технологическая информация приложений и другие данные.

Среда виртуализации – изолированная программная среда, созданная с помощью технологии виртуализации.

Средство виртуализации – программное средство, обеспечивающие создание и функционирование виртуальных машин.

Средство вычислительной техники (аппаратное) – аппаратный комплекс, предназначенный для выполнения вычислений, как правило, выполняющихся под управлением операционной системы.

Средство контейнеризации – программное средство, обеспечивающее создание и функционирование контейнеров.

Субъект доступа – пользователь, процесс или устройство, запрашивающее доступ к информации или ресурсам информационной системы.

Технологии искусственного интеллекта – технологии, основанные на использовании искусственного интеллекта, включающие в себя компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и перспективные методы искусственного интеллекта.

Точка беспроводного доступа – устройство или оборудование, позволяющие беспроводным устройствам подключаться к вычислительной сети.

Удаленный доступ – доступ пользователей к информационным системам и (или) содержащейся в них информации с использованием сетей связи общего пользования, включая сеть «Интернет», и иных сетей связи, находящихся

за пределами контролируемой зоны, включая доступ с применением технологий виртуальных частных сетей (VPN), туннелирования и иных средств удаленного подключения.

Уровень сигнала – количественная характеристика сигнала, рассматриваемая относительно выбранного опорного значения.

Устройство «интернета вещей» – устройство, производящее измерение свойств (характеристик) внешней среды и преобразующее их в цифровое представление, которое может передаваться по вычислительной сети через интерфейс взаимодействия датчика**,** а также устройство «интернета вещей», функционирующее во внешней среде и преобразующее цифровые команды, поступающие по вычислительной сети через интерфейс взаимодействия исполнительного устройства, в действия во внешней среде.

Хостовая операционная система – операционная система, составляющая среду функционирования средства контейнеризации.

Централизованное управление – подход к администрированию, при котором настройки и политики для распределенных систем управляются из единой контрольной точки.

Черный список – перечень ресурсов (IP-адресов, доменных имен, приложений), доступ к которым запрещен.

Приложение № 2
к методическому документу

Содержание базовых мер защиты информации для соответствующего класса защищенности информационной системы

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Классы защищенности информационной системы		
		3	2	1
1. Идентификация и аутентификация (ИАФ)				
ИАФ.1	Идентификация пользователей	+	+ 1	+ 1
ИАФ.2	Идентификация устройств			
ИАФ.3	Аутентификация пользователей	+	+	+ 1
ИАФ.4	Аутентификация устройств			
2. Управление доступом (УПД)				
УПД.1	Реализация модели управления доступом	+	+ 1, 2	+ 1, 2
УПД.2	Разграничение и контроль прав доступа	+	+ 1	+ 1, 2
УПД.3	Управление учетными записями	+	+ 1	+ 1, 2
УПД.4	Ограничение неуспешных и нерегламентированных попыток доступа в информационную систему	+	+ 1, 2	+ 1, 2
УПД.5	Предупреждение пользователя при его доступе к информационной системе			
УПД.6	Оповещение пользователя о предыдущем входе в информационную систему			
УПД.7	Ограничение числа параллельных сеансов доступа		+	+ 1а
УПД.8	Блокирование сеанса доступа пользователя при неактивности	+	+	+

УПД.9	Контроль действий субъектов доступа до идентификации и аутентификации	+	+	+
3. Регистрация событий безопасности (РСБ)				
РСБ.1	Определение событий безопасности и данных о них, подлежащих регистрации	+ 1	+ 1, 2	+ 1, 2, 3
РСБ.2	Анализ событий безопасности и реагирование на них	+	+	+
РСБ.3	Генерация временных меток при регистрации событий безопасности	+	+	+
РСБ.4	Требования к сбору, хранению и защите данных о событиях безопасности	+	+	+
РСБ.5	Реагирование на сбои при регистрации событий безопасности	+	+	+
4. Защита виртуализации и облачных вычислений (ЗСВ)				
ЗСВ.1	Доверенная загрузка средства виртуализации и виртуальных машин	+	+ 1	+ 1, 2
ЗСВ.2	Контроль целостности средств виртуализации и виртуальных машин	+	+ 1, 2	+ 1, 2
ЗСВ.3	Регистрация событий безопасности в среде виртуализации	+	+	+
ЗСВ.4	Управление доступом в среде виртуализации	+	+	+
ЗСВ.5	Резервное копирование в среде виртуализации	+	+	+
ЗСВ.6	Ограничение программной среды в среде виртуализации	+	+	+ 1
ЗСВ.7	Защита памяти в среде виртуализации	+	+	+
ЗСВ.8	Идентификация и аутентификация в среде виртуализации	+	+	+

ЗСВ.9	Управление виртуальными машинами		+	+
5. Защита технологий контейнерных сред и их оркестрации (ЗКО)				
ЗКО.1	Контроль целостности в контейнерных средах	+	+ 1, 2	+ 1,2,3,4,5,6
ЗКО.2	Регистрация событий безопасности в контейнерных средах	+	+	+
ЗКО.3	Управление доступом в контейнерных средах	+	+	+
ЗКО.4	Резервное копирование в контейнерных средах	+	+	+
ЗКО.5	Изоляция контейнеров в контейнерной среде	+	+ 1	+ 1
ЗКО.6	Идентификация и аутентификация в контейнерной среде	+	+	+
ЗКО.7	Управление контейнерами и их образами (оркестрация)	+	+	+
ЗКО.8	Выявление и устранение уязвимостей в контейнерной среде	+	+ 1, 2	+ 1, 2
6. Защита сервисов электронной почты (ЗЭП)				
ЗЭП.1	Защита ящиков и сообщений электронной почты	+	+	+
ЗЭП.2	Управление доступом пользователей	+	+	+
ЗЭП.3	Защита от вредоносных вложений	+	+	+
ЗЭП.4	Защита от фишинга	+	+ 1	+ 1
ЗЭП.5	Защита от спама	+	+	+
ЗЭП.6	Защита метаданных и иной технической информации сервисов электронной почты	+	+	+
7. Защита веб-технологий (ЗВТ)				
ЗВТ.1	Защита пользовательских данных	+	+	+

ЗВТ.2	Управление доступом пользователей	+	+ 1	+ 1
ЗВТ.3	Контроль и фильтрация трафика веб-приложений	+	+	+ 1
ЗВТ.4	Регистрация событий безопасности в веб-приложениях и реагирование на них	+	+	+
ЗВТ.5	Проверка файлов, передаваемых веб-приложениями, на вредоносное программное обеспечение	+	+	+
8. Защита программных интерфейсов взаимодействия приложений (API) (ЗПИ)				
ЗПИ.1	Защита данных API	+	+ 1	+ 1
ЗПИ.2	Управление доступом пользователей и приложений	+	+	+
ЗПИ.3	Проверка на соответствие спецификации API	+	+	+ 1
9. Защита конечных устройств (ЗКУ)				
ЗКУ.1	Управление доступом к конечным устройствам	+	+	+
ЗКУ.2	Обеспечение целостности программного обеспечения конечного устройства	+	+	+
ЗКУ.3	Антивирусная защита и обнаружение и предотвращение вторжений на конечных устройствах	+	+ 1	+ 1
ЗКУ.4	Мониторинг процессов и состояния устройства	+	+	+
ЗКУ.5	Контроль и фильтрация трафика на конечном устройстве			
ЗКУ.6	Анализ и реагирование на события безопасности	+	+ 1	+ 1
10. Защита мобильных устройств (ЗМУ)				
ЗМУ.1	Идентификация и аутентификация пользователей	+	+ 1	+ 1

ЗМУ.2	Управление доступом пользователей к мобильным устройствам	+	+	+
ЗМУ.3	Обеспечение целостности	+	+ 1	+ 1, 2
ЗМУ.4	Защита данных	+	+	+ 1
ЗМУ.5	Антивирусная защита	+	+	+
ЗМУ.6	Контроль приложений	+	+	+
ЗМУ.7	Ограничение и контроль функциональности	+	+	+
ЗМУ.8	Определение и контроль геопозиции			
ЗМУ.9	Регистрация, анализ и реагирование на события безопасности	+	+ 1	+ 1
11. Защита технологий «интернета вещей» (ЗИВ)				
ЗИВ.1	Идентификация и аутентификация	+	+	+
ЗИВ.2	Управление доступом	+	+	+
ЗИВ.3	Защита данных	+	+ 1	+ 1
ЗИВ.4	Контроль целостности	+	+	+
ЗИВ.5	Регистрация, анализ и реагирование на события безопасности	+	+ 1	+ 1
12. Защита точек беспроводного доступа (ЗБД)				
ЗБД.1	Идентификация и аутентификация	+	+	+ 1
ЗБД.2	Управление доступом	+	+	+
ЗБД.3	Защита пользовательских данных	+	+	+
ЗБД.4	Контроль целостности	+	+	+
ЗБД.5	Ограничение уровней сигналов	+	+	+
ЗБД.6	Регистрация, анализ и реагирование на события безопасности	+	+ 1	+ 1

13. Антивирусная защита (АВЗ)				
АВЗ.1	Антивирусная защита устройств	+	+	+
АВЗ.2	Антивирусная защита электронной почты	+	+	+
АВЗ.3	Антивирусная проверка сетевого трафика	+	+	+
АВЗ.4	Применение замкнутой системы (среды) предварительного выполнения программ («песочницы»)			
14. Обнаружение и предотвращение вторжений на сетевом уровне (СОВ)				
СОВ.1	Обнаружение и предотвращение вторжений на периметре	+	+ 1	+ 1
СОВ.2	Обнаружение и предотвращение вторжений в сегментах информационной системы	+	+	+
15. Сегментация и межсетевое экранирование (МСЭ)				
МСЭ.1	Сегментация сети	+	+	+ 1
МСЭ.2	Организация демилитаризованной зоны	+	+	+
МСЭ.3	Контроль сетевого доступа и фильтрация трафика	+	+	+
МСЭ.4	Маскирование системы			
МСЭ.5	Создание ложных систем			
16. Защита от компьютерных атак, направленных на отказ в обслуживании (ЗОО)				
ЗОО.1	Защита от компьютерных атак, направленных на отказ в обслуживании, при доступе внешних пользователей к прикладным сервисам, предоставляемым информационной системой	+	+	+
ЗОО.2	Контроль и фильтрация входящего трафика	+	+	+ 1

ЗОО.3	Мониторинг состояния сервисов и интерфейсов	+	+	+
ЗОО.4	Балансировка нагрузки			
ЗОО.5	Ограничение нагрузки	+	+	+
ЗОО.6	Поддержка резерва достаточной пропускной способности и расширение ресурсов при сбоях		+	+
17. Защита каналов связи и сетевого взаимодействия (ЗКС)				
ЗКС.1	Защита данных при передаче по каналам связи	+	+	+
ЗКС.2	Контроль атрибутов безопасности при сетевом взаимодействии	+	+	+
ЗКС.3	Контроль доступа к внешним ресурсам	+	+	+
ЗКС.4	Контекстная проверка исходящего трафика			

«+» – мера защиты информации включена в базовый набор мер для соответствующего класса защищенности информационной системы и должны выполняться требования к реализации данной меры защиты информации.

«цифра» или «цифра»«буква» – должны выполняться требования к усилению данной меры защиты информации, указанные в подразделе «Требования к усилению». Цифры и буквы, не включенные в таблицу и указанные под рубриками «требования к усилению» 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.

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.

Приложение № 3
к методическому документу

Выбор мер защиты информации для реализации в информационной системе

Выбор мер защиты информации осуществляется исходя из класса защищенности информационной системы, определяющего требуемый уровень защищенности содержащейся в ней информации, и угроз безопасности информации, включенных в модель угроз безопасности информационной системы, а также с учетом структурно-функциональных характеристик информационной системы, к которым относятся архитектура, структура и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, взаимосвязи 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.

Определение класса защищенности информационной системы проводится в соответствии с приложением к Требованиям о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденным приказом ФСТЭК России от 11 апреля 2025 г. № 117.

Устанавливаются три класса защищенности информационной системы (первый класс (К1), второй класс (К2), третий класс (К3), определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс – третий, самый высокий – первый.

При обработке в информационной системе информации, содержащей персональные данные, реализуемые в соответствии с пунктом 63 Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденных приказом ФСТЭК России от 11 апреля 2025 г. № 117, меры защиты информации:

для информационной системы 1 класса защищенности обеспечивают 1, 2, 3 и 4 уровни защищенности персональных данных[12];

[12] Устанавливается в соответствии с Требованиями к защите персональных

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.

В случае если информационная система является значимым объектом критической информационной инфраструктуры Российской Федерации, реализуемые в соответствии с пунктом 63 Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденных приказом ФСТЭК России от 11 апреля 2025 г. № 117, меры защиты информации:

для информационной системы 1 класса защищенности обеспечивают I, II и III категории значимости объектов критической информационной инфраструктуры[13];

для информационной системы 2 класса защищенности обеспечивают II и III категории значимости объектов критической информационной инфраструктуры;

для информационной системы 3 класса защищенности обеспечивают III категорию значимости объектов критической информационной инфраструктуры.

Выбор мер защиты информации для их реализации в информационной системе включает:

реализацию базовых мер защиты информационных систем и содержащейся в них информации соответствующих классов защищенности, устанавливаемых оператором (обладателем информации);

адаптацию базовых мер защиты информационных систем и содержащейся в них информации применительно к архитектуре информационных систем, применяемым информационным технологиям, особенностям функционирования информационных систем;

верификацию адаптированных базовых мер защиты информационных систем и содержащейся в них информации в соответствии с актуальными угрозами и возможностями нарушителей, их дополнение и (или) усиление.

данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

[13] Устанавливается в соответствии с Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127.

Определение базовых мер защиты информации для установленного класса защищенности информационной системы является первым шагом в выборе мер защиты информации, подлежащих реализации в информационной системе. Определение базового набора мер защиты информации основывается на классе защищенности информационной системы. В соответствии с настоящим методическим документом в качестве начального выбирается один из трех базовых наборов мер защиты информации, соответствующий установленному классу. Меры защиты информации, обозначенные знаком «+» в приложении № 2 к настоящему методическому документу включены в базовый набор мер защиты информации для соответствующего класса защищенности информационной системы. Меры защиты информации, не обозначенные знаком «+», к базовому набору мер не относятся, и могут применяться при последующих действиях по адаптации и верификации мер защиты информации, а также разработке компенсирующих мер защиты информации.

Базовые меры защиты информации, выбранные в соответствии с классом защищенности информационной системы, подлежат адаптации применительно к структурно-функциональным характеристикам и особенностям функционирования информационной системы, уточнению в зависимости от угроз безопасности информации и при необходимости дополнению мерами защиты информации, включенными в иные нормативные правовые акты, нормативные и методические документы по защите информации.

При адаптации базового набора мер защиты информации учитываются:

применяемые информационные технологии и структурно-функциональные характеристики информационной системы;

цели и задачи защиты информации в информационной системе;

перечень проводимых оператором мероприятий по защите информации.

Адаптация базового набора мер защиты информации, как правило, предусматривает исключение мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе.

Верификация адаптированных базовых мер защиты информации проводится с учетом результатов оценки возможности адаптированного базового набора мер защиты информации блокировать угрозы безопасности информации, включенные в модель угроз безопасности информации, или снизить вероятность их реализации исходя из условий функционирования информационной системы.

Исходными данными при уточнении адаптированного базового набора мер защиты информации являются перечень угроз безопасности информации

и возможности нарушителей, включенные в модель угроз безопасности информации.

При верификации адаптированных мер защиты информации для каждой угрозы безопасности информации, включенной в модель угроз, сопоставляется мера защиты информации из адаптированного базового набора мер защиты информации, обеспечивающая блокирование этой угрозы безопасности или снижающая вероятность ее реализации исходя из условий функционирования информационной системы. В случае если адаптированный базовый набор мер защиты информации не обеспечивает блокирование угроз безопасности информации, в него дополнительно включаются меры защиты информации, приведенные в разделе 4 настоящего методического документа.

В подразделах «Требования к реализации» для каждой меры, приведенной в разделе 4 настоящего методического документа, указано требование к тому, каким образом и в каком объеме должна быть реализована каждая мера защиты информации. Требования к реализации мер защиты информации являются минимальными требованиями, выполнение которых должно быть обеспечено в информационной системе соответствующего класса защищенности в случае, если эта мера выбрана для реализации в качестве верифицированной адаптированной базовой меры защиты информации.

В зависимости от класса защищенности информационной системы минимальные требования к реализации верифицированной адаптированной базовой меры защиты информации подлежат усилению для повышения уровня защищенности информации. Все возможные усиления мер защиты информации приведены в подразделах «Требования к усилению» раздела 4 настоящего методического документа для каждой меры защиты информации. Усиления мер защиты информации применяются дополнительно к требованиям по реализации мер защиты информации, приведенным в подразделах «Требования к реализации».

Итоговое содержание каждой верифицированной адаптированной базовой меры защиты информации, которое, как минимум, должно быть реализовано в информационной системе, приведено в таблице подраздела «Реализация в информационной системе».