Проект

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

Экз. № _

Утвержден ФСТЭК России
«__» _____ 202_г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕРОПРИЯТИЯ И МЕРЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

2026

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий методический документ «Мероприятия и меры 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), в информационно-телекоммуникационных инфраструктурах, выполняющих общие технологические функции и обеспечивающие 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 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.

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

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

1.6. Для целей настоящего методического документа используются термины и определения, установленные национальными стандартами в

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.

области защиты информации и обеспечения информационной безопасности, а также термины и определения, приведенные в приложении № 1 к настоящему методическому документу.

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

2.1. Повышение уровня цифровой зрелости органов (организаций), усиленная цифровизация производственных, промышленных, бизнес-процессов обусловила критическую зависимость 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 наступление 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, управления и контроля. При этом требуется однозначное задокументированное определение мероприятий (процессов), 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 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 утвержденной в органе (организации) политике защиты информации и иных документах по защите информации (стандартах, регламентах), содержащих цели защиты информации и требования по защите информации, а также исключить осуществление полномочий (функций), проведение работ (оказание услуг)
без учета требований по защите информации. Фактором, оказывающим существенное 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, 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 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 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, а должны предусматривать организацию процессов по поиску, анализу и принятию мер, направленных на блокирование угроз. При анализе угроз 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 обеспечивающие 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] 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.

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 программно-аппаратных средств, электронной компонентной базы и телекоммуникационного оборудования в соответствии с требованиями по 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 достаточности и эффективности проведения мероприятий по защите информации осуществляется на основе оценки уровня зрелости органа (организации) ($П_{зи}$). 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.

3. 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 информационной системы, 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 актуальных угроз безопасности информации должны проводиться в ходе создания (развития) информационных систем и в ходе их эксплуатации.

Выявление и оценка актуальных 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 актуальных угроз безопасности информации должна предусматривать определение угроз, 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 актуальных угроз 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 безопасности информации. 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 безопасности информации исходя из критериев возможных последствий их реализации (возникновения);

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

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

Выявление и оценку актуальных угроз организует структурное подразделение, специалисты по защите информации оператора.

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
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 источниками данных из систем управления событиями безопасности, систем обнаружения и предотвращения вторжений, средств антивирусной защиты, средств

---

[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.

[4] Усиления мероприятий (процессов) по защите информации, приведенные в подразделе «требования к усилению», 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

защиты конечных устройств (точек), межсетевых экранов, 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 (TI-платформы).

3.2. Контроль конфигураций информационных систем

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 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 конфигураций текущих;

определение конфигураций объектов инвентаризации и контроль

их изменений, выявление фактов несанкционированного изменения конфигураций объектов инвентаризации;

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

Должны быть определены подразделения (работники), ответственные за контроль состава информационных систем и соответствия их конфигураций внутренним стандартам. Подразделением (работниками), ответственным
за обеспечение эксплуатации информационных систем, должен быть обеспечен доступ к указанным сведениям структурного подразделения специалистов
по защите информации.

По всем фактам несанкционированных изменений состава объектов инвентаризации и их конфигураций структурным подразделением, специалистами по защите информации 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 подлежащие контролю в рамках контроля конфигураций;

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

настройки и конфигурации программных, программно-аппаратных средств, предназначенных для обеспечения доступа пользователей к сети «Интернет»;

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

подразделение (работники), ответственные за настройку и установку конфигураций программных, программно-аппаратных средств, а также за контроль конфигураций информационных систем;

действия 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 (SMDB-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

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 осуществляется 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 соответствии с Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России.

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 осуществляется 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 критичность) должны корректироваться способы их устранения.

Процесс управления уязвимостями должен быть взаимоувязан с другими процессами и процедурами деятельности органа (организации) в области защиты информации и информационных технологий.

Управление уязвимостями осуществляется структурным подразделением, специалистами по защите информации с участием подразделений (работников), обеспечивающих эксплуатацию информационных систем. В процессе управления уязвимостями могут быть задействованы другие подразделения и специалисты, в частности, подразделение, ответственное за организацию закупок программных и программно-аппаратных средств, подразделение, ответственное
за эксплуатацию инженерных систем.

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

перечень информационных систем, для которых осуществляется управление уязвимостями;

подразделения (работники), ответственные за организацию и контроль управления уязвимостями, а также участвующие 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 подразделения (работников) при реализации операций по управлению уязвимостями.

Требования к усилению:

1) для управления уязвимостями используются автоматизированные системы управления уязвимостями;

2) для мониторинга уязвимостей и оценки их применимости используются результаты контроля (оценки) уровня защищенности информации;

3) для мониторинга уязвимостей применяются средства анализа угроз (TI-платформы);

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

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

3.4. Управление обновлениями

Цель: Своевременная установка обновлений программного обеспечения, направленных на устранение уязвимостей, и обеспечение

безопасности обновлений программного обеспечения и процессов по его установке.

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 в соответствии с Методикой тестирования обновлений программных, программно-аппаратных средств, утвержденной ФСТЭК России;

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

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

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 (online) обновлений программных, программно-аппаратных средств не допускается.

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 информационных систем, для которых осуществляется управление обновлениями;

подразделения (работники), ответственные за организацию и контроль управления обновлениями, а также участвующие в реализации процессов управления обновлениями, их обязанности (функции) и права (полномочия);

описание операций, осуществляемых при управлении обновлениями;

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

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 (SMDB-системы);

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

3) для тестирования обновлений применяется стенд тестирования, предназначенный в том числе для тестирования обновлений программного обеспечения.

3.5. Обеспечение защиты информации при обработке, хранении и обращении с информаций ограниченного доступа

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 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.

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

Средства хранения информации ограниченного доступа должны размещаться в пределах контролируемой зоны, несанкционированный доступ
в которую лиц, не являющихся работниками оператора, должен быть ограничен.

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;

программно-аппаратные средства, предназначенные для хранения информации ограниченного доступа, подлежащие 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 используемые при проведении таких мероприятий программные, программно-аппаратные средства;

подразделения (работники), ответственные 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 подразделения (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 сертифицированных 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 средствах хранения информации за пределы контролируемой зоны;

7) исключение возможности несанкционированной передачи, распространения, вывода информации ограниченного доступа из информационной системы за счет применения средств защиты от утечек информации (DLP-систем);

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

3.6. Обеспечение защиты информации при использовании конечных устройств

Цель: Исключение возможности несанкционированного доступа к информационным системам и конечным устройствам или воздействия на них через интерфейсы и порты, 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;

реализацию на конечных устройствах мер по антивирусной защите;

осуществление на конечных устройствах (автоматизированных рабочих местах пользователей) 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 подразделением (работниками), обеспечивающими функционирование информационных систем, только 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 ее использования
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 централизовано структурным подразделением, специалистами
по защите информации.

3.7. Обеспечение защиты информации при применении мобильных устройств

Цель: Исключение возможности несанкционированного доступа (воздействия) 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 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;

реализацию в мобильных устройствах мер по антивирусной защите;

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

Предоставление доступа к информационным системам с использованием мобильных 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.

В информационных системах при доступе к ним с использованием мобильных устройств должны быть приняты меры по идентификации и строгой аутентификации подключаемых с использованием мобильных устройств пользователей, реализованной с применением сертифицированных шифровальных (криптографических) средств защиты информации, 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 сертифицированных шифровальных (криптографических) средств защиты информации, а также контролю сетевых доступов к сегментам информационной систем удаленных пользователей и обнаружению и предотвращению вторжений на сетевом уровне при осуществлении доступа с использованием мобильных устройств.

В мобильных устройствах пользователей принимаются меры по идентификации и аутентификации пользователей, разграничению и контролю доступа пользователей к мобильным программам и приложениям, регистрации событий безопасности в мобильном устройстве, антивирусной защите, поддержке механизмов строгой аутентификации пользователей и защите данных, передаваемых по сети «Интернет».

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.

Доступ пользователей к информационным системам и содержащейся в них информации в целях выполнения своих обязанностей (функций) с использованием мобильных устройств должен осуществляться с применением строгой аутентификации, реализованной с применением сертифицированных шифровальных (криптографических) средств защиты информации.

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.

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 соответствия мобильных устройств настоящим Требованиям 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.

При применении пользователями мобильных устройств для доступа к информационным системам и содержащейся в них информации, не связанного с выполнением пользователем свих 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.

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

требования к типам мобильных устройств, с использованием которых разрешен доступ к информационным системам и содержащейся в них информации;

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

требования к составу портов, интерфейсов, протоколов мобильных устройств (автоматизированных рабочих мест пользователей) 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 ее использования в случае взаимодействия с сетью «Интернет».

Требования к усилению:

1) на мобильных устройствах вычислительная среда, используемая для доступа к информационным системам и обработке содержащейся в них информации, должна быть изолирована от вычислительной среды, используемой для работы с общедоступными ресурсами и сервисами;

2) при хранении в мобильных устройствах конфиденциальной информации вне контролируемой зоны ее защита обеспечивается с использованием сертифицированных шифровальных (криптографических) средств защиты информации;

3) 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), обеспечивающими функционирование информационной системы, по согласованию со структурным подразделением, специалистами по защите информации;

4) по всем фактам несанкционированного изменения конфигураций и настроек мобильных устройств относительно конфигураций и настроек, определенных во внутренних стандартах, структурным подразделением, специалистами по защите информации проводится анализ и выявляются причины таких изменений;

5) в случае использования для доступа к информационным системам

более 30 мобильных устройств должно обеспечиваться автоматизированное управление и контроль использования мобильных устройств.

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

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 и порты 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 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 с использованием сетей связи общего пользования, включая сеть «Интернет», и соответствующих сетевых протоколов удаленного доступа.

Доступ пользователей к информационным системам и содержащейся в них информации с использованием технологии виртуальных частных сетей
не относится к удаленному доступу. Подключаемые с использованием технологии виртуальных частных сетей программно-аппаратные средства или
их совокупность рассматриваются как сегменты информационной системы образующие соответствующие домены, в которых реализуются меры по

защите информации в соответствии с установленными к информационным системам требованиями.

Удаленный доступ к информационным системам предоставляется подразделением (работниками), обеспечивающими функционирование информационных систем, в соответствии с заявками подразделений, эксплуатирующих информационные системы, согласованными со структурным подразделением, специалистами по защите информации.

В информационных системах при осуществлении удаленного доступа к ним пользователей должны быть приняты меры по идентификации и строгой аутентификации удаленно подключаемых пользователей, реализованной
с применением сертифицированных шифровальных (криптографических) средств защиты информации, 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 сертифицированных шифровальных (криптографических) средств защиты информации, а также контролю сетевых доступов к сегментам информационной систем 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). Возможность удаленного доступа
с использованием протоколов telnet, rdp, http, ftp, SMB и аналогичных

им небезопасных протоколов не допускается.

Предоставление удаленного доступа к информационным системам с использованием личных программно-аппаратных средств работников допускается при условии применения сертифицированных 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.

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;

подразделения (работники), ответственные 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 подразделения (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 обеспечивается 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) должно быть обеспечено незамедлительное блокирование учетных записях в случае обнаружения сведений о них в общедоступных источниках,
в том числе в базах утечек информации;

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

5) 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;

6) 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.

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

Цель: Исключение возможности несанкционированного доступа (воздействия) к информационным системам и содержащейся в них информации
за счет несанкционированного подключения к точкам беспроводного доступа
и доступа к беспроводным каналам передачи данных, подмены взаимодействующих с ними программно-аппаратных средств или доступа к ним.

Требования к реализации: Обеспечение защиты информации при беспроводном доступе пользователей к информационным системам 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, логическое разделение 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).

3.10. Обеспечение защиты информации при предоставлении

пользователям привилегированного доступа

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, 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, реализованной с применением сертифицированных шифровальных (криптографических) средств защиты информации, или усиленной многофакторной аутентификации;

регистрацию всех 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 осуществлять использование привилегированных учетных записей 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 использования структурным подразделением, специалистами по защите информации.

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. 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, не определенных во внутренних стандартах, 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 в соответствии с настоящими Требованиями. 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 в соответствии с настоящими Требованиями.

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.

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

перечень лиц (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 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) привилегированный доступ должен осуществляться с выделенных для этого автоматизированных рабочих мест. Доступ к информационным системам
по протоколам управления должен быть разрешен только с выделенных автоматизированных рабочих мест. Доступ к выделенным рабочим станциям должен быть разрешен только для работников, на которых возложены функции
по администрированию информационных систем;

2) применение автоматизированных систем управления привилегированными учетными записями для предоставления возможности использования, учета, изменения, блокирования и контроля использования привилегированных учетных записей допускается;

3) главный администратор создает, изменяет, блокирует привилегированные учетные записи 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 должны быть переданы
в структурное подразделение (специалистам) по защите информации для учета
и контроля использования. Привилегированные учетные записи структурного подразделения, специалистов по защите информации создаются по решению руководителя, ответственного лица;

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 настоящими Требованиями, внутренними регламентами и стандартами в части, касающейся;

5) системные администраторы и администраторы безопасности для выполнения своих обязанностей (функций) должны использовать только выделенные оператором для администрирования программно-аппаратные

средства, защита информации в которых обеспечивается в соответствии с настоящими Требованиями. Использование для этих целей иных программно-аппаратных средств допускается только при использовании сертифицированных средств обеспечения безопасной дистанционной работы;

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

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

8) 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

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 информационной безопасности;

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;

выявление фактов эксплуатации уязвимостей информационных систем

на основе анализа событий безопасности и иных данных мониторинга;

своевременное информирование руководителя оператора или ответственного лица о выявленных нарушениях безопасности информации и (или) нарушениях функционирования информационных систем.

Руководство работами по мониторингу информационной безопасности информационных систем оператора осуществляет ответственное лицо оператора.

Мониторинг информационной безопасности проводится структурным подразделением, специалистами по защите информации.

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

перечень информационных систем, отдельных программно-аппаратных средств, включенных в область действия мониторинга информационной безопасности;

подразделение (работники), на которое возложены функции по мониторингу информационной безопасности, его функции (обязанности) и права;

перечень и содержание мероприятий по мониторингу информационной безопасности;

действия подразделений, пользователя в случае выявления по результатам мониторинга информационной безопасности факта или признаков реализации угроз;

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

Во внутреннем стандарте устанавливаются требования к сбору, регистрации и анализу событий безопасности, подлежащие 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, оператором 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) использование доверенных технологий искусственного интеллекта для анализа зафиксированных событий безопасности, выявленных в них признаков возникновения компьютерных инцидентов и компьютерных атак;

4) реагирование на актуальные угрозы обеспечивают структурное подразделение, специалисты по защите информации и подразделение, работники, обеспечивающие функционирование информационных систем. Порядок взаимодействия подразделений (работников) оператора при осуществлении мониторинга информационной безопасности определяется во внутренних регламентах;

5) структурным подразделением, специалистами по защите информации ежегодно в срок, установленный внутренними регламентами, разрабатывается отчет о результатах мониторинга в прошедшем году, который представляется руководителю оператора. В отчет включаются сведения об объектах мониторинга, выявленных актуальных угрозах и принятых мерах по защите от них, предложения по совершенствованию организации и управления защитой информации, мер по повышению уровня защищенности информации, содержащейся в информационных системах.

3.12. Обеспечение разработки 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.

Цель: Предотвращение появления, выявление и устранение уязвимостей
в разрабатываемом оператором (обладателем информации) программном обеспечении.

Требования к реализации: Разработка безопасного программного обеспечения должна предусматривать:

планирование мероприятий по разработке безопасного программного обеспечения;

обучение работников, осуществляющих разработку, поддержку безопасного программного обеспечения;

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.

В случае самостоятельной разработки оператором (обладателем информации) программного обеспечения, предназначенного для использования
в информационных системах, должны быть реализованы меры, предусмотренные ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» и иными национальными стандартами
по разработке безопасного программного обеспечения.

Мероприятия (процессы) по разработке безопасного программного обеспечения разрабатываются структурным подразделением, специалистами
по защите информации совместно с работниками, на которых возложены обязанности (функции) по разработке программного обеспечения.

Требования к документированию: Внутренний регламент по разработке безопасного программного обеспечения[6] в случае его самостоятельной разработки оператором (обладателем информации) должен содержать:

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

подразделения (работники), на которые 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;

инструментальные средства, используемые при реализации мероприятий (процессов) по разработке безопасного программного обеспечения;

подразделения (работники), на которые возложены функции по контролю процессов разработки безопасного программного обеспечения, их функции

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

и полномочия;

порядок 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.

3.12. Обеспечение физической защиты информационных систем

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;

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 программно-аппаратным средствам информационных систем, предназначенным для 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 программно-аппаратным 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 содержащейся 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 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);

перечень помещений (зон помещений, шкафы, футляры, корпуса), в которых установлены, хранятся средства обработки и хранения информации, физический доступ к которым должен быть исключен;

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;

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

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.

3.13. Обеспечение непрерывности функционирования информационных систем при возникновении нештатных ситуаций

Цель: Обеспечение возможности восстановления выполнения функций (процессов, видов работ) информационных систем, для которых оператором (обладателем информации) 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 значимые 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;

выделение необходимого для проведения работ по восстановлению функционирования информационных систем количества 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.

Непрерывность функционирования информационных систем при возникновении нештатных ситуаций должна обеспечиваться подразделением (работниками), ответственным за обеспечение функционирования информационных систем.

Интервалы времени восстановления функционирования информационных систем, их сегментов, выполняющих значимые функции, устанавливаются оператором (обладателем информации) 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.

Оператор (обладатель информации) должен проводить 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.

На период проведения работ по восстановлению функционирования информационных систем должна быть обеспечена возможность выполнения пользователями значимых функций, в том числе в неавтоматизированном режиме, в соответствии с внутренними регламентами.

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

состав значимые функции;

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 проведения 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.

3.14. Повышение уровня знаний и информированности пользователей по вопросам защиты информации

Цель: Снижение возможности реализации угроз безопасности

информации, связанных 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 информационных материалов, в том числе
в форме памяток, баннеров, буклетов, по актуальным вопросам защиты информации;

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

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

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

Должны быть определены категории работников, для которых проводится повышение 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 повышения уровня знаний и компетенций работников, а также привлекаемые для такого лица и используемые ими средства определяются
во внутренних регламентах.

При повышении уровня знаний и компетенций работников по вопросам защиты информации используются следующие способы:

доведение информационных материалов (памяток, баннеров, буклетов, иллюстраций);

проведение обучающих курсов в формах лекций, семинаров по вопросам защиты информации;

проведение обучающих игр по вопросам защиты информации;

проведение имитационных рассылок электронных писем на служебные адреса электронной почты с целью оценки устойчивости работников к методам социальной инженерии;

проведение тренировок с работниками по практической отработке

мероприятий 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 не реже одного раза в три года или после компьютерного инцидента, произошедшего у оператора (обладателя 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. Периодичность и формы тестирования работников определяются во внутренних регламентах.

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

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

подразделения (работники, категории работников), для которых требуется повышение уровня знаний и информированности пользователей по вопросам защиты информации;

применяемые способы повышения уровня знаний и компетенций работников по вопросам защиты информации, и условия их использования;

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

подразделение (работники), ответственное 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) разработка курсов для повышения уровня знаний и компетенций работников, организация периодического повышения уровня знаний и компетенций работников в соответствии разработанными курсами;

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

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

4) для работников, показавших по результатам тестирования неудовлетворительный уровень знаний и компетенций по вопросам защиты информации, организация повторного прохождения обучающих курсов по вопросам защиты информации;

5) для работников, нарушивших настоящие Требования, внутренние стандарты или регламенты, осуществление внеочередной проверки уровня знаний и компетенций.

3.15. Обеспечение защиты информации при взаимодействии с подрядными организациями

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.

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 подрядных организаций должны быть созданы отдельные учетные записи, соответствующие каждой подрядной организации, с правами доступа, минимально необходимыми для выполнения условий договора.

Подрядные организации должны осуществлять использование созданных для них учетных записей в соответствии с настоящими Требованиями, внутренними регламентами и стандартами.

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 сертифицированные 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, которые должны быть доведены до работников подрядных организаций в части, 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, которые должны быть изолированы от эксплуатируемых информационных систем оператора (обладателя информации). 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 информации осуществляется с использованием сертифицированных шифровальных (криптографических) средств защиты информации, обеспечивающих защиту каналов передачи данных.

Удаленный доступ подрядных организаций к информационным системам должен осуществляться только с сетевых адресов, закрепленных за автономными системами 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 настоящими Требованиями.

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, устанавливаются оператором.

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;

информационные системы, сегменты информационных систем, отдельные программно-аппаратные средства, стенды разработки и тестирования, категории информации, которым предоставляется доступ подрядным организациям;

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);

подразделение (работники), ответственные за контроль выполнения подрядными организациями требований по защите информации, и порядок проведения контроля.

Требования к усилению:

1) учетные записи подрядных организаций должны быть персонифицированы;

2) должно быть обеспечено централизованное управление учетными записями (группами учетных записей) подрядных организаций и их аутентификационной информацией. Доступ работников подрядных организаций к информационным системам оператора должен

осуществляться
с применением строгой аутентификации;

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

4) 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 с целью выявления нарушений требований внутренних регламентов по обращению с информацией ограниченного доступа.

3.16. Обеспечение защиты от компьютерных атак, направленных на отказ в обслуживании

Цель: Исключение возможности блокирования доступа к информационным системам и (или) содержащейся в них информации вследствие несанкционированных воздействий на интерфейсы, порты, сервисы, 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 (IP-адресов, протоколов, портов), 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 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 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 (GeoIP);

обеспечение хранения в течении трех лет информации о фактах реализации атак, направленных на отказ в обслуживании;

использование правил фильтрации, запрещающих пропуск всего трафика, т.е. от любого сетевого адреса источника и (или) сервиса к любому сетевому адресу назначения и (или сервиса), которые реализуют логику «все, что явно не разрешено – запрещено». Таким образом, правила фильтрации должны быть описаны максимально специфично и точно, не оставляя возможности пропуска пакетов по протоколам и сервисам, которые не используются информационной системой в соответствии с матрицей коммуникации;

анализ логической схемы сети с целью поиска узких мест на пути прохождения трафика и реализацию мер по увеличению ресурсов для обработки трафика и сетевых соединений минимум с двухкратным запасом от ожидаемого легитимного трафика.

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

Оператором (обладателем информации) должно быть обеспечено взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Оператором также должно быть обеспечено взаимодействие с Центром мониторинга и управления сетью связи общего пользования[7] при наличии такой возможности.

---

[7] Пункт 5 Положения о Центре мониторинга и управления сетью связи общего пользования, утвержденного приказом Роскомнадзора от 31 июля 2019 г. № 225

Мероприятия, предусмотренные настоящим пунктом, оператор (обладатель информации) реализует самостоятельно и (или) с привлечением провайдеров хостинга или организаций, предоставляющих услуги связи, 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 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 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 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, в том числе устанавливается время восстановления функционирования в случае нарушения штатного режима функционирования
в следствие 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;

2) организация надежного способа доставки очищенного трафика в случае привлечения организаций, оказывающих услуги по контролю,

---

(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).

фильтрации
и блокированию сетевых запросов, обладающих признаками компьютерных атак, направленных на отказ в обслуживании.

3.17. Обеспечение защиты информации при использовании искусственного интеллекта

Цель: Исключение возможности несанкционированного доступа к информации или воздействия на информационные системы, несанкционированного распространения и модификации информации, а также использования информационных систем не по их назначению за счет воздействия на обучающие данные, применяемые модели искусственного интеллекта
и их параметры, процессы и сервисы по обработке данных и поиску решений.

Требования к реализации:

Посредством проведения мероприятий по обеспечению защиты информации при использовании для функционирования информационных систем искусственного интеллекта[8] должна быть исключена возможность нарушения конфиденциальности, целостности и доступности информации, обрабатываемой
в системе искусственного интеллекта, за счет действий внешних и внутренних нарушителей безопасности информации.

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

В информационной инфраструктуре подрядной организации, используемой для разработки и (или) предоставления операторам систем искусственного интеллекта в качестве внешнего сервиса, должны быть реализованы мероприятия и меры по защите информации, установленные настоящими Требованиями по классу защищенности не ниже класса защищенности информационной системы оператора (обладателя информации).

Взаимодействие информационной системы оператора (обладателя информации) с информационной инфраструктурой подрядной организации,

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

используемой для предоставления системы искусственного интеллекта в качестве сервиса, должно осуществляться с учетом настоящих Требований.

При внедрении 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.

В случае применения систем искусственного интеллекта в качестве внешнего сервиса, оператор информационной системы должен установить требования к подрядной организации по оценке угроз системы искусственного интеллекта, связанных с разработкой и (или) эксплуатацией системы искусственного интеллекта.

Угрозы безопасности информации систем искусственного интеллекта должны рассматриваться в отношении следующих объектов защиты информации:

программное обеспечение, обеспечивающее разработку и реализацию технологии искусственного интеллекта;

входная модель машинного обучения (при наличии);

наборы обучающих данных;

выходная модель машинного обучения и ее параметры (веса).

В отношении указанных объектов защиты информации должны быть приняты меры по защите технологии искусственного интеллекта.

В случае самостоятельной разработки оператором (обладателем информации) программного обеспечения, обеспечивающего реализацию технологии искусственного интеллекта, должны быть реализованы меры, предусмотренные разделами 4 и 5 ГОСТ Р 56939-2024.

В случае привлечения оператором (обладателем информации) для разработки программного обеспечения подрядной организации по решению руководителя (ответственного лица) в техническое задание на разработку программного обеспечения могут быть включены требования по разработке безопасного программного обеспечения в соответствии с ГОСТ Р 56939-2024.

В отношении программного обеспечения, обеспечивающего реализацию технологии искусственного интеллекта, должны быть проведены анализ уязвимостей и проверки на отсутствие недекларированных возможностей в соответствии с методическими документами, утвержденными 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: Не предъявляются.

3.18. Проведение периодического контроля уровня защищенности информации, содержащейся в информационных системах

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 одним или совокупностью следующих методов:

автоматизированное и (или) ручное 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 организационных мер и применяемых средств защиты информации;

выявление несанкционированных подключений устройств к информационным системам.

Периодичность и методы контроля уровня защищенности информации устанавливаются оператором во внутренних регламентах в соответствии с имеющимися у него силами и выделенными на эти цели средствами. При этом проведение контроля уровня защищенности информации одним из способов должно проводиться не реже чем один раз в год.

Руководство работами по контролю уровня защищенности информации осуществляет ответственное лицо оператора. Контроль уровня защищенности информации проводится структурным подразделением, специалистами по защите информации самостоятельно или с привлечением специализированных организаций, имеющих лицензии ФСТЭК России на деятельность по технической конфиденциальной защите информации (с правом оказания услуг по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации)[9].

В случае выявления по результатам контроля уровня защищенности

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

информации возможности реализации актуальных угроз и (или) признаков реализации актуальных угроз, структурным подразделением, специалистами
по защите информации совместно с подразделением, работниками, обеспечивающими функционирование информационных систем, осуществляется разработка и реализация мер, направленных на оперативное их блокирование.

По результатам контроля уровня защищенности информации структурным подразделением, специалистами по защите информации или специализированной организацией, проводившей работы по контролю уровня защищенности информации, разрабатывается отчет, который подписывается лицами, проводившими контроль. Отчет должен содержать наименование информационных систем, которые были охвачены мероприятиями по контролю уровня защищенности информации, время и место проведения контроля, перечень участников контроля, методы контроля, актуальные угрозы, возможность реализация которых оценивалась, результаты оценки возможности реализации актуальных угроз, рекомендации по повышению уровня защищенности информации.

Отчет об оценке должен быть представлен руководителю оператора для принятия им решения о необходимости выделения дополнительных ресурсов с целью повышения уровня защищенности информации.

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

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

подразделение (работники), ответственные за организацию и проведение контроля уровня защищенности информации, содержащейся в информационных системах;

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;

действия 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 одним

из способов должно проводиться не реже чем один раз в год;

2) проведение в соответствии с едиными замыслом и планом тренировок
по отработке работниками оператора действий по обеспечению требуемого уровня защищенности информации, содержащейся в информационных системах, в условиях реализации актуальных угроз.

4. 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, входящих в состав информационной системы (далее – внутренние пользователи).

К внутренним пользователям относятся работники оператора (привилегированные и непривилегированные пользователи, администраторы), выполняющие свои обязанности (функции) с использованием информации, информационных технологий и средств вычислительной техники информационной системы в соответствии с регламентами (инструкциями), утвержденными
в информационной системе, и которым в информационной системе присвоены учетные записи.

В качестве внутренних пользователей также рассматриваются работники обладателя информации, заказчика, уполномоченного лица и (или) оператора иной информационной системы, а также лица (подрядные организации), привлекаемые
на договорной основе для обеспечения функционирования информационной системы (ремонт, гарантийное обслуживание, регламентные и иные работы) 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 входящих в состав иных информационных систем,

соответствующих требованиям по защите информации или требованиям по защите информации, установленным оператором информационной системы (далее – внешние пользователи).

К внешним пользователям относятся все пользователи информационной системы, не указанные в качестве внутренних пользователей. 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.

Внутренние и внешние 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 УПД.10.

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 и процессах, запускаемых от имени этих пользователей, а также присвоение пользователю и (или) процессу идентификатора доступа и его регистрацию в перечне присвоенных идентификаторов. Первичная идентификация пользователя должна проводиться один раз в момент установления личности физического или юридического 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 актуализироваться и обновляться при изменении идентификационных данных пользователей (например, при смене фамилии, при изменении номера мобильного телефона, если он используется для целей дополнительной идентификации пользователя).

Вторичная идентификация должна включать проверку предъявленного пользователем идентификатора по списку зарегистрированных идентификаторов в информационной системе и распознавание пользователя. При положительном результате проверки должен производиться переход к аутентификации пользователя в информационной системе, при отрицательном случае — отказ в доступе.

Вторичная идентификация является многократно повторяющимся процессом, осуществляющимся каждый раз при новом запросе пользователя
на доступ к ресурсам информационной системы.

Требования к первичной и вторичной аутентификации пользователей приведены в разделе 5 национального стандарта ГОСТ Р 58833-2020 «Защита информации. Идентификация и аутентификация. Общие положения».

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 УПД.10.

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

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
и (или) устройства в течение установленного оператором периода времени;

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, средств защиты информации от несанкционированного доступа, а также средств и систем, предназначенных для автоматизации и аналитической поддержки деятельности по защите информации. Реализация меры по идентификации устройств достигается применением одного или совокупности программных, программно-аппаратных средств.

Требования к документированию: Внутренний стандарт, устанавливающий требования к первичной идентификации лиц, обладающих правами доступа к информационным системам и (или) содержащейся в них информации и их использованию (пользователей), должен определять требования к реализации первичной и вторичной идентификации пользователей, предусматривающие определение:

перечня видов пользователей (пользователи, системные администраторы, администраторы безопасности, подрядные организации и другие виды пользователей);

состава идентификационных данных для каждого вида пользователей минимально необходимого для однозначной идентификации пользователей;

перечня исключений и порядка действий в случае, если объем идентификационных данных устройства недостаточен;

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

порядка привязки идентификационной информации к пользователю;

правил хранения, поддержания актуального состояния (обновления) идентификационной информации пользователей, периодичности обновления (актуализации), мест их хранения, организации доступа к ним;

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

порядка действий оператора информационной системы по

идентификации пользователей.

Во внутреннем порядке предоставления доступа работникам подрядных организаций доступа к информационным системам, содержащейся в них информации, и (или) передачи им информации, контроля за таким доступом, передачей в случае привлечения подрядных организаций, а также внутреннем порядке предоставления работникам иных государственных органов, организаций доступа к информационным системам, содержащейся в них информации и (или) передачи им информации и контроля за такими доступом, передачей (в случае информационного взаимодействия с иными государственными органами, организациями) должен быть предусмотрен порядок идентификации внешних пользователей, которым разрешен доступ к информационной системе оператора.

Требования к усилению:

1) В информационной системе должно быть исключено использование идентификатора пользователя информационной системы при создании учетной записи пользователя публичной электронной почты или иных публичных сервисов;

2) В информационной системе должно быть обеспечено управление идентификаторами внешних пользователей, учетные записи которых используются для доступа к общедоступным ресурсам информационной системы;

3) В информационной системе должно быть реализовано централизованное управление идентификаторами.

Реализация в информационной системе:

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

ИАФ.2 Идентификация устройств

Цель: Предоставление доступа к информационным системам и содержащейся в них информации идентифицированным устройствам (программно-аппаратным средствам).

Требования к реализации: В информационной системе должен быть определен перечень типов устройств (сервера, автоматизированные рабочие места, телекоммуникационное оборудование, мобильные устройства, системы хранения данных, машинные носителей информации, средства защиты информации и другие устройства), используемых в информационной системе

и подлежащих идентификации до начала информационного взаимодействия.

Идентификации подлежат:

устройства, входящие в состав информационной системы;

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

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

устройства, предназначенные для удаленного доступа работников 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[10] и вторичная идентификация[8].

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 и (или) с установленной периодичностью для актуализации (обновления) идентификационной информации, либо по мере необходимости ее изменения.

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

---

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

присвоенных идентификаторов процесс вторичной идентификации считается успешно пройденным, затем проводится аутентификация устройств (мера ИАФ.3).

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

Идентификация устройств обеспечивается применением входящих в состав информационной системы операционной системы, средств защиты информации от несанкционированного доступа, а также программных и программно-аппаратных средств контроля настроек и конфигураций информационных систем, а также средств и системам, предназначенными для автоматизации и аналитической поддержки деятельности по защите информации. Реализация меры по идентификации устройств достигается применением одного или совокупности программных, программно-аппаратных средств.

Требования к документированию: Внутренний стандарт к типовым конфигурациям и настройкам программных, программно-аппаратных средств должен устанавливать требования к реализации первичной и вторичной идентификации устройств, предусматривающие определение:

перечня типов устройств (сервер, монитор, коммутатор, съемный машинный носитель и другие типы устройств);

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

перечня исключений и порядка действий в случае, если объем идентификационных данных устройства недостаточен;

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

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

правил хранения, поддержания актуального состояния (обновления) идентификационной информации устройств, периодичности обновления (актуализации), мест их хранения, организации доступа к ним;

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

порядка действий оператора информационной системы по идентификации устройств.

Во внутреннем порядке предоставления доступа работникам подрядных организаций доступа к информационным системам, содержащейся в них информации, и (или) передачи им информации, контроля за таким доступом, передачей в случае привлечения подрядных организаций, а также внутреннем порядке предоставления работникам иных государственных органов, организаций доступа к информационным системам, содержащейся в них информации и (или) передачи им информации и контроля за такими доступом, передачей (в случае информационного взаимодействия с иными государственными органами, организациями) должен быть предусмотрен порядок идентификации устройств внешних пользователей, с которых разрешен доступ к информационной системе оператора.

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) для информационных систем с доверенной 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);

5) реализация 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.2	+	+	+
Усиление ИАФ.2	2	2	1

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.

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

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 УПД.10.

Аутентификация пользователя осуществляется с использованием паролей, аппаратных средств, биометрических характеристик, иных средств или в случае многофакторной (двухфакторной) аутентификации – определенной комбинации данных средств, указанных в разделе 5 национального стандарта ГОСТ Р 58833-2020 «Защита информации. Идентификация и аутентификация. Общие положения».

В информационной системе должны обеспечиваться:

однофакторная аутентификация для локального доступа в информационную систему непривилегированных пользователей;

многофакторная (двухфакторная) усиленная аутентификация для удаленного доступа в информационную систему непривилегированных пользователей;

многофакторная (двухфакторная) для локального доступа в информационную систему привилегированных пользователей;

строгая аутентификация для удаленного доступа в информационную систему привилегированных пользователей, а в случае технической невозможности применения строгой аутентификации — использование усиленной многофакторной аутентификации;

строгая аутентификация для локального и удаленного доступа в информационную систему пользователей с мобильных устройств.

При усиленной аутентификации удаленных пользователей должна применяться двух- или трехфакторная взаимная аутентификация с организацией двустороннего обмена аутентификационной информацией между пользователем и объектом доступа.

При доступе в информационную систему с использованием каналов связи, имеющих выход за пределы контролируемой зоны, беспроводных каналов связи и (или) при доступе в информационную систему с использованием мобильных устройств должна обеспечиваться двусторонняя аутентификация, предусматривающая обоюдную проверку подлинности как субъекта доступа, осуществляющего доступ в информационную систему так и сервиса информационной системы, к которому осуществляется доступ или устройства информационной системы, установленного в точке доступа в информационную систему.

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.

После прохождения аутентификации в информационной системе для аутентификации в прикладном программном обеспечении (например, системах электронного документооборота, сервисах электронной почты, системах управления базами данных), средствах вычислительной техники должна обеспечиваться однофакторная аутентификация.

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. Аутентификационная информация встроенных привилегированных учетных записей должна быть изменена в соответствии с внутренними стандартами и регламентами по защите информации.

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:

определение работника оператора, ответственного за хранение, выдачу, инициализацию, блокирование аутентификаторов и принятие мер в случае утраты и (или) компрометации аутентификаторов;

изменение аутентификационной информации (аутентификаторов),

заданных их производителями и (или) используемых при внедрении системы защиты информации информационной (автоматизированной) системы;

выдачу аутентификаторов пользователям;

генерацию и выдачу начальной аутентификационной информации (начальных значений аутентификаторов);

установление характеристик пароля (при использовании в информационной (автоматизированной) системе механизмов аутентификации на основе пароля):

задание минимальной сложности пароля с определяемыми оператором требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистров, цифр и специальных символов;

задание минимального количества измененных символов при создании новых паролей;

задание максимального времени действия пароля;

задание минимального времени действия пароля;

запрет на использование пользователями определенного оператором числа последних использованных паролей при создании новых паролей;

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

назначение необходимых характеристик аутентификаторов (в том числе механизма пароля);

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

защиту аутентификационной информации от неправомерного доступа к ней и модифицирования.

В информационной системе должно быть исключено использование технологии аутентификации с сохранением аутентификационных данных в открытом виде в памяти средств вычислительной техники.

В информационной системе должны быть:

определены меры, исключающие возможность передачи аутентификационной информации в открытом виде по каналам связи и ввода аутентификационной информации при выполнении процедур, не связанных с аутентификацией в информационной системе.

определены меры, обеспечивающие защиту аутентификационной информации от несанкционированного доступа при ее хранении на машинных носителях информации.

Осуществлена защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

Защита обратной связи «система-пользователь» в процессе 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.

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

Требования к документированию: Внутренний регламент, устанавливающих порядок создания, учета, изменения и блокирования, контроля, удаления учетных записей, а также внутренний регламент, устанавливающих порядок создания, учета, изменения и блокирования, контроля, удаления привилегированных учетных записей, должны определять:

состав аутентификационной информации для каждого вида пользователей минимально необходимый для однозначной идентификации пользователей;

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

порядок привязки аутентификационной информации к пользователю;

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

Внутренний регламент, устанавливающий порядок создания, изменения, блокирования, контроля, удаления аутентификационной информации и средств аутентификации, должен определять:

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

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

Требования к усилению:

1) в случае использования в информационной (автоматизированной) системе механизмов аутентификации на основе пароля (иной

последовательности символов, используемой для аутентификации) или применения пароля в качестве одного из факторов многофакторной аутентификации, его характеристики должны быть следующими:

а) длина пароля не менее десяти символов, алфавит пароля не менее 30 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 3 до 15 минут, смена паролей не более чем через 120 дней;

б) длина пароля не менее десяти символов, алфавит пароля не менее 60 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 5 до 30 минут, смена паролей не более чем через 120 дней;

в) длина пароля не менее десяти символов, алфавит пароля не менее 70 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 5 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 10 до 30 минут, смена паролей не более чем через 90 дней;

2) в информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация при доступе в систему с правами привилегированных пользователей, где один из факторов обеспечивается аппаратным устройством аутентификации, отделенным от информационной (автоматизированной) системы, к которой осуществляется доступ;

3) в информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация при доступе в систему с правами непривилегированных пользователей, где один из факторов обеспечивается устройством, отделенным от информационной системы, к которой осуществляется доступ;

4) в информационной системе должен использоваться механизм одноразовых паролей при аутентификации пользователей, осуществляющих удаленный или локальный доступ;

5) процесс строгой аутентификации должен быть организован с применением корпоративного (отраслевого) центра сертификации в

качестве доверенной третьей стороны;

6) в информационной системе должна обеспечиваться двусторонняя аутентификация, предусматривающая проверку подлинности взаимодействующих с ней сервисов иных информационных систем;

7) в информационной системе проверка подлинности взаимодействующих
с ней сервисов иных информационных систем должна осуществляться с участием третьей стороны, которой доверяют взаимодействующие стороны;

8) защита аутентификационной информации должна предусматривать передачу взамен аутентификационной информации субъекта доступа сгенерированной проверяющей стороной информации, преобразованной (маскированной) с использованием аутентификационной информации субъекта доступа;

9) защита аутентификационной информации обеспечивается применением
в соответствии с законодательством Российской Федерации криптографических методов защиты информации;

10) в информационной (автоматизированной) системе должен использоваться механизм одноразовых паролей при аутентификации пользователей, осуществляющих удаленный или локальный доступ;

11) в информационной (автоматизированной) системе должно быть обеспечено использование автоматизированных средств для формирования аутентификационной информации (генераторов паролей) с требуемыми характеристиками стойкости (силы) механизма аутентификации и для оценки характеристик этих механизмов;

12) в информационной (автоматизированной) системе должно быть обеспечено использование серверов и (или) программного обеспечения аутентификации для единой аутентификации в компонентах информационной (автоматизированной) системы и компонентах программного обеспечения, предусматривающего собственную аутентификацию;

13) в информационной системе должно быть обеспечено получение (запрос)
у поставщика технических средств и программного обеспечения информационной (автоматизированной) системы аутентификационной информации, заданной производителем этих технических средств и программного обеспечения
и не указанной в эксплуатационной документации;

14) в информационной системе должны быть определены меры

по исключению возможности использования пользователями их идентификаторов и паролей в других информационных (автоматизированных) системах;

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

16) в информационной системе должна применяться система централизованного управления аутентификаторами (аутентификационной информацией) пользователей;

17) в информационной системе должна применяться система централизованного управления аутентификаторами (аутентификационной информацией) привилегированных пользователей.

18) в информационной (автоматизированной) системе для аутентификации пользователей должно обеспечиваться применение в соответствии
с законодательством Российской Федерации криптографических методов защиты информации.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ИАФ.3	+	+	+
Усиление ИАФ.3	1а	1б	1в, 2, 6, 14

ИАФ.4 Аутентификация устройств

Цель: Предоставление доступа к информационным системам и содержащейся в них информации устройствам (программно-аппаратных средствам), в отношении которых проведена процедура 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 должен быть определен способ аутентификации устройств и применяемые протоколы аутентификации. В процессе аутентификации устройств должны использоваться

поддерживаемые ими протоколы аутентификации (например, EAP, 802.1x, CMP, SCEP, 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 идентификации устройств достигается применением одного или совокупности программных, программно-аппаратных средств.

Требования к документированию: внутренний стандарт к типовым конфигурациям и настройкам программных, программно-аппаратных средств должен устанавливать требования к реализации аутентификации устройств, предусматривающие определение:

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

способов аутентификации устройств;

действий администратора по настройке и контролю функционирования способов аутентификации устройств;

действий администраторов информационной системы в случае утери, поломки, вывода устройств из эксплуатации и (или) компрометации аутентификационной информации устройств;

правил и процедур управления средствами аутентификации устройств;

мониторинга и аудита действий администраторов и пользователей, связанных с обслуживанием и жизненным циклом аутентификационной информации и средств аутентификации;

процедур и регламентов эксплуатации системы централизованного управления (при ее наличии).

Во внутреннем порядке предоставления работникам подрядных организаций доступа к информационным системам, содержащейся в них информации и (или) передачи им информации, контроля за таким доступом, передачей в случае привлечения подрядных организаций, а также внутреннем порядке предоставления работникам иных государственных органов, организаций доступа к информационным системам, содержащейся в них информации и (или) передачи им информации и контроля за таким доступом, передачей (в случае информационного взаимодействия с иными государственными органами, организациями) должен быть предусмотрен порядок аутентификации устройств внешних пользователей, с которых разрешен доступ к информационной системе оператора.

Требования к усилению:

1) смена аутентификационных данных устройств не реже чем один раз

в два года для информационных систем 1 класса защищенности;

2) смена аутентификационных данных устройств не реже чем один раз в три года для информационных систем 2 и 3 классов защищенности;

3) реализация аутентификации с использованием MAC-адресов устройств;

4) реализация аутентификации с использованием криптографических протоколов аутентификации;

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

6) реализация 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	2, 3	2, 4	1, 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 разработана модель управления доступом, формализующая методы управления доступом, типы доступа субъектов к объектам доступа и правила разграничения доступа субъектов доступа к объектам доступа, реализуемые в информационной системе.

В информационной системе должны быть определены используемый в информационной системе метод управления доступом или комбинация следующих методов:

дискреционный метод управления доступом;

ролевой метод управления доступом;

мандатный метод управления доступом;

атрибутный метод управления доступом.

В информационной системе в модели управления доступом необходимо определить:

типы субъектов и объектов доступа (например, пользователи,

устройства, приложения (процессы), файлы и иные субъекты и объекты доступа);

типы учетных записей 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 (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);

перечни субъектов и объектов доступа в информационной системе;

правила разграничения доступа субъектов доступа к объектам доступа в информационной системе в соответствии с заданными типами доступа.

В информационной системе должны быть реализованы модели управления доступом за счет применения в информационной системе сертифицированных операционных систем, систем управления базами данных, средств виртуализации, средств контейнеризации, средств доверенной загрузки, иных сертифицированных средств защиты информации.

Требования к документированию: Внутренний стандарт, содержащий требования к применяемой модели доступа, должен устанавливать требования к реализации модели управления доступом, предусматривающие определение:

используемых методов доступа;

типов субъектов и объектов доступа;

типов учетных записей субъектов доступа;

типов доступа субъектов к объектам доступа

перечней субъектов и объектов доступа;

правил разграничения доступа (матрицы доступа) субъектов доступа к объектам доступа;

средств защиты информации, реализующих правила разграничения доступа.

Требования к усилению:

1) 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;

2) модель управления доступом должна учитывать особенности моделей доступа, применяемых в составляющих информационную систему сертифицированных операционных системах, системах управления базами данных, средствах виртуализации, средствах контейнеризации, иных

средствах защиты информации;

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

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

5) модель управления доступом должна быть представлена в формализованном виде, позволяющем однозначно идентифицировать субъекты, объекты и правила доступа.

Реализация в информационной системе:

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

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 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.

Требования к документированию: Внутренний стандарт, устанавливающий ограничения и запреты действий для пользователей при использовании и обеспечении эксплуатации ими информационных систем, должен определять:

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 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;

2) 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;

3) 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;

4) 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;

5) в информационной системе должен быть определен привилегированный пользователь (администратор-супервизор), 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, 2	1, 2, 3	1, 2, 3, 4

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 (проверка 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 автоматизированные средства поддержки управления учетными записями пользователей.

Требования к документированию: Внутренний стандарт, устанавливающий порядок создания, учета, изменения и блокирования, контроля, удаления учетных записей, должен определять порядок:

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

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

Внутренний стандарт, устанавливающий порядок создания, учета, изменения и блокирования, контроля, удаления привилегированных учетных записей, должен определять порядок, определенный внутренним стандартом, устанавливающим порядок создания, учета, изменения и блокирования, контроля, удаления учетных записей, в отношении привилегированных учетных записей. Дополнительно внутренний стандарт должен определять:

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 выявленные нарушения;

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;

3) в информационной системе должен быть реализован анализ журналов регистрации событий безопасности, связанных с управлением учетными записями, с целью выявления нарушений и событий безопасности информации и реагирования на выявленные нарушения.

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 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: Внутренние стандарты, устанавливающие порядок создания, учета, изменения и блокирования, контроля, удаления учетных записей непривилегированных и привилегированных пользователей, должны определять:

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) конкретных типов 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 учетных записей в случае неуспешных попыток аутентификации от имени учетной записи и иных определенных в информационной системе событий безопасности, а также оповещение о данном событии привилегированного пользователя (администратора), отвечающего
за управление и контроль над учетными записями пользователей;

2) 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;

3) при доступе в информационную систему должно обеспечиваться противодействие автоматизированному подбору паролей с использованием однократных кодов, требующих визуального распознавания (в том числе с использованием технологии CAPTCHA);

4) в информационной системе должна быть обеспечена реализация автоматического блокирования учетных записей в случае неуспешных попыток аутентификации от имени учетной записи в нештатное (нерегламентированное) время;

5) разблокирование доступа привилегированных субъектов доступа, превысивших число неуспешных попыток доступа в информационную систему, может выполняться только привилегированным пользователем информационной системы (администратором);

6) признаки, характеризующие субъект доступа, осуществляющий неуспешные попытки получения доступа в информационную систему (например, IP-адрес, сигнатуры сведений о пользовательском агенте), должны быть переданы в систему обнаружения вторжений (компьютерных атак).

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
УПД.4	+	+	+
Усиление УПД.4		1, 3, 5	1, 2, 3, 4, 5, 6

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 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 ИАФ.1 — ИАФ.4.

Оповещение должно содержать информацию о как минимум 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: Эксплуатационная документация оператора (обладателя информации) информационной системы должна содержать следующие сведения:

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 информации) 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	1	1, 2, 5, 6	1, 2, 4, 5, 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: Внутренние стандарты, устанавливающие порядок создания, учета, изменения и блокирования, контроля, удаления учетных записей непривилегированных и привилегированных пользователей, должны определять:

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) от их имени с разных устройств
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 устройствам отображения, кроме необходимых для разблокирования сеанса.

Разблокирование сеанса доступа субъекта доступа в

информационную систему должно осуществляться после повторной аутентификации,
в соответствии с мерами ИАФ.1 — ИАФ.4.

Требования к документированию: Внутренние стандарты, устанавливающие порядок создания, учета, изменения и блокирования, контроля, удаления учетных записей непривилегированных и привилегированных пользователей, должны определять:

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;

значения минимального времени до момента возможности разблокирования сеанса после его блокирования;

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

Требования к усилению:

1) в информационной системе на устройстве отображения (мониторе) после блокирования сеанса не должна отображаться информация сеанса субъекта доступа;

2) разблокирование должно осуществляться с использованием ввода второго фактора при использовании многофакторной аутентификации в составе информационной системы в соответствии с мерами ИАФ.1 — ИАФ.4;

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

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

5) в информационной системе должна осуществляться регистрация событий превышения установленного оператором допустимого числа неуспешных попыток разблокирования доступа.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
УПД.8	+	+	+
Усиление УПД.8	1, 3, 4	1, 2, 3, 4, 5	1, 2, 3, 4, 5

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 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 аутентификации и идентификации, 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: Внутренний стандарт, устанавливающий ограничения и запреты действий для пользователей при использовании и обеспечении эксплуатации ими информационных систем,

должен определять:

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;

перечень случаев, когда привилегированному пользователю разрешается выполнять действия в обход процедур идентификации и аутентификации (например, восстановление работоспособности системы при сбоях или отказах компонентов системы), и описание механизмов контроля таких действий;

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.

В первоочередном порядке 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 распространения;

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

на интерфейсах информационной системы, 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, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

В информационной системе как минимум подлежат регистрации следующие события:

вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (остановки) операционной системы;

подключение машинных носителей информации и вывод информации на носители информации;

запуск (завершение) программ и процессов (заданий, задач), 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, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;

попытки удаленного доступа.

Зарегистрированная информация о событиях безопасности должна

передаваться в средства мониторинга событий информационной безопасности.

Требования к документированию: Внутренний стандарт, содержащий требования к сбору, регистрации и анализу событий безопасности, должен устанавливать 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 централизованное управление записями регистрации 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.

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: Осуществить анализ результатов регистрации событий безопасности
и реагирование на них.

Требования к реализации: Анализ записей регистрации должен проводиться для всех событий, подлежащих регистрации в соответствии с

мерой РСБ.1, с периодичностью, установленной оператором и обеспечивающей своевременное выявление признаков инцидентов безопасности в информационной системе.

В случае выявления признаков инцидентов безопасности в информационной системе осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности.

Требования к документированию: Внутренние стандарты по защите информации, содержащие в том числе перечень событий, подлежащих анализу, периодичность проведения анализа событий безопасности, а также перечень мероприятий по реагированию на выявленные инциденты безопасности.

Требования к усилению:

1) в информационной системе должны обеспечиваться интеграция 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).

Реализация в информационной системе:

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

РСБ.3 Генерация временных меток при регистрации событий безопасности

Цель: Осуществить генерацию надежных меток времени и (или) синхронизацию системного времени.

Требования к реализации: В информационной системе должно обеспечиваться получение меток времени, включающих дату и время,

используемых при генерации записей регистрации событий безопасности.

Генерация временных меток при регистрации событий безопасности достигается посредством применения внутренних системных часов информационной системы.

Требования к документированию: Внутренний стандарт, содержащий требования к сбору, регистрации и анализу событий безопасности, должен устанавливать требования к генерации надежных меток времени при регистрации событий безопасности, предусматривающие определение правил и процедур генерации надежных меток времени.

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

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 данных о событиях безопасности в течение установленного оператором времени хранения информации о событиях безопасности и защиты данных о событиях безопасности от несанкционированного доступа к ним.

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 в течение установленного времени хранения должны предусматривать:

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

генерацию (сбор, запись) записей регистрации для 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 информации, регистрируемых в информационной системе. Защита информации о событиях безопасности обеспечивается путем реализации следующих мер защиты информации:

обеспечение целостности событий безопасности, регистрируемых в информационной системе;

предоставление доступа к журналам регистрации событий безопасности уполномоченным работникам оператора, прошедшим процедуру идентификации
и аутентификации;

управление доступом уполномоченных работников оператора к местам хранения сведений о событиях безопасности, в том числе исключение возможности их уничтожения или изменения.

Требования к документированию: Внутренний стандарт, содержащий требования к сбору, регистрации и анализу событий безопасности, должен устанавливать требования к:

определению событий безопасности, подлежащих регистрации в заданный момент времени из перечня событий безопасности, определенных в соответствии
с мерой РСБ.1;

порядку хранения сведений о событиях безопасности, в том числе к местам хранения сведений о событиях безопасности и периоду времени хранения информации о событиях безопасности;

мерам защиты 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 записей системных журналов и записей о событиях безопасности в обособленном хранилище, физически отделенном от 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		1	1, 3

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: Внутренний стандарт, содержащий

требования к сбору, регистрации и анализу событий безопасности, должен устанавливать требования к правилам и процедурам реагирования на сбои при регистрации событий безопасности.

Требования к усилению:

1) в информационной системе обеспечивается выдача предупреждения администратору при заполнении установленной оператором части (процент или фактическое значение) объема памяти для хранения информации о событиях безопасности;

2) в информационной системе обеспечивается выдача предупреждения администратору в масштабе времени, близком к реальному, при наступлении критичных сбоев в механизмах сбора информации, определенных в информационной системе;

3) в информационной системе обеспечивается 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			1, 2

4.4. Защита виртуализации и облачных технологий (ЗСВ)

ЗСВ.1 Доверенная загрузка средства виртуализации и виртуальных машин

Цель: Контроль целостности средства 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 и блокировка загрузки виртуальных машин, состав и настройки виртуального оборудования которых содержат несанкционированные изменения.

Указанные меры защиты информации реализуются за счет применения в информационной системе сертифицированных базовых систем ввода-

вывода или средств доверенной загрузки, а также хостовых операционных систем и средств виртуализации.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должны обеспечиваться выявление и 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 известные уязвимости и 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, устанавливаемых администратором 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 средства виртуализации и виртуальных машин

Цель: Контроль целостности средства 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 сертифицированных средств виртуализации.

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) должны обеспечиваться выявление и блокировка запуска компонентов программного обеспечения хостовой операционной системы и средства виртуализации, целостность которых нарушена;

4) должна обеспечиваться целостность сведений о событиях безопасности;

5) 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);

6) 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, 3, 4

ЗСВ.3 Регистрация событий безопасности в среде виртуализации

Цель: Регистрация событий безопасности в среде виртуализации.

Требования к реализации: При применении средств виртуализации должна обеспечиваться в соответствии с мерами 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 ролевой модели;

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 сертифицированных средств виртуализации и (или) средств управления событиями безопасности.

Требования к документированию: Требования к регистрации событий безопасности средств виртуализации должны быть включены во внутренний стандарт, устанавливающий требования к сбору, регистрации и анализу событий, связанных с возможным нарушением безопасности информации, нарушением функционирования информационных систем, реализацией угроз безопасности информации.

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: Управление доступом в среде виртуализации.

Требования к реализации: Должны обеспечиваться меры по управлению доступом пользователей в среде виртуализации в соответствии с мерами

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 сертифицированных средств виртуализации.

Требования к документированию: Модель управления доступом в среде виртуализации должна быть включена во внутренний стандарт «Требования
к применяемым моделям доступа пользователей».

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: Резервное копирование в среде виртуализации.

Требования к реализации: При применении средств виртуализации должно обеспечиваться резервное копирование:

образов виртуальных машин;

конфигураций виртуального оборудования виртуальных машин;

Указанные меры защиты информации реализуются за счет применения
в информационной системе сертифицированных средств виртуализации, хостовых операционных систем и (или) средств резервного копирования.

Требования к документированию: Порядок реализации резервного копирования должен содержаться во внутреннем стандарте, устанавливающем требования к резервному копированию информации, программного обеспечения
и его конфигураций.

Требования к усилению:

1) должно обеспечиваться резервное копирование параметров настройки средств виртуализации;

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		1	1, 2

ЗСВ.6 Ограничение программной среды в среде виртуализации

Цель: Блокирование несанкционированного запуска программного обеспечения в среде виртуализации.

Требования к реализации: Должны обеспечиваться выявление и блокировка 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 сертифицированных средств виртуализации и (или) хостовых операционных систем.

Требования к документированию: Перечень программного обеспечения, разрешенного в среде виртуализации, должны быть включены во внутренний стандарт, устанавливающий перечень разрешенного и (или) запрещенного для использования программного обеспечения.

Требования к усилению:

1) должна обеспечиваться блокировка запуска компонентов программного обеспечения хостовой операционной системы и средства виртуализации, не прошедших аутентификацию с использованием свидетельств подлинности.

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, использованной для хранения данных виртуальных машин, при ее освобождении или перераспределении.

Указанные меры защиты информации реализуются за счет применения в информационной системе сертифицированных средств виртуализации и (или) хостовых операционных систем.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) удалять объекты файловой системы, используемые средством виртуализации, путем многократной перезаписи уничтожаемых (стираемых) объектов файловой системы специальными битовыми последовательностями.

2) изолировать области памяти виртуальных машин путем применения механизмов управления памятью аппаратной платформы.

3) контролировать целостность 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: Идентификация и аутентификация объектов доступа и субъектов доступа в среде виртуализации.

Требования к реализации: Должна обеспечиваться идентификация и аутентификация субъектов доступа в среде виртуализации в соответствии с мерами ИАФ.1 — ИАФ.4, в том числе:

разработчиков виртуальных машин;

администраторов безопасности средств виртуализации;

администраторов средств виртуализации;

администраторов виртуальных машин;

администраторов хостовых операционных систем;

администраторов средств вычислительной техники, входящих в состав виртуальной инфраструктуры.

Должна обеспечиваться идентификация объектов доступа в соответствии
с мерами ИАФ.1 — ИАФ.4, в том числе:

виртуальных машин;

средств виртуализации;

средств вычислительной техники, входящих в состав виртуальной инфраструктуры.

Указанные меры защиты информации реализуются за счет применения в информационной системе сертифицированных средств виртуализации и (или) хостовых операционных систем.

Требования к документированию: Порядок идентификации и аутентификации объектов и субъектов доступа в среде виртуализации должен быть определен во внутреннем регламенте, устанавливающем порядок создания, изменения, блокирования, контроля, удаления аутентификационной информации и средств аутентификации.

Требования к усилению: Не предъявляются.

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);

управление размещением и перемещением исполняемых виртуальных машин между серверами виртуализации;

управление размещением и перемещением данных, обрабатываемых с использованием виртуальных машин, между носителями (системами хранения данных).

Управление перемещением виртуальных машин и обрабатываемых на

них данных должно обеспечивать перемещение виртуальных машин и обрабатываемых
на них данных только с применением технических средств, входящих в состав информационной системы.

Указанные меры защиты информации реализуются за счет применения в информационной системе сертифицированных средств виртуализации и (или) хостовых операционных систем.

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)

ЗКС.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.

Указанные меры защиты информации реализуются за счет применения
в информационной системе сертифицированных средств контейнеризации и хостовых операционных систем.

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) должны обеспечиваться выявление и блокировка запуска компонентов программного обеспечения хостовой операционной системы и средства контейнеризации, целостность которых нарушена;

4) должна обеспечиваться целостность сведений о событиях безопасности, регистрируемых средством контейнеризации;

5) 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;

6) 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);

7) должны обеспечиваться выявление и блокировка запуска образа контейнера, целостность которого нарушена.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКС.1	+	+	+
Усиление ЗКС.1		1, 2	1, 2, 3, 4, 5, 6, 7

ЗКС.2 Регистрация событий безопасности в контейнерных средах

Цель: Обеспечение информирования администраторов информационной системы и администраторов безопасности информационной системы о событиях безопасности, связанных с применением контейнерных сред, а также расследования компьютерных инцидентов.

Требования к реализации: При применении контейнерных сред должна обеспечиваться в соответствии с мерами РСБ.1 — РСБ.5 регистрация следующих событий безопасности:

попытки осуществления несанкционированного доступа к средству контейнеризации;

успешные и неуспешные 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 ролевой модели доступа;

модификация запускаемых контейнеров.

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 сертифицированных средств контейнеризации.

Требования к документированию: Требования к регистрации событий безопасности при применении контейнерных сред должны быть включены во внутренний стандарт, устанавливающий требования к сбору, регистрации и анализу событий, связанных с возможным нарушением безопасности информации, нарушением функционирования информационных систем, реализацией угроз безопасности информации.

Требования к усилению:

1) должна обеспечиваться регистрация следующих событий безопасности:

выявление известных уязвимостей в образах контейнеров и некорректности
их конфигурации;

факты нарушения целостности объектов контроля.

Реализация в информационной системе:

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

ЗКС.3 Управление доступом в контейнерных средах

Цель: Обеспечение правил разграничения доступа субъектов доступа к объектам доступа в контейнерных средах.

Требования к реализации: При применении контейнерных сред должно обеспечиваться в соответствии с мерами 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 сертифицированных средств контейнеризации и хостовой операционной системы.

Требования к документированию: Модели управления доступом в контейнерных средах, применяемых в информационной системе, должны быть включены во внутренний стандарт «Требования к применяемым моделям доступа пользователей».

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

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

ЗКС.4 Резервное копирование в контейнерных средах

Цель: Обеспечение восстановления функционирования контейнерной среды информационной системы.

Требования к реализации: При применении контейнерной среды должно обеспечиваться резервное копирование образов контейнеров.

Указанные меры защиты информации реализуются за счет применения
в информационной системе сертифицированных средств резервного копирования.

Требования к документированию: Порядок резервного копирования должен содержаться во внутреннем стандарте, устанавливающем требования к резервному копированию информации, программному обеспечению и его конфигурациям.

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
ЗКС.4	+	+	+
Усиление ЗКС.4		1	1, 2

ЗКС.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 сертифицированных средств контейнеризации и хостовых операционных систем.

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
ЗКС.5	+	+	+
Усиление ЗКС.5		1	1

ЗКС.6 Идентификация и аутентификация в контейнерной среде

Цель: Авторизация субъектов доступа в контейнерной среде.

Требования к реализации: Должна обеспечиваться в соответствии с мерами 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.

Должна обеспечиваться в соответствии с мерами ИАФ.2, ИАФ.4 идентификация и аутентификация в контейнерной среде следующих объектов доступа:

образы контейнеров;

контейнеры;

средства контейнеризации.

Указанные меры защиты информации реализуются за счет применения в информационной системе сертифицированных средств контейнеризации и хостовых операционных систем.

Требования к документированию: Порядок идентификации и аутентификации объектов и субъектов доступа в контейнерной среде должен быть определен во внутреннем регламенте, устанавливающем порядок создания, изменения, блокирования, контроля, удаления аутентификационной информации
и средств аутентификации.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКС.6	+	+	+
Усиление ЗКС.6			

ЗКС.7 Управление контейнерами и их образами (оркестрация)

Цель: Обеспечение защиты информации в контейнерной среде за счет управления контейнерами и их образами.

Требования к реализации: В контейнерной среде должны обеспечиваться:

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).

Управление образами контейнеров должно обеспечивать размещение образов контейнеров, запускаемых в рамках информационной системы, только на ресурсах технических средств, входящих в состав информационной системы.

Управление перемещением контейнеров и обрабатываемых на них данных должно обеспечивать перемещение контейнеров и обрабатываемых на них данных только с применением технических средств, входящих в состав информационной системы.

Указанные меры защиты информации реализуются за счет применения в информационной системе сертифицированных средств контейнеризации и хостовых операционных систем.

Требования к документированию: Не предъявляются.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКС.7	+	+	+
Усиление ЗКС.7			

ЗКС.8 Выявление уязвимостей в контейнерной среде

Цель: Выявление уязвимостей в образах 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 с сертифицированным средством контроля и анализа защищенности на основе сведений, содержащихся в банке данных угроз безопасности информации ФСТЭК России bdu.fstec.ru, а также в иных источниках, содержащих сведения об известных уязвимостях;

оповещение о выявленных уязвимостях администратора безопасности информационной системы.

Выявление известных уязвимостей в образах контейнеров должно осуществляться не реже одного раза в месяц.

Требования к документированию: Порядок выявления и устранения уязвимостей в образах контейнеров должен быть включен во внутренний

регламент, устанавливающий порядок выявления, оценки и устранения уязвимостей информационных систем.

Требования к усилению:

1) выявление известных уязвимостей в образах контейнеров должно осуществляться не реже одного раза в неделю.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКС.8	+	+	+
Усиление ЗКС.8		1	1

4.6. Защита сервисов электронной почты (ЗЭП)

ЗЭП.1 Защита ящиков и сообщений электронной почты

Цель: Исключить возможность несанкционированного доступа к объектам электронной почты (ящикам и сообщениям электронной почты) информационной системы.

Требования к реализации: Должны быть реализованы следующие меры защиты информации для обеспечения защиты ящиков и сообщений электронной почты:

периодическое резервное копирование содержимого ящиков электронной почты;

периодический анализ (аудит) ящиков электронной почты на наличие ящиков, подлежащих удалению;

регистрация событий безопасности, связанных с действиями пользователей в отношении объектов электронной почты.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должна обеспечиваться регистрация событий безопасности, связанных
с контролем состояния сервисов электронной почты;

2) должно обеспечиваться резервирование (дублирование) сервисов электронной почты;

3) должно обеспечиваться автоматическое блокирование доступа к ящикам электронной почты после установленного времени их неиспользования (неактивности);

4) должно быть определено и контролироваться допустимое время

доступа пользователей к сервисам электронной почты с учетом выполняемых функциональных обязанностей.

Реализация в информационной системе:

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

ЗЭП.2 Контроль доступа пользователей

Цель: Реализация контроля доступа пользователей к информации, содержащейся в ящиках электронной почты, с целью предотвращения несанкционированного доступа.

Требования к реализации: Должны быть реализованы следующие меры защиты информации для обеспечения защиты ящиков и сообщений электронной почты:

идентификация и аутентификация субъектов доступа (пользователи информационной системы, программное обеспечение) в сервисах электронной почты в соответствии с мерами ИАФ.1 — ИАФ.4;

доступ субъектов доступа к объектам электронной почты должен осуществляться с учетом минимально необходимых прав и привилегий и обеспечиваться в соответствии с мерой УПД.2.

Доступ субъектов доступа к общим (групповым) ящикам электронной почты и группам рассылки должен осуществляться по согласованию владельцем группы ящиков (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 защиты от вредоносных вложений (файлов, архивов)
и ссылок в составе сообщений электронной почты.

Требования к реализации: Должна обеспечиваться антивирусная

защита
в соответствии с мерой 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 эмулятора среды функционирования программного обеспечения, представляющего собой замкнутую программную среду исполнения («песочницу»);

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.

Требования к реализации: Должен 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.

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, сигнатурным и (или) эвристическим методами.

Должна обеспечиваться возможность проведения ретроспективного анализа сообщений электронной почты (по историческим данным мониторинга, отражающим события предыдущих временных периодов) на наличие поддельных данных и (или) фишинговых элементов.

Должно быть обеспечено обучение пользователей информационной системы, направленное на выявление сообщений электронной почты, содержащих поддельные данные и (или) фишинговые элементы.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должно осуществляться реагирование на получение сообщений электронной почты от недоверенных отправителей – блокирование сообщений электронной почты 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 эмулятора среды функционирования программного обеспечения, представляющего собой замкнутую программную среду исполнения («песочницу»).

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗЭП.4	+	+	+
Усиление ЗЭП.4		1	1, 2, 3

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, которые не относятся к функционированию информационной системы. Контроль поступающих сообщений электронной почты должен осуществляться за счет применения технологий, позволяющих однозначно верифицировать адреса электронной почты, от имени которых были отправлены сообщения.

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 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, при превышении которого последующие сообщения электронной почты должны блокироваться.

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 клиентами электронной почты и сервером электронной почты должно осуществляться с использованием технологий и сетевых протоколов, обеспечивающих конфиденциальность 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 почтового сервера, при которых 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.

Сервер электронной почты, доступный из сети «Интернет», не должен поддерживать прием и передачу почтового сетевого трафика, предназначенного для других информационных систем (доменов).

Требования к документированию: Не предъявляются.

Требования к усилению: Не предъявляются.

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 (пользователями, устройствами и приложениями) и объектами доступа, реализованными веб-приложением, должно осуществляться посредством программного интерфейса приложений, защита данных в котором обеспечивается в соответствии с мерой ЗПИ.1.

Доступ к пользовательским данным (объектам доступа), хранящимся в веб-приложении, пользовательским данным, хранящимся в веб-браузере пользователя (субъекта доступа), а также доступ к функциям веб-приложения должен осуществляться в соответствии с мерой УПД.2.

Требования к документированию: Внутренний стандарт, устанавливающий требования к применяемой модели доступа, должен включать:

определение объектов доступа, являющихся пользовательскими данными, хранящимися в веб-приложении;

определение объектов доступа, являющихся пользовательскими данными, хранящимися в веб-браузере пользователя (субъекта доступа);

определение типов доступа к пользовательским данным (функций веб-приложения), доступных различным типам учетных записей субъектов доступа.

Требования к усилению:

1) в информационной системе должна быть исключена возможность доступа пользователей, не являющихся привилегированными, к информации (данным) посредством передачи в веб-приложение запросов на взаимодействие с информацией (данными) на языке работы с данными (например, написание и исполнение скриптов на языке программирования высокого уровня в интерпретаторе веб-приложения, передача самостоятельно сформированного SQL-запроса в средство управления базами данных).

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗВТ.1	+	+	+

Усиление ЗВТ.1			1

ЗВТ.2 Контроль доступа пользователей

Цель: Обеспечение управления субъектов доступа (пользователей, устройств, приложений) к данным и функциям веб-приложений.

Требования к реализации: В информационной системе должны быть обеспечены:

идентификация и аутентификация субъектов доступа веб-приложения в соответствии с мерами ИАФ.1 — ИАФ.4;

управление доступом субъектов доступа к функциям и данным веб-приложений в соответствии с мерами УПД.1 — УПД.9;

ограничение числа параллельных сеансов доступа к веб-приложению в соответствии с мерой УПД.7;

автоматическое завершение сеансов доступа к веб-приложению при неактивности в соответствии с мерой 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 УПД.9.

Идентификация и аутентификация субъектов доступа должны осуществляться на стороне веб-приложения, 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) параметры сеанса доступа к веб-приложению должны включать уникальный идентификатор сеанса доступа (Session ID), защищенный от подмены и перехвата при информационном обмене с веб-приложением;

2) 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 ИАФ.1 — ИАФ.4.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1

ЗВТ.2	+	+	+
Усиление ЗВТ.2	1	1,2	1,2

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 ЗПИ.3.

Указанные меры защиты информации реализованы с использованием межсетевого экрана уровня веб-приложения, или многофункционального межсетевого экрана уровня сети, сертифицированного на соответствие требованиям ФСТЭК России.

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 (схема 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.

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

схемы легитимных запросов к веб-приложениям в машиночитаемой нотации (например, Swagger);

используемые веб-приложениями расширения протокола передачи гипертекста и иные версии прикладных протоколов;

атрибуты пользовательских запросов, подлежащие контролю с целью фильтрации и обнаружения событий безопасности;

типы и глубина вложений (полезной нагрузки) пользовательских запросов, подлежащих контролю с целью фильтрации и обнаружения событий безопасности;

признаки попыток реализации угроз безопасности;

признаки формирования запросов автоматизированными инструментальными средствами поиска и эксплуатации уязвимостей веб-приложений и перебора (подбора) аутентификационной информации.

Требования к усилению:

Наряду с обязательными мерами защиты информации дополнительно:

1) в информационной системе должна осуществляться актуализация признаков формирования запросов автоматизированными инструментальными средствами поиска и эксплуатации уязвимостей веб-приложений и перебора (подбора) аутентификационной информации;

2) в информационной системе должна осуществляться инвентаризация состава расширений протокола передачи гипертекста и иных версий прикладных протоколов, используемых веб-приложениями. Инвентаризация должна осуществляться динамическим методом анализа трафика веб-приложений. Инвентаризация должна осуществляться не реже 1 раза в 6 месяцев, либо при изменении программной реализации веб-приложения;

3) в информационной системе контроль и фильтрация трафика веб-приложений должны осуществляться в том числе методом анализа вложений (полезной нагрузки) пользовательских запросов.

Реализация в информационной системе:

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

ЗВТ.4 Регистрация событий безопасности в веб-приложениях и реагирование на них

Цель: Обеспечение регистрации событий безопасности, связанных с функционированием веб-приложения и попытками реализации угроз безопасности информации.

Требования к реализации: В информационной системе в соответствии
с мерами РСБ.1 — РСБ.5 должна быть обеспечена регистрация событий безопасности, связанных с попытками доступа субъектов доступа к объектам доступа (функциям и данным) веб-приложения в соответствии с мерами
УПД.1 — УПД.9.

В информационной системе должна быть обеспечена регистрация событий безопасности на уровне межсетевого экрана уровня веб-приложения 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-приложением;

события безопасности, связанные с управлением учетными записями пользователей веб-приложения;

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 (функций веб-приложения — 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;

события безопасности, связанные с выполнением процедуры установки, обновления или удаления компонентов (модулей) веб-приложения;

события безопасности, связанные с управлением запуском/остановкой компонентов веб-приложения.

На уровне межсетевого экрана уровня веб-приложения 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;

уведомления администратора (администратора безопасности) информационной системы о факте и причинах блокирования сетевого сеанса.

Требования к документированию: Внутренний стандарт, содержащий требования к сбору, регистрации и анализу событий, связанных с нарушением безопасности информации, нарушением функционирования информационных систем, реализацией угроз безопасности информации, должен определять:

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;

параметры веб-приложений и средств защиты информации, осуществляющих регистрацию событий безопасности, связанных с веб-приложением, необходимые для настройки получения событий безопасности.

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 веб-приложений на вредоносное программное обеспечение

Цель: Обеспечение выявления вредоносного программного обеспечения
в файлах, передаваемых в веб-приложение.

Требования к реализации: Должна обеспечиваться проверка всех файлов веб-приложений на вредоносное программное обеспечение в соответствии
с мерой АВЗ.1.

Контроль должен осуществляться с использованием сертифицированного многофункционального межсетевого экрана уровня сети либо совместно используемыми сертифицированными межсетевым экраном уровня
веб-приложения, изолированной замкнутой системой (средой) предварительного выполнения программ и средством антивирусной защиты.

Проверка должна включать анализ всех передаваемых в теле запроса файлов, а также составляющих тело запроса скриптов и данных, поступающих
в веб-приложение.

Требования к документированию: Внутренний стандарт, устанавливающий ограничения и запреты действий для пользователей при использовании и обеспечении эксплуатации ими информационных систем, должен определять перечень допустимых типов файлов, разрешенных к загрузке в веб-приложение.

Внутренний стандарт, устанавливающий требования к сбору, регистрации

и анализу событий, связанных с возможным нарушением безопасности информации, нарушением функционирования информационных систем, реализацией угроз безопасности информации, должен определять объем и продолжительность хранения файлов, переданных в составляющие информационную систему веб-приложения, с целью обеспечения возможности проведения их ретроспективного анализа.

Требования к усилению:

1) 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);

2) должен осуществляться автоматический контроль всех файлов, передаваемых посредством веб-приложения в смежные системы, на предмет выявления вредоносного программного обеспечения;

3) в информационной системе должна обеспечиваться возможность проведения ретроспективного анализа файлов, передаваемых веб-приложению,

а также посредством веб-приложения в смежные системы, на предмет выявления вредоносного программного обеспечения.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗВТ.5	+	+	+
Усиление ЗВТ.5	1	1, 3	1, 2, 3

ЗВТ.6 Защита систем управления контентом

Цель: Обеспечение защищенного функционирования системы управления контентом, используемой в составе веб-приложения.

Требования к реализации: В информационной системе в отношении системы управления контентом веб-приложения должны быть обеспечены:

идентификация и аутентификация пользователей системы управления контентом веб-приложения в соответствии с мерами ИАФ.1-ИАФ.4;

управление доступом пользователей к функциям и данным системы управления контентом веб-приложения в соответствии с мерами УПД.1-УПД.9.

Требования к документированию: Внутренний стандарт, содержащий требования к применяемым моделям доступа, должен определять:

перечень пользователей информационной системы, имеющих право взаимодействия с системой управления контентом веб-приложения;

регламент обновления контента в веб-приложении.

Внутренний стандарт, содержащий перечень разрешенного и (или) запрещенного для использования программного обеспечения, должен содержать список разрешенных компонентов (модулей) для системы управления контентом, а также источники их получения.

Требования к усилению:

1) в информационной системе обеспечивается защита системы управления контентом веб-приложения посредством определения и реализации порядка изменения списка компонентов (модулей) системы управления контентом веб-приложения;

2) в информационной системе должны рассматриваться в качестве системы управления контентом low-code и no-code платформы, служащие основой построения либо входящие в состав веб-приложения;

3) в информационной системе обеспечивается учет типов субъектов доступа, типов объектов доступа и типов доступа субъектов доступа к объектам доступа (функций веб-приложения) в модели управления доступом, создание, модификация и удаление которых возможны с помощью системы управления контентом, используемой в составе веб-приложения.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗВТ.6	+	+	+
Усиление ЗВТ.6		1, 2	1, 2

4.8. Защита программных интерфейсов взаимодействия приложений (API) (ЗПИ)

ЗПИ.1 Защита данных API

Цель: Обеспечение конфиденциальности информации и служебных данных, передаваемых при сетевом информационном взаимодействии с программным интерфейсом взаимодействия приложений.

Требования к реализации: При организации сетевого взаимодействия между субъектами доступа (пользователями, устройствами и приложениями) и объектами доступа посредством API должны обеспечиваться:

минимизация объема информации, раскрывающей структуру информационной системы, или иной конфиденциальной информации, передаваемой посредством API;

конфиденциальность информации и служебной информации, передаваемой посредством API.

При сетевом информационном взаимодействии внутренних пользователей информационной системы с API через сеть «Интернет» такое взаимодействие должно осуществляться с использованием криптографических средств защиты информации в соответствии с законодательством Российской Федерации.

При сетевом информационном взаимодействии внешних пользователей информационной системы с API через сеть «Интернет» должна обеспечиваться защита от несанкционированного доступа к передаваемой конфиденциальной информации.

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

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 программному обеспечению пользователей информационной системы, с помощью которого осуществляется доступ к API информационной системы (например, семейства операционных систем и минимальные версии веб-браузеров).

Требования к усилению:

1) должна обеспечиваться минимизация состава информации, возвращаемой в сообщениях об ошибках взаимодействия с API, раскрывающей структуру и особенности функционирования информационной системы или иную конфиденциальную информацию;

2) должна обеспечиваться минимизация состава информации, содержащейся в аутентификаторах доступа к API путем исключения данных, раскрывающих структуру информационной системы или иные конфиденциальные сведения;

3) должен осуществляться ежегодный пересмотр режимов и настроек программного обеспечения, реализующего API, с целью выявления уязвимостей его конфигурации;

4) при сетевом информационном взаимодействии внутренних пользователей с программным обеспечением посредством внутренних API информационной системы должна обеспечиваться защита от несанкционированного доступа к передаваемой конфиденциальной информации;

5) при сетевом информационном взаимодействии приложений с другими приложениями (например, между микросервисами) должна обеспечиваться защита от несанкционированного доступа к передаваемой конфиденциальной информации.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗПИ.1	+	+	+
Усиление ЗПИ.1	1, 2	1, 2, 3	1, 2, 3, 4

ЗПИ.2 Аутентификация и авторизация пользователей, устройств и приложений

Цель: Обеспечение аутентификации и авторизации субъектов доступа (пользователей, устройств и приложений), взаимодействующих с программным обеспечением информационной системы посредством API.

Требования к реализации: При реализации меры по аутентификации и авторизации пользователей, устройств и приложений, получающих доступ к информационной системе посредством API, в информационной системе должен быть определен перечень API, для которых требуется аутентификация и авторизация пользователей, устройств и приложений.

В информационной системе должны быть определены права и полномочия пользователей, устройств и приложений, получающих доступ к информационной системе посредством входящих в перечень API, в соответствии с мерами УПД.1 — УПД.2.

Пользователи, устройства и приложения, получающие доступ к информационной системе посредством входящих в перечень API, должны пройти процедуры идентификации и аутентификации в соответствии с мерами ИАФ.1 — ИАФ.4.

В отношении API, для доступа к которым не требуется аутентификации и авторизации пользователей, устройств и приложений, должен быть реализован контроль действий пользователей, устройств и приложений в соответствии
с мерой УПД.10.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должна обеспечиваться аутентификация и авторизация внутренних субъектов доступа (устройств и приложений) для доступа посредством API к определенным в информационной системе приложениям (микросервисам).

Реализация в информационной системе:

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

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, устройствами
и приложениями) и объектами доступа в информационной системе посредством API в информационной системе должна быть разработана спецификация API.

В информационной системе должна быть обеспечена возможность автоматической проверки запросов, поступающих извне информационной системы к API информационной системы, 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.

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

спецификации API, которые должны содержать номенклатуру запросов, типы и диапазоны допустимых значений полей запросов к API;

правила, описывающие виды запросов, не соответствующих спецификации API, подлежащие автоматическому блокированию средствами защиты информации информационной системы, которые должны быть описаны
в машиночитаемом формате, допускающем его применение в соответствующих средствах защиты информации, а также снабжены информацией о дате и авторе, сформировавшем правило и кратким комментарием, объясняющим причину создания данного правила. Должны быть зафиксированы порядок и частота актуализации правил.

Требования к усилению:

1) проверка поступающих к API запросов на соответствие формату, структуре и ограничениям, и блокировка запросов, не соответствующих спецификации API, должны осуществляться с использованием межсетевого экрана уровня веб-приложений или многофункционального межсетевого экрана уровня сети, сертифицированного на соответствие требованиям ФСТЭК России;

2) спецификация API должна быть представлена в машиночитаемом формате. В частности, для API в формате HTTP/REST спецификация API должна быть представлена в формате Open API (Swagger);

3) в информационной системе должен быть осуществлен пересмотр перечня и спецификации API не реже 1 раза в 3 месяца;

4) в информационной системе должен быть осуществлен пересмотр перечня и спецификации API не реже 1 раза в месяц либо при изменении кода или конфигурации приложений, реализующих данные API;

5) должен обеспечиваться непрерывный 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	1, 2, 3	1, 2, 4

4.9. Защита конечных устройств (ЗКУ)

ЗКУ.1 Контроль доступа

Цель: Обеспечение идентификации и аутентификации конечных устройств и их пользователей, а также обеспечение контроля доступа пользователей
к конечным устройствам.

Требования к реализации: Должна обеспечиваться идентификация и аутентификация конечных устройств в соответствии с мерами ИАФ.2 и ИАФ.4.

Должна обеспечиваться идентификация и аутентификация пользователей конечных устройств в соответствии с мерами ИАФ.1 и ИАФ.3.

Должны обеспечиваться меры по управлению доступом пользователей
к конечным устройствам в соответствии с мерами УПД.1 — УПД.4, а также обеспечиваться:

управление правами доступа пользователей к конечным устройствам;

блокировка удаленного доступа пользователей к конечным устройствам
с использованием сетей связи общего пользования при отсутствии защиты канала связи с применением средств криптографической защиты информации, прошедших процедуру оценки соответствия в соответствии с законодательством Российской Федерации.

При предоставлении пользователям доступа к конечным устройствам должен применяться принцип наименьших привилегий.

На конечных устройствах должен быть обеспечен запрет на установку

(инсталляцию) неразрешенного к использованию программного обеспечения.

Должен осуществляться контроль доступа пользователей к интерфейсам ввода (вывода) конечных устройств.

Указанные меры защиты информации реализуются путем применения механизмов безопасности сертифицированных операционных систем и (или) сертифицированными средствами идентификации и аутентификации.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должна осуществляться настройка параметров запуска компонентов программного обеспечения таким образом, чтобы текущий пользователь конечного устройства не мог получить через данные компоненты доступ к объектам доступа, на доступ к которым у него нет прав.

Реализация в информационной системе:

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

ЗКУ.2 Контроль целостности

Цель: Обеспечение целостности программной среды конечного устройства.

Требования к реализации: В информационной системе должен осуществляться контроль целостности следующего программного обеспечения конечных устройств:

операционные системы;

программное обеспечение средств защиты информации;

иное программное обеспечение, определяемое в информационной системе.

Контроль целостности программного обеспечения конечных устройств реализуется путем применения механизмов безопасности сертифицированных операционных систем.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должна осуществляться доверенная загрузка с использованием сертифицированных средств доверенной загрузки уровня базовой системы ввода-вывода или уровня платы расширения;

2) должна осуществляться доверенная загрузка с использованием сертифицированных средств доверенной загрузки уровня базовой системы

ввода-вывода или уровня платы расширения, реализованная на основе программно-аппаратного модуля;

3) должна осуществляться доверенная загрузка программного обеспечения телекоммуникационного оборудования;

4) должна обеспечиваться блокировка запуска программного обеспечения
и (или) блокировка конечного устройства в случае обнаружения фактов нарушения целостности;

5) должен обеспечиваться контроль целостности базовой системы ввода-вывода конечных устройств;

6) должен обеспечиваться контроль целостности микропрограммного обеспечения и аппаратных компонентов конечных устройств.

Реализация в информационной системе:

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

ЗКУ.3 Антивирусная защита и обнаружение и предотвращение вторжений на конечных устройствах

Цель: Обнаружение вторжений (компьютерных атак), компьютерных вирусов и их нейтрализация на конечных устройствах.

Требования к реализации: Должна обеспечиваться антивирусная защита конечных устройств информационной системы в соответствии с мерой АВЗ.1.

На конечных устройствах информационной системы должны обеспечиваться обнаружение вторжений (компьютерных атак) и реагирование на них с использованием сертифицированных средств обнаружения и реагирования на уровне узла.

Должно обеспечиваться обновление служебных баз данных применяемых средств защиты информации (средств антивирусной защиты, средств обнаружения и реагирования на уровне узла) с настраиваемых локальных ресурсов по расписанию и (или) по требованию.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должно обеспечиваться централизованное управление (администрирование) применяемыми средствами защиты информации (средствами антивирусной защиты, средствами обнаружения и реагирования
на уровне узла);

2) должно обеспечиваться взаимодействие средств обнаружения и реагирования на уровне узла с сертифицированной системой управления событиями безопасности информации;

3) должно обеспечиваться взаимодействие средств обнаружения и реагирования на уровне узла с сертифицированными средствами антивирусной защиты с целью обеспечения реагирования на обнаружение компьютерных вирусов;

4) должен обеспечиваться периодический ретроспективный анализ событий безопасности средств обнаружения и реагирования на уровне узла на наличие признаков вторжений (компьютерных атак);

5) должны обеспечиваться блокирование сетевого трафика и (или) изоляция конечного устройства, на котором обнаружены вторжения (компьютерные атаки), с сохранением доступности средства обнаружения и реагирования на уровне узла;

6) должно обеспечиваться взаимодействие с глобальной репутационной базой угроз для обогащения информацией о признаках вторжений (компьютерных атак);

7) должно обеспечиваться применение глобальной репутационной базы угроз для проверки файловых объектов, сетевых и прикладных артефактов
(IP-адресов, доменов, URL) в масштабе, близком к реальному времени;

8) должна обеспечиваться передача файловых объектов (исполняемых файлов, архивов) от применяемых на узлах информационной системы средств обнаружения и реагирования на уровне узла в эмуляторы среды функционирования программного обеспечения, представляющие собой замкнутую программную среду исполнения, для динамического анализа
в автоматическом режиме;

9) должно обеспечиваться бесперебойное функционирование средства обнаружения и реагирования на уровне узла при нарушении взаимодействия конечного устройства со средствами централизованного управления;

10) должна обеспечиваться возможность разработки (модернизации) решающих правил с целью предотвращения компьютерных атак, специфичных для информационной системы, а также новых компьютерных

атак, информация о которых была получена из открытых или иных источников.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКУ.3	+	+	+
Усиление ЗКУ.3		1, 2, 3	1, 2, 3, 4, 5, 6, 7, 8, 9, 10

ЗКУ.4 Мониторинг процессов и состояния устройства

Цель: Выявление несанкционированных действий (аномального поведения) в действиях пользователей и выполняемых процессах конечных устройств.

Требования к реализации: Должен обеспечиваться мониторинг процессов и состояния конечных устройств, включающий отслеживание следующих процессов и состояний:

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

выполнение процессов с высоким уровнем привилегий, скрытых процессов и системных служб;

процессы, инициированные средствами защиты информации конечных устройств;

выполнение команд в интерпретаторе командной строки;

попытки доступа программных средств 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 сертифицированных операционных систем, сертифицированных средств обнаружения и реагирования на уровне узла и (или) иными сертифицированными средствами 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;

3) должно отслеживаться потребление вычислительных ресурсов конечных устройств.

Реализация в информационной системе:

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

ЗКУ.5 Контроль и фильтрация трафика на устройстве

Цель: Обеспечение безопасности сетевого взаимодействия конечных устройств.

Требования к реализации: Должен обеспечиваться контроль сетевого трафика конечного устройства, включающий контроль:

доступа к внешним ресурсам;

доступа к внутренним ресурсам информационной системы;

загрузки файлов из внешних ресурсов;

удаленного доступа.

Должна осуществляться фильтрация сетевого трафика конечного устройства по определенным правилам фильтрации (по IP-адресам, портам, протоколам,
по содержимому и иным правилам).

Указанные меры защиты информации реализуются путем применения механизмов безопасности сертифицированных операционных систем, сертифицированных средств обнаружения и реагирования на уровне узла и (или) иными сертифицированными средствами 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) должна быть обеспечена возможность интеграции средств контроля и фильтрации сетевого трафика со средствами защиты информации, осуществляющими анализ сетевого трафика на предмет наличия вторжений (компьютерных атак);

3) должен выполняться анализ сетевого трафика конечного устройства трафика, включающий определение потоков данных, информацию
об отправителях и получателях, используемых сетевых протоколов и портов, статусах сетевых соединений (открытое, закрытое).

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКУ.5	+	+	+
Усиление ЗКУ.5			1, 2

ЗКУ.6 Регистрация, анализ и реагирование на события безопасности

Цель: Предотвращение компьютерных инцидентов и реагирование на события безопасности на конечных устройствах.

Требования к реализации: Должна обеспечиваться регистрация событий безопасности на конечных устройствах в соответствии с мерами РСБ.1 — РСБ.5.

Должен выполняться анализ зарегистрированных событий безопасности, по результатам анализа должно осуществляться реагирование на выявленные компьютерные инциденты.

Должно обеспечиваться реагирование на обнаружение компьютерных инцидентов сертифицированными средствами защиты информации.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должна обеспечиваться регистрация событий безопасности, связанных
с реагированием на выявленные компьютерные инциденты;

2) реагирование на выявленные компьютерные инциденты должно включать отправку уведомлений администратору безопасности информационной системы;

3) должен обеспечиваться анализ зарегистрированных на конечном устройстве событий безопасности сертифицированной системой управления событиями безопасности информации;

4) должно обеспечиваться реагирование на обнаружение компьютерных инцидентов сертифицированными средствами управления инцидентами информационной безопасности;

5) 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, 2	1, 2, 3

4.10 Защита мобильных устройств (ЗМУ)

ЗМУ.1 Идентификация и аутентификация пользователей

Цель: Идентификация и аутентификация пользователей мобильных устройств.

Требования к реализации: Должна обеспечиваться идентификация и аутентификация пользователей в мобильном устройстве в соответствии с мерами ИАФ.1, ИАФ.3.

При применении пользователями мобильных устройств для доступа к информационной системе, а также предоставлении доступа пользователям
к информации, содержащейся в мобильных устройствах, в целях выполнения своих служебных обязанностей (функций) должна быть реализована строгая аутентификация пользователей в соответствии с мерами ИАФ.1, ИАФ.3.

Указанные меры реализуются за счет применения в информационной системе сертифицированных операционных систем и (или) сертифицированными средствами идентификации и аутентификации.

Требования к документированию: Порядок идентификации и аутентификации пользователей мобильных устройств должен быть определен во внутреннем регламенте, устанавливающем порядок создания, изменения, блокирования, контроля, удаления аутентификационной информации и средств аутентификации.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

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

ЗМУ.2 Контроль доступа

Цель: Обеспечение контроля доступа пользователей к мобильным устройствам.

Требования к реализации: Должны обеспечиваться меры по управлению доступом пользователей к мобильным устройствам в соответствии с мерами УПД.1 — УПД.10, а также:

управление правами доступа пользователей к мобильным устройствам;

управление правами доступа приложений, установленных на мобильных устройствах, к ресурсам мобильной операционной системы (например, оперативной памяти, доступу к сети «Интернет», к другим приложениям);

блокировка удаленного доступа пользователей к мобильным устройствам с использованием сетей связи общего пользования при отсутствии защиты канала связи с применением средств криптографической защиты информации, прошедших процедуру оценки соответствия в соответствии с законодательством Российской Федерации.

При предоставлении пользователям доступа к мобильным устройствам, а также при применении пользователями мобильных устройств для доступа к информационной системе, а также предоставлении доступа пользователям к информации доступа, содержащейся в мобильных устройствах, должен применяться принцип наименьших привилегий.

На мобильных устройствах должен быть обеспечен запрет на установку (инсталляцию) неразрешенного к использованию программного обеспечения.

Указанные меры защиты информации реализуются путем применения сертифицированных операционных систем, и (или) сертифицированных средств идентификации и аутентификации, и (или) сертифицированных 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 Контроль 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;

иное программное обеспечение, определяемое в информационной системе.

Контроль целостности программного обеспечения мобильных устройств реализуется за счет применения механизмов безопасности сертифицированных операционных систем.

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.
В информационной системе обеспечивается выделение мобильных устройств
с активированными функциями разработки и отладки программ в отдельный сегмент (тестовую среду);

2) должна обеспечиваться блокировка запуска программного обеспечения
и (или) блокировка мобильного устройства в случае обнаружения фактов нарушения целостности;

3) должен обеспечиваться контроль целостности микропрограммного обеспечения и аппаратных компонентов мобильных устройств.

Реализация в информационной системе:

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

Создание резервных копий данных информационной системы в облачных сервисах с помощью мобильных устройств или установленного на них программного обеспечения должно быть заблокировано.

Указанные меры защиты информации реализуются путем применения сертифицированных операционных систем.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) передача данных между информационной системой и мобильными устройствами посредством сети «Интернет» должна осуществляться с использованием средств криптографической защиты информации, прошедших процедуру оценки соответствия в соответствии с законодательством
Российской Федерации;

2) должна проводиться очистка памяти мобильного устройства и переустановка программного обеспечения при передаче мобильного устройства от одного пользователя другому;

3) должны осуществляться очистка и (или) удаление информации на мобильном устройстве при превышении допустимого числа неуспешных попыток разблокировки мобильного устройства;

4) программное обеспечение мобильных устройств должно сохранять данные информационной системы только в изолированную область данных,
к которой имеет доступ только указанное программное обеспечение;

5) должна быть исключена возможность сохранения информации из программного обеспечения на мобильном устройстве, используемом для доступа к информационной системе, с помощью снимков экрана.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗМУ.4	+	+	+
Усиление ЗМУ.4	1	1, 2	1, 2, 3, 4

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 АВЗ.1.

Должно обеспечиваться обновление служебных баз данных применяемых средств защиты информации (средств антивирусной защиты, средств обнаружения и реагирования на уровне узла) с настраиваемых локальных ресурсов по расписанию и (или) по требованию.

Антивирусная защита мобильных устройств реализуется путем применения сертифицированных средств антивирусной защиты.

Требования к документированию: Не предъявляются.

Требования к усилению:

должно обеспечиваться централизованное управление (администрирование) применяемыми средствами защиты информации (средствами антивирусной защиты);

должно обеспечиваться применение глобальной репутационной базы угроз для проверки файловых объектов, сетевых и прикладных артефактов (IP-адресов, доменов, URL) в масштабе, близком к реальному времени.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗМУ.5	+	+	+
Усиление ЗМУ.5		1	1, 2

ЗМУ.6 Контроль приложений

Цель: Обеспечение управления установкой, запуском и функционированием программного обеспечения, установленного на мобильное устройство (далее – приложение).

Требования к реализации: На мобильном устройстве должны осуществляться:

контроль установки, запуска и функционирования приложений;

запрет на установку и запуск неразрешенных к использованию приложений;

запуск и функционирование приложений с минимальными правами, необходимыми для работы приложения;

контроль обновления приложений.

Указанные меры защиты информации реализуются за счет применения сертифицированных операционных систем и (или)

сертифицированных систем управления мобильными устройствами.

Требования к документированию: Состав и типовые конфигурации программного обеспечения, подлежащего установке на мобильных устройствах (приложений), должны быть определены во внутреннем стандарте, устанавливающем требования к типовым конфигурациям и настройкам программных, программно-аппаратных средств.

Требования к усилению:

1) должно осуществляться централизованное управление параметрами настройки и правами приложений, включая программные компоненты средств защиты информации, установленных на мобильном устройстве;

2) должны применяться средства автоматизации, позволяющие в автоматизированном режиме централизованно получать данные об изменениях мобильных устройств, связанных с их конфигурацией и настройками;

3) для учета используемых мобильных устройств должны применяться автоматизированные средства инвентаризации.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗМУ.5	+	+	+
Усиление ЗМУ.5			

ЗМУ.7 Ограничение и контроль функциональности

Цель: Ограничение возможностей нарушителя по получению доступа к информационной системе через мобильные устройства.

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;

реализован запрет использования функций удаленного управления мобильным устройством сторонними приложениями.

Должен обеспечиваться мониторинг процессов и состояния мобильных устройств, включающий отслеживание следующих процессов и состояний:

попытки идентификации и аутентификации пользователей мобильных устройств;

попытки удаленного доступа к мобильному устройству;

изменение программной конфигурации мобильного устройства.

Указанные меры защиты информации реализуются за счет применения сертифицированных операционных систем и (или) сертифицированных систем управления мобильными устройствами.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должен обеспечиваться мониторинг подключения внешних устройств
с использованием интерфейсов ввода-вывода;

2) должно быть реализовано централизованное управление функциональными возможностями мобильного устройства;

3) должно отслеживаться потребление вычислительных ресурсов мобильных устройств;

4) должна быть реализована взаимная аутентификация мобильных устройств и точек беспроводного доступа, используемых для подключения пользователей мобильных устройств к информационным системам.

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 достоверного получения, регистрации и контроля сведений о фактическом местоположении мобильных устройств, подключенных
к информационной системе.

Требования к реализации: Должна обеспечиваться регистрация информации о местоположении мобильного устройства, с которого осуществляется доступ
к информационной системе.

Должно осуществляться уведомление пользователя мобильного устройства о запросе информации о геопозиции его мобильного устройства.

Должны регистрироваться факты невозможности определения геопозиции мобильного устройства вследствие недоступности сигналов спутников, сигналов сотовых вышек или других беспроводных точек, по информации о которых делается вывод о геопозиции мобильного устройства.

Указанные меры защиты информации реализуются за счет применения сертифицированных систем управления мобильными устройствами.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должно быть реализовано ограничение доступа к информационной системе в зависимости от геопозиции мобильного устройства;

2) должно быть реализовано централизованное управление источниками, при помощи которых осуществляется сбор информации о геопозиции мобильных устройств.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗМУ.8	+	+	+
Усиление ЗМУ.8		1	1

ЗМУ.9 Защита личных устройств

Цель: Исключение несанкционированного доступа к ресурсам информационной системы, реализуемого с использованием личных мобильных устройств работников.

Требования к реализации: Не допускается обработка информации, доступ
к которой ограничен в соответствии с законодательством Российской Федерации,
с использованием личных мобильных устройств.

Для подключения личных мобильных устройств к информационной системе должен быть создан отдельный сегмент информационной системы.

В личных мобильных устройствах должны быть:

реализованы идентификация и аутентификация пользователей в программном обеспечении (приложении), используемом для доступа в информационную систему,
в соответствии с мерой ЗМУ.1;

обеспечен контроль доступа пользователей информационной системы с личного мобильного устройства в соответствии с мерой ЗМУ.2;

обеспечен контроль целостности программной среды личных мобильных устройств в соответствии с мерой ЗМУ.3;

реализована защита данных информационной системы, обрабатываемых
на личных мобильных устройствах и передаваемых между информационной системой и личными мобильными устройствами, в соответствии с мерой ЗМУ.4 за счет организации на личном мобильном устройстве защищенной информационной изолированной области (контейнера), в которой должно размещаться программное обеспечение (приложения), используемое для доступа в информационную систему;

обеспечена антивирусная защита личных мобильных устройств в соответствии с мерой ЗМУ.5;

реализован контроль приложений на личных мобильных устройствах в соответствии с мерой ЗМУ.6 в рамках защищенной информационной изолированной области (контейнера), в которой должно размещаться программное обеспечение (приложения), используемое для доступа в информационную систему;

обеспечены ограничение и контроль функциональности личных мобильных устройств в соответствии с мерой ЗМУ.7 в рамках защищенной информационной изолированной области (контейнера), в которой должно размещаться программное обеспечение (приложения), используемое для доступа в информационную систему;

обеспечены определение и контроль геопозиции личных мобильных устройств в соответствии с мерой ЗМУ.8.

Должна быть исключена передача данных из информационной изолированной области (контейнера), в которой должно размещаться программное обеспечение (приложения), используемое для доступа в информационную систему на личных мобильных устройствах, с помощью буфера обмена и функций «поделиться (переслать)» или «открыть в».

Указанные меры защиты информации реализуются за счет применения сертифицированных систем управления мобильными устройствами, сертифицированными средствами идентификации и аутентификации.

Требования к документированию: Не предъявляются.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

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

4.11. Защита устройств «интернета вещей» (ЗИВ)

ЗИВ.1 Идентификация и аутентификация

Цель: Идентификация и аутентификация устройств «Интернета вещей».

Требования к реализации: Должна обеспечиваться идентификация и аутентификация устройств «Интернета вещей» в соответствии с мерами ИАФ.2 и ИАФ.4.

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 соответствующих 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 цифровых сертификатов;

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 Контроль доступа

Цель: Управление доступом к устройствам «Интернета вещей».

Требования к реализации: При реализации контроля доступа к устройствам «Интернета вещей» должны быть установлены:

методы управления доступом к устройствам «Интернета вещей» (например, ролевой метод управления доступом; метод управления доступом, основанный на атрибутах устройств «Интернета вещей», метод управления доступом, основанный на списках управления доступом);

виды устройств «Интернета вещей», разрешенные для применения в информационной системе;

виды доступа (беспроводной, проводной (коммутируемый), широкополосный 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 пользователям доступа к устройствам «Интернета вещей» должен применяться принцип наименьших привилегий.

Требования к документированию: Во внутреннем стандарте по защите информации, устанавливающем требования к применяемым моделям доступа пользователей, должна быть определена модель управления доступом к устройствам «интернета вещей» в информационной системе.

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) должна быть исключена возможность несанкционированных изменений настроек устройств «Интернета вещей»;

4) должно обеспечиваться определение местонахождения несанкционированных устройств «Интернета вещей»;

5) должно обеспечиваться блокирование функционирования несанкционированного устройства «Интернета вещей».

Реализация в информационной системе:

Мера защиты	Класс защищенности

информации	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:

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.

Должен выполняться анализ уязвимостей прошивок устройств «Интернета вещей». В случае выявления уязвимостей – должно выполняться обновление версий прошивок устройств «Интернета вещей» на версии, не содержащие известные уязвимости.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должен обеспечиваться анализ сетевого трафика сетей устройств «Интернета вещей» с целью выявления аномалий – атак, направленных на отказ
в обслуживании; повышенных значениях нагрузки сетевого трафика (перегрузки сети), признаков компьютерных вирусов;

2) должна проводиться инвентаризация устройств «Интернета вещей» с целью выявления неиспользуемых устройств, а также устройств, не предусмотренных к использованию;

3) должны использоваться шлюзы безопасности сетей устройств «Интернета вещей».

Реализация в информационной системе:

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

ЗИВ.4 Контроль целостности

Цель: Обеспечение целостности программного обеспечения устройств «Интернета вещей».

Требования к реализации: При реализации мер по контролю целостности устройств «Интернета вещей» и вычислительной сети устройств «Интернета вещей» должны обеспечиваться:

контроль состава аппаратной части компонентов устройств «Интернета вещей» и вычислительной сети устройств «Интернета вещей», а также выявления фактов несанкционированного добавления новых устройств «Интернета вещей»;

контроль состава программного обеспечения устройств «Интернета вещей» и выявления фактов несанкционированного добавления нового программного обеспечения устройств «Интернета вещей»;

контроль целостности обновлений программного обеспечения вычислительной сети устройств «Интернета вещей»;

контроль целостности файлов, содержащих параметры настройки (конфигурацию) программного обеспечения устройств «Интернета вещей».

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должен осуществляться контроль целостности прошивок устройств «Интернета вещей» путем верификации цифровой подписи 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 программного обеспечения которых нарушена.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗИВ.4	+	+	+
Усиление ЗИВ.4			1

4.12 Защита точек беспроводного доступа (ЗБД)

ЗБД.1 Идентификация и аутентификация

Цель: Идентификация и аутентификация объектов и субъектов беспроводного доступа.

Требования к реализации: В соответствии с мерами ИАФ.1 — ИАФ.4 должна обеспечиваться идентификация и аутентификация следующих объектов
и субъектов беспроводного доступа:

пользователей, запрашивающих доступ к беспроводной локальной вычислительной сети (внутренних пользователей, привилегированных пользователей, администраторов);

устройств, запрашивающих доступ к беспроводной локальной вычислительной сети;

точек беспроводного доступа беспроводной локальной вычислительной сети.

Идентификация точек беспроводного доступа должна обеспечиваться по логическим именам (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.

Аутентификация устройств при подключении к точкам беспроводного доступа в информационной системе обеспечивается с использованием соответствующих протоколов аутентификации (например, WPA2/WPA3).

Не допускается осуществлять аутентификацию точек беспроводного доступа с использованием паролей, установленных по умолчанию.

Указанные меры защиты информации реализуются за счет применения
в информационной системе сертифицированных средств идентификации и аутентификации, реализованных и (или) применяемых в точках беспроводного доступа, ином оборудовании локальной сети беспроводного доступа, устройствах пользователей.

Требования к документированию: Во внутреннем регламенте, устанавливающем порядок создания, изменения, блокирования, контроля, удаления аутентификационной информации и средств аутентификации, должен быть определен порядок идентификации и аутентификации объектов и субъектов беспроводного доступа.

Требования к усилению:

1) должно обеспечиваться сокрытие имени сети (SSID) в списке доступных сетей;

2) аутентификация пользователей точек беспроводного доступа должна осуществляться с применением средств двухфакторной аутентификации;

3) должно обеспечиваться ограничение количества попыток входа пользователей точек беспроводного доступа;

4) для управления учетными записями и учетными данными субъектов беспроводного доступа в беспроводной локальной вычислительной сети должны использоваться системы (средства) управления учетными записями;

5) 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.

Реализация в информационной системе:

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

ЗБД.2 Контроль доступа

Цель: Управление доступом к точкам беспроводного доступа.

Требования к реализации: Должны обеспечиваться меры по управлению доступом субъектов и объектов доступа к точкам беспроводного доступа

в информационной системе в соответствии с мерами УПД.1 — УПД.4, а также обеспечиваться:

фильтрация устройств пользователей, используемых для беспроводного доступа, по физическим адресам (MAC-адресам) для управления разрешениями по доступу к локальной беспроводной 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;

регистрация доступа пользователей и устройств пользователя к точкам беспроводного доступа;

регистрация и анализ событий, связанных с использованием точек беспроводного доступа, в том числе для выявления попыток несанкционированного подключения к информационной системе через точки беспроводного доступа.

Указанные меры защиты информации реализуются за счет применения
в информационной системе сертифицированных средств управления доступом, реализованных и (или) применяемых в точках беспроводного доступа, ином оборудовании локальной сети беспроводного доступа, устройствах пользователей.

При предоставлении пользователям доступа к точкам беспроводного доступа должен применяться принцип наименьших привилегий.

Требования к документированию: Во внутренний стандарт по защите информации, устанавливающий перечень разрешенного и (или) запрещенного для использования программного обеспечения, должны быть включены:

перечень точек беспроводного доступа, разрешенных в информационной системе;

перечень устройств пользователей, разрешенных для использования при беспроводном доступе в информационной системе.

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.

Реализация в информационной системе:

Мера защиты	Класс защищенности

информации	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 сетей в отдельные сегменты информационной системы;

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);

отключение функциональной возможности автоматического подключения устройств пользователей к точкам беспроводного доступа, а также неиспользуемых функциональных возможностей;

контроль подключения устройств пользователей к точкам беспроводного доступа пользователей (процессов запускаемых от имени 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 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 несанкционированных подключений;

2) должен обеспечиваться анализ сетевого трафика сетей беспроводного доступа с целью выявления аномалий – атак, направленных на отказ в обслуживании; повышенных значений нагрузки сетевого трафика (перегрузки сети); признаков компьютерных вирусов;

3) должна проводиться инвентаризация точек беспроводного доступа с целью выявления неиспользуемых устройств, а также устройств, не предусмотренных к использованию;

4) должны применяться механизмы фильтрации (ограничения доступа) при подключении к точкам удаленного доступа по физическим и (или) логическим адресам;

5) должно обеспечиваться выделение беспроводных сетей в отдельные сегменты с использованием виртуальных локальных сетей (VLAN).

Реализация в информационной системе:

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

ЗБД.4 Контроль целостности

Цель: Обеспечение целостности прошивок и программного обеспечения точек беспроводного доступа.

Требования к реализации: Должны обеспечиваться следующие меры по контролю целостности точек беспроводного доступа в информационной системе:

еженедельный или с меньшей периодичностью, устанавливаемой в информационной системе, контроль отсутствия несанкционированных изменений в точках беспроводного доступа;

контроль целостности программного обеспечения и аппаратных компонентов точек беспроводного доступа;

отключение неиспользуемых интерфейсов;

размещение точек беспроводного доступа в пределах контролируемой зоны (чтобы исключить нарушителю физический доступ для внесения изменений);

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 контроль целостности прошивок и программного обеспечения точек беспроводного доступа путем верификации цифровой подписи или контрольных сумм;

2) должно обеспечиваться исключение возможности изменения пользователем подключаемого устройства настроек точек беспроводного доступа;

3) 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 информационной системы (сегментов информационной системы).

Требования к реализации: Должны применяться точки беспроводного доступа, имеющие возможность настройки уровня мощности сигнала.

Должно обеспечиваться ограничение уровней сигналов точек беспроводного доступа до установленных значений. 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 предъявляется.

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.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗБД.5			+
Усиление ЗБД.5			

4.13. Антивирусная защита (АВЗ)

АВЗ.1 Антивирусная защита устройств и серверов

Цель: Обеспечение антивирусной защиты информационной системы на устройствах и серверах, включающей 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 (компьютерных вирусов) в информационной системе, сокрытия свидетельств несанкционированного доступа к любым ресурсам информационной системы; обеспечение реагирования на обнаружение компьютерных вирусов.

Требования к реализации: Реализация антивирусной защиты должна предусматривать:

определение физических и виртуальных устройств и серверов, входящих
в состав информационной системы, на которых необходимо применение средств антивирусной защиты;

установку, конфигурирование и управление средствами антивирусной защиты;

предоставление 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 и серверов на наличие компьютерных вирусов;

настройку средств антивирусной защиты на устройствах и серверах информационной системы, через которые в нее могут быть внедрены компьютерные вирусы, 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) при загрузке,

открытии или исполнении таких файлов;

выявление компьютерных вирусов и реагирование на их 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 регламентом по антивирусной защите;

оповещение в масштабе времени, близком к реальному, об обнаружении компьютерных вирусов;

определение и выполнение действий по реагированию на обнаружение в информационной системе объектов, подвергшихся заражению компьютерными вирусами;

обновление баз данных признаков компьютерных вирусов в соответствии с информацией, поступающей от разработчика средства антивирусной защиты, в порядке, установленном регламентом по антивирусной защите;

автоматическую проверку устройств и серверов на наличие компьютерных вирусов после обновления базы данных признаков компьютерных вирусов.

Указанные меры защиты информации реализуются за счет применения сертифицированных средств антивирусной защиты.

Требования к документированию: В информационной системе должен быть разработан регламент по антивирусной защите.

Регламент по антивирусной защите должен определять:

область применения механизмов антивирусной защиты: перечень устройств и серверов, на которых необходимо применение средств антивирусной защиты;

действия по установке, настройке и управлению средствами антивирусной защиты;

порядок и правила проведения периодических проверок устройств и серверов на наличие компьютерных вирусов;

действия при оповещении о компьютерных вирусах и объектах, подвергшихся заражению компьютерными вирусами;

порядок и правила обновления базы данных признаков компьютерных вирусов, в том числе получения уведомлений о необходимости обновлений и непосредственного обновления базы данных признаков компьютерных вирусов, получения из доверенных источников и установки обновлений

базы данных признаков компьютерных вирусов, а также контроля целостности обновлений базы данных признаков компьютерных вирусов.

Порядок и правила, касающиеся действий пользователей в рамках выполнения регламента по антивирусной защите в информационной системе, должны быть отражены в инструкциях пользователей информационной системы.

Требования к усилению:

1) в информационной системе должно обеспечиваться выявление компьютерных вирусов и реагирование на их обнаружение на устройствах и серверах средством антивирусной защиты до загрузки операционных систем;

2) в информационной системе должно обеспечиваться централизованное управление антивирусной защитой за счет применения сертифицированных средств, обеспечивающих централизованное управление сертифицированными средствами антивирусной защиты.

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.

Требования к реализации: Реализация антивирусной защиты электронной почты должна предусматривать:

обнаружение в сообщениях электронной почты компьютерных вирусов;

реагирование на обнаружение угроз безопасности информации путем удаления компьютерных вирусов 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 сертифицированных средств антивирусной защиты электронной почты.

Требования к документированию: Регламент по антивирусной защите должен определять порядок осуществления антивирусной защиты

электронной почты.

Требования к усилению:

1) в информационной системе должно обеспечиваться помещение в карантин сообщений электронной почты;

2) в информационной системе должно обеспечиваться обнаружение компьютерных вирусов во вложениях сообщений электронной почты, содержащих зашифрованные и архивированные файлы.

Реализация в информационной системе:

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

АВЗ.3 Антивирусная проверка сетевого трафика

Цель: Обеспечение антивирусной защиты сетевого трафика.

Требования к реализации: Реализация антивирусной защиты сетевого трафика должна предусматривать:

антивирусную проверку файлов сетевого трафика;

анализ сетевого трафика на предмет наличия компьютерных вирусов в масштабе времени, близком к реальному;

анализ сетевого трафика на предмет наличия компьютерных вирусов с использованием сигнатурного метода обнаружения;

реагирование по результатам антивирусной проверки сетевого трафика, включающее: остановку (блокирование) передачи файлов или сетевых пакетов, содержащих компьютерные вирусы; удаление из сетевого трафика файлов, содержащих компьютерные вирусы; оповещение о выполненных действиях (удалении файлов, содержащих компьютерные вирусы, остановке (блокировании) передачи файлов или сетевых пакетов, содержащих компьютерные вирусы).

Указанные меры защиты информации реализуются за счет применения сертифицированных средств антивирусной защиты электронной почты и многофункциональных межсетевых экранов уровня сети.

Требования к документированию: Регламент по антивирусной защите должен определять порядок осуществления антивирусной защиты сетевого трафика.

Требования к усилению:

1) в информационной системе должен обеспечиваться анализ сетевого трафика на предмет наличия компьютерных вирусов с использованием эвристических методов обнаружения;

2) в информационной системе должен обеспечиваться анализ сетевого трафика на предмет наличия компьютерных вирусов на прикладном уровне для установленных регламентом приложений (веб-приложений, клиентов файловых хранилищ, мессенджеров и иных приложений);

3) в информационной системе должен осуществляться анализ зашифрованного сетевого трафика на предмет наличия компьютерных вирусов.

Реализация в информационной системе:

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

АВЗ.4 Применение замкнутой программной среды исполнения («песочницы»)

Цель: Выявление компьютерных вирусов и целевых атак на информационную систему путем запуска подозрительных объектов в замкнутой программной среде исполнения («песочнице») и анализа поведения указанных объектов.

Требования к реализации: В информационной системе должны применяться сертифицированные эмуляторы среды функционирования программного обеспечения, представляющие собой замкнутую среду («песочницу»), позволяющие обеспечивать:

выполнение проверок объектов, имеющих формат исполняемых файлов, на компонентах информационной системы (серверах, автоматизированных рабочих местах), определенных в информационной системе;

получение подозрительных объектов для поведенческого анализа от иных средств защиты информации, например, от средств защиты от целенаправленных атак.

Требования к документированию: Регламент по антивирусной защите должен определять порядок использования замкнутой программной среды исполнения.

Требования к усилению:

1) в информационной системе должны применяться сертифицированные эмуляторы среды функционирования программного обеспечения, представляющие собой замкнутую среду («песочницу»), позволяющие обеспечивать выполнение проверок различных типов объектов (например, скриптов автоматизации, документов, архивированных файлов, иных объектов);

2) в информационной системе должны применяться сертифицированные эмуляторы среды функционирования программного обеспечения, представляющие собой замкнутую среду («песочницу»), позволяющие обеспечивать возможность запуска подозрительных объектов на исполнение в виртуальных образах нескольких операционных систем;

3) в информационной системе должны применяться сертифицированные эмуляторы среды функционирования программного обеспечения, представляющие собой замкнутую среду («песочницу»), позволяющие обеспечивать возможность имитации пользовательских действий с подозрительными объектами.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
АВЗ.4		+	+
Усиление АВЗ.4			1, 2, 3

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: Должно обеспечиваться:

обнаружение (предотвращение) вторжений (компьютерных атак) с использованием сертифицированных систем обнаружения вторжений уровня сети, размещаемых на периметре информационной системы;

обнаружение компьютерных атак и реагирование на них (уведомление администратора безопасности, блокирование трафика и иные действия по реагированию) в масштабе времени, близком к реальному;

защита информации, собранной и сгенерированной системой

обнаружения вторжений;

обновление баз решающих правил и индикаторов атак систем обнаружения вторжений с серверов обновлений разработчика средства и (или) с настраиваемых локальных ресурсов по расписанию и (или) по требованию.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должны применяться сертифицированные системы обнаружения вторжений на прикладном уровне базовой эталонной модели взаимосвязи открытых систем;

2) должна обеспечиваться возможность анализа зашифрованного сетевого трафика;

3) должна обеспечиваться возможность разработки (модернизации) решающих правил с целью предотвращения компьютерных атак, специфичных для информационной системы, а также новых компьютерных атак, информация о которых была получена из открытых или иных источников;

4) должна обеспечиваться возможность хранения фрагментов собранного сетевого трафика;

5) должна обеспечиваться возможность периодического ретроспективного анализа сетевого трафика;

6) должна обеспечиваться возможность анализа аномальной активности в сети;

7) должна обеспечиваться возможность анализа вложений и объектов, извлекаемых из сетевого трафика (исполняемых файлов, ссылок, архивов и др.), с возможностью их передачи в эмуляторы среды функционирования программного обеспечения, представляющие собой замкнутую программную среду исполнения («песочницу»), для динамического анализа в автоматическом режиме;

8) должны применяться средства защиты от целенаправленных атак, обладающие комплексными функциональными возможностями по обнаружению вторжений, анализу сетевого трафика на предмет наличия компьютерных вирусов, в том числе с использованием эмуляторов среды функционирования программного обеспечения, представляющих собой замкнутую программную среду исполнения («песочницу»);

9) должно обеспечиваться информирование при возникновении ошибок в процессе обновления баз решающих правил;

10) должно обеспечиваться использование глобальной репутационной базы угроз для проверки сетевых и прикладных артефактов (IP-адресов, доменов, URL) в масштабе, близком к реальному времени.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
СОВ.1	+	+	+
Усиление СОВ.1		1, 2	1, 2, 4, 5, 6, 7, 8, 9, 10

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) с использованием сертифицированных систем обнаружения вторжений, размещаемых в сегментах (на границах сегментов) информационной системы.

В качестве таких сегментов должны рассматриваться:

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 типами устройств – отдельные сети для серверов, рабочих станций, мобильных устройств.

Должен обеспечиваться анализ всех запросов между сегментами на наличие вторжений (компьютерных атак) и аномальных запросов.

Должно обеспечиваться обновление баз решающих правил и индикаторов атак систем обнаружения вторжений с настраиваемых локальных ресурсов
по расписанию и (или) по требованию.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должно обеспечиваться централизованное управление (администрирование) компонентами системы обнаружения вторжений, установленными в различных сегментах информационной системы;

2) должно обеспечиваться блокирование сетевого трафика или изоляция сегмента, в котором обнаружены компьютерные атаки.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
СОВ.2	+	+	+
Усиление СОВ.2		1, 2	1, 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 с целью разбиения информационной системы на изолированные сегменты.

Сегментация информационной системы проводится путем:

выделения сегментов по функциональному назначению (например, пользовательский и серверный сегменты, сегмент демилитаризованной зоны, сегмент администрирования и другие сегменты);

выделения сегментов информационной системы, имеющих разные классы защищенности;

выделения сегментов информационной системы с разными уровнями конфиденциальности информации;

выделения сегментов информационной системы по иным структурно-функциональным характеристикам.

При сегментации информационной системы должны обеспечиваться контроль и фильтрация сетевого трафика на границах сегментов.

Указанные меры защиты информации реализуются за счет применения
в информационной системе сертифицированных межсетевых экранов и (или) сертифицированных многофункциональных межсетевых экранов уровня сети.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должна проводиться проверка корректности сегментации информационной системы не реже одного раза в год;

2) должны централизовано регистрироваться события блокировки попыток доступа в обход правил межсетевого экранирования с

применением средств мониторинга информационной безопасности;

3) должен быть обеспечен принцип минимальных привилегий при взаимодействии между сегментами, при предоставлении доступа субъектов доступа к сегментам информационной системы;

4) должна быть реализована микросегментация на уровне сегментов информационной системы, обеспечивающая их разделение на изолированные сегменты в соответствии с функциональными обязанностями субъектов доступа;

5) должна быть реализована возможность предоставления доступа внешних пользователей к приложениям (сервисам) информационной системы
без предоставления доступа к сегментам информационной системы;

6) должна быть реализована автоматизация управления правилами межсетевого экранирования сегментации для обеспечения согласованности правил на различных межсетевых экранах.

Реализация в информационной системе:

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

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 сертифицированных межсетевых экранов и (или) сертифицированных многофункциональных межсетевых экранов уровня сети.

Все сетевые соединения между демилитаризованной зоной, внешними информационными системами, сетями и внутренними

сегментами должны проходить через сертифицированные средства межсетевого экранирования и (или) сертифицированные многофункциональные межсетевые экраны уровня сети. Правила фильтрации должны исключать доступ из демилитаризованной зоны во внутренние сегменты информационной системы.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должна обеспечиваться защита компонентов информационной системы, находящихся в демилитаризованной зоне, с применением средств межсетевого экранирования уровня веб-приложений;

2) должны использоваться обратные прокси-серверы для организации доступа к компонентам информационной системы, находящимся в демилитаризованной зоне;

3) в демилитаризованной зоне должна обеспечиваться защита от компьютерных атак, реализуемых на прикладном уровне, с применением сертифицированных средств обнаружения вторжений.

Реализация в информационной системе:

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

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 безопасности информации.

Правила фильтрации трафика должны обеспечивать анализ пакетов на сетевом, транспортном и прикладном уровнях. Фильтрации подлежат входящие и исходящие сетевые соединения.

Все события сетевого доступа должны регистрироваться и анализироваться в ходе мониторинга информационной безопасности.

Требования к документированию: Во внутреннем стандарте, устанавливающем требования к защите информации при подключении к информационным системам иных информационных систем, включая требования к каналам передачи данных при взаимодействии с такими информационными системами, должны быть определены правила фильтрации трафика на границах между сегментами информационной системы, а также на границе с внешними системами и сетями, включая сеть «Интернет».

Требования к усилению:

1) должен обеспечиваться глубинный анализа пакетов путем применения сертифицированных многофункциональных межсетевых экранов уровня сети;

2) должен проводиться анализ вредоносного программного обеспечения в сетевом трафике путем применения 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 состоянии информационной системы (например, сетевых адресов, наименований узлов, типов и версий программного обеспечения, коды ошибок).

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 путем искусственного затягивания сетевых сессий;

3) должна быть реализована генерация игнорирования 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
к информационной системе с использованием специально созданных (эмулированных) ложных информационных систем.

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 во внешние системы мониторинга информационной безопасности.

Ложные информационные системы должны быть изолированы от информационной системы, обладать признаками функционирующих сервисов и не должны содержать информации ограниченного доступа.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) ложные информационные системы или их компоненты должны создавать ложные данные на автоматизированных рабочих местах пользователей информационной системы. Например, ложные информационные системы или их компоненты могут обеспечивать создание и функционирование следующих типов 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 ложной информационной системы за счет использования уникальных IP-адреса и MAC-адреса.

Реализация в информационной системе:

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

4.16. Защита от атак, направленных на отказ в обслуживании (ЗОО)

ЗОО.1 Контроль и фильтрация входящего трафика

Цель: Исключение заблаговременно известных нелегитимных потоков входящего трафика защищаемых сервисов информационной системы.

Требования к реализации: При реализации контроля и фильтрации входящего трафика в информационной системе должно быть обеспечено:

применение правил фильтрации входящего трафика на постоянной основе или в момент после обнаружения атаки, направленной на отказ в обслуживании;

применение правил фильтрации входящего трафика до транспортного уровня информационных систем (4 уровня модели OSI) на всех эшелонах периметра сети, в которой расположена информационная система. Под эшелонами сети понимаются любые средства или сервисы провайдеров услуг, направленные на защиту от атак, направленных на отказ в обслуживании, а также межсетевые экраны, которые логически и функционально позволяют реализовать списки доступа на скоростях выше, чем следующий на пути к защищаемому сервису эшелон. Каждый вышестоящий эшелон должен стремиться устранять дефицит вычислительных, канальных и иных ресурсов, направленных на обработку трафика;

применение правил фильтрации на основе матрицы коммуникаций информационных систем с сетью «Интернет» на транспортном уровне информационных систем (4 уровне модели OSI) 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 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 атак, направленных на отказ в обслуживании, при которых не удается обеспечить должный уровень фильтрации (обеспечить доступность информационной системы) на основе матрицы коммуникаций информационных систем и иных мер защиты от атак, направленных на отказ в обслуживании.

Для защиты информационных систем и фильтрации трафика атак, направленных на отказ в обслуживании на прикладном уровне оператор в том числе должен использовать специализированные программные, программно-аппаратные средства или услуги провайдеров хостинга или организаций, предоставляющих услуги связи, или организаций, оказывающих услуги по контролю, фильтрации и блокированию входящего трафика, способных работать на прикладном уровне информационных систем (7 уровне модели OSI).

Требования к документированию: Внутренний регламент по порядку вывода в контур промышленной эксплуатации сервисов, доступ к которым осуществляется с использованием сети «Интернет», должен в том числе содержать:

перечень интерфейсов и сервисов информационных систем, которые

должны быть постоянно доступны из сети «Интернет» и подлежащих защите от компьютерных атак, направленных на отказ в обслуживании;

состав и содержание мероприятий по предоставлению (открытию) доступа пользователям из сети «Интернет» интерфейсов и сервисов информационных систем, подлежащих 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;

логическую схему сети, отображающую весь путь прохождения трафика от точки публикации защищаемых сервисов в сеть «Интернет» до конечного хоста внутри информационной системы с указанием информационных потоков;

требование о хранении в течении трех лет информации о фактах реализации атак, направленных на отказ в обслуживании: дата и время начала и окончания реализации атак, тип атаки, 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, а также признаков атак на прикладном уровне, подверженных атакам, принимаемые меры.

Требования к усилению:

1) оператор должен обеспечить применение правил фильтрации входящего трафика на постоянной основе;

2) наличие возможности анализа TLS-трафика путем 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.1	+	+	+
Усиление ЗОО.1			1

ЗОО.2 Мониторинг состояния сервисов и интерфейсов

Цель: Обеспечение непрерывного контроля состояния доступности информационных систем и показателей ключевых метрик производительности сервисов и средств, используемых для защиты от 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) всех 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 приложения и других средств), реализующих сетевые функции с контролем состояния соединений;

количества запросов на прикладном уровне информационных систем для средств и сервисов, функционирующих на 7 уровне модели OSI;

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: Не предъявляются.

Требования к усилению:

1) в случае использования услуг провайдеров хостинга или организаций, предоставляющих услуги связи, 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.2	+	+	+
Усиление ЗОО.2			1

ЗОО.3 Балансировка нагрузки

Цель: Обеспечение возможности обработки повышенного объема или всплесков трафика и повышение уровня отказоустойчивости сервисов

информационной системы.

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 или организаций, предоставляющих услуги связи, 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 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 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.3	+	+	+
Усиление ЗОО.3			1

ЗОО.4 Ограничение скорости

Цель: Ограничение возможности создания условий для исчерпания ресурсов информационной системы.

Требования к реализации: При реализации меры по ограничению скорости

в информационной системе необходимо установить ограничение:

по максимальному числу одновременно установленных TCP-соединений

с одного IP-адреса;

по максимальному числу одновременно выполняемых запросов в секунду на прикладном уровне с одного IP-адреса.

Требования к документированию: Не предъявляются.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

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

ЗОО.5 Поддержка резерва достаточной пропускной способности и расширение ресурсов при сбоях

Цель: Обеспечение резерва ресурсов пропускной способности, позволяющего обрабатывать входящий трафик в условиях реализации атак, направленных на отказ в обслуживании.

Требования к реализации: В информационной системе должны быть обеспечены:

двукратный резерв полосы пропускания на каналах провайдера услуг доступа к сети «Интернет». Резерв рассчитывается от пика полосы легитимного трафика в условиях отсутствия реализации атак, направленных на отказ в обслуживании;

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 атак, направленных на отказ в обслуживании;

двукратный резерв по возможности обработки трафика на всех элементах информационной системы. Для каждого элемента информационной системы резерв рассчитывается от пиковой нагрузки, создаваемой легитимным трафиком в условиях отсутствия реализации 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.5	+	+	+
Усиление ЗОО.5			

4.17. Защита каналов связи и сетевого взаимодействия (ЗКС)

ЗКС.1. Защита данных при передаче по каналам связи

Цель: Обеспечение конфиденциальности, целостности и доступности информации при передаче по каналам связи за пределы контролируемой зоны.

Требования к реализации: В информационной системе должна быть обеспечена защита информации при передаче по каналам связи, выходящим
за пределы контролируемой зоны, для следующих сценариев:

передача информации ограниченного доступа за пределы контролируемой зоны;

удаленный доступ пользователей к информационной системе из-за пределов контролируемой зоны;

сетевое взаимодействие пользователей, приложений, сетевых сервисов, находящихся в разных сегментах информационной системы;

сетевое взаимодействие пользователей, приложений, сетевых сервисов информационной системы с другими информационными системами.

В информационной системе должна быть обеспечена защита каналов передачи данных, 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;

ограничение доступа пользователей, приложений и сетевых сервисов к неиспользуемым портам, сетевым службам и сервисам.

Реализация указанной меры защиты информации обеспечивается за счет применения сертифицированных межсетевых экранов и (или) сертифицированных многофункциональных межсетевых экранов.

Все события, связанные с передачей информации по каналам связи, должны регистрироваться и анализироваться в рамках мониторинга информационной безопасности.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должно обеспечиваться резервное копирование перечня правил межсетевого экранирования;

2) должны быть отключены устаревшие и небезопасные версии протоколов и сетевых служб;

3) должен осуществляться мониторинг аномалий сетевого трафика.

Реализация в информационной системе:

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

ЗКС.2. Контроль атрибутов безопасности при сетевом взаимодействии

Цель: Обеспечение доверенного сетевого взаимодействия на основе контроля атрибутов безопасности передаваемой информации и субъектов доступа.

Требования к реализации: В информационной системе должен быть определен перечень атрибутов безопасности, в соответствии с которыми осуществляется контроль получаемой и передаваемой информации за пределами 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 идентификаторы пользователей и 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.

Присвоение и передача атрибутов безопасности должна быть защищена
от несанкционированного извлечения, модификации или удаления.

Все операции с атрибутами, включая проверки и принятые решения о доступе, должны регистрироваться.

Реализация указанных мер защиты информации обеспечивается за счет применения сертифицированных межсетевых экранов и (или)

сертифицированных многофункциональных межсетевых экранов.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должна быть реализована централизованная система управления атрибутами безопасности;

2) должно обеспечиваться резервное копирование конфигураций атрибутов безопасности отправителей и получателей.

Реализация в информационной системе:

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

ЗКС.3. Обеспечение подлинности сетевых соединений

Цель: Обеспечение подлинности установления сетевых соединений только с доверенными внешними информационными системами, приложениями
и сервисами.

Требования к реализации: В информационной системе должно быть обеспечено подтверждение подлинности сетевых соединений, устанавливаемых при взаимодействии с внешними информационными системами, приложениями
и сервисами, на основе атрибутов безопасности.

Доступ к сетевым сервисам должен предоставляться только после успешной идентификации и аутентификации пользователей. Несанкционированные попытки подключения должны блокироваться сертифицированными средствами межсетевого экранирования и (или) сертифицированными многофункциональными межсетевыми экранами. Все успешные и неуспешные попытки аутентификации должны регистрироваться в журналах событий безопасности сертифицированных средств межсетевого экранирования и (или) сертифицированных многофункциональных межсетевых экранов.

В информационной системе должны быть реализованы защита от повторного использования аутентификационных данных и контроль целостности установленных сессий.

Требования к документированию: Не предъявляются.

Требования к усилению: Не предъявляются.

Реализация в информационной системе:

Мера защиты	Класс защищенности

информации	К3	К2	К1
ЗКС.3	+	+	+
Усиление ЗКС.3			

ЗКС.4. Контроль доступа к внешним ресурсам

Цель: Контроль и фильтрация исходящего сетевого трафика с целью исключения несанкционированного доступа к информационной системе через взаимодействие с внешними информационными системами и ресурсами.

Требования к реализации: В информационной системе должны быть:

сформирован и поддерживаться в актуальном состоянии список разрешенных внешних ресурсов, необходимых для выполнения функциональных задач (белый список);

реализован контроль доступа пользователей, приложений и сетевых сервисов информационной системы к ресурсам внешних сетей, включая сеть «Интернет», в соответствии с заданным белым списком;

заблокированы попытки доступа к ресурсам внешних сетей, включая сеть «Интернет», не содержащихся в белых списках;

определен список разрешенных в информационной системе используемых сетевых протоколов, сетевых приложений и сервисов.

Требования к документированию: Не предъявляются.

Требования к усилению:

1) должны применяться механизмы анализа зашифрованного трафика;

2) должен проводиться морфологический анализ запрашиваемых веб-ресурсов перед их открытием;

3) должна использоваться категоризация веб-ресурсов;

4) должны применяться механизмы поведенческого анализа пользовательской активности.

Реализация в информационной системе:

Мера защиты информации	Класс защищенности		
	К3	К2	К1
ЗКС.4	+	+	+
Усиление ЗКС.4			1

ЗКС.5. Контекстная проверка исходящего трафика

Цель: Предотвращение утечки информации ограниченного доступа и выявление несанкционированного обмена данными путем комплексного

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».

Все выявленные попытки несанкционированной передачи информации,
в том числе содержащей сведения, составляющие информацию ограниченного доступа, должны блокироваться за счет применения сертифицированных средств защиты от неправомерной передачи информации из информационной системы (средств предотвращения утечки защищаемой информации).

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.5			+
Усиление ЗКС.5			

4.18. Защита систем искусственного интеллекта (ЗИИ)

ЗИИ.1 Обеспечение безопасной разработки системы искусственного интеллекта

Цель: Обеспечение защиты информации в инфраструктуре разработки системы искусственного интеллекта, обеспечение ее безопасного
и устойчивого функционирования, а также обеспечение безопасной разработки систем искусственного интеллекта.

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

информационная инфраструктура разработки системы искусственного интеллекта;

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

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

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

наборы обучающих данных;

выходная модель машинного обучения и ее параметры (веса).

В информационной инфраструктуре разработки системы искусственного интеллекта должны быть реализованы меры по защите информации, установленные настоящим методическим документом 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 программного обеспечения, обеспечивающего разработку системы искусственного интеллекта, должны быть обеспечены:

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 принятие мер по их устранению;

проведение испытаний по выявлению уязвимостей и недекларированных возможностей.

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 машинного обучения должен быть проведен анализ сведений об уязвимостях указанной модели, получаемых из внешних источников. В отношении выявленных уязвимостей разработчиков системы искусственного интеллекта должны быть приняты меры, направленные на нейтрализацию выявленных уязвимостей.

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 сертифицированных шифровальных (криптографических) средств защиты информации;

3) в отношении выходной модели машинного обучения 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.

Реализация в информационной системе:

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

ЗИИ.2 Защита системы искусственного интеллекта в ходе эксплуатации

Цель: Обеспечение защиты информации в информационной системе при эксплуатации системы искусственного интеллекта, а также обеспечение ее безопасного и устойчивого функционирования.

Требования к реализации: При эксплуатации системы искусственного интеллекта в информационной системе дополнительно должна быть обеспечена защита следующих объектов:

программное обеспечение, обеспечивающее реализацию технологии искусственного интеллекта (модели машинного обучения), а также агентов искусственного интеллекта, API-интерфейсов, систем цензуры;

обученная и готовая к использованию модель машинного обучения, 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, установленные настоящим методическим документом, по классу защищенности не ниже класса защищенности информационной системы оператора (обладателя информации).

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

обеспечение фильтрации входных данных (запросов) системы искусственного интеллекта с применением системы цензуры;

обеспечение фильтрации выходных данных (ответов) системы

искусственного интеллекта с применением системы цензуры;

мониторинг и квотирование количества запросов к системе искусственного интеллекта;

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

обеспечение целостности параметров (весов) модели машинного обучения
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.

Требования к документированию: Не предъявляются.

Требования к усилению:

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

2) должна быть обеспечена целостность модели машинного обучения с использованием сертифицированных шифровальных (криптографических) средств защиты информации.

Реализация в информационной системе:

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

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: это 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.

Белый список: перечень ресурсов (IP-адресов, доменных имен, приложений), доступ к которым разрешен; весь остальной трафик блокируется.

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.

Глубинный 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.

Глубокий анализ пакетов: технология анализа сетевого трафика, позволяющая проверять содержимое передаваемых пакетов данных beyond simple header information.

Гостевая операционная система: операционная система, управляющая виртуальной машиной.

Демилитаризованная зона: это обособленный сегмент информационной системы, расположенный между сетью связи общего пользования (внешними информационными системами) и внутренней инфраструктурой информационной системы.

Дискреционный метод управления доступом: 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;

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: это программные,

программно-аппаратные средства, обеспечивающие выполнение заданной задачи
в информационной системе, взаимодействуя с другими элементами системы (например, почтовый сервис, веб-сайт, сетевой сервис).

Конечные устройства: физические и виртуальные устройства информационной системы, имеющие постоянный доступ к 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 осуществляются мероприятия по защите информации
от утечки по техническим каналам.

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: это 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: 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: это 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: это 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.

Мобильные устройства: смартфоны и планшетные компьютеры под управлением мобильных операционных систем. Для защиты переносных компьютеров и планшетных компьютеров под управлением

десктопных операционных систем должны применяться требования по защите информации при применении конечных устройств и требования по защите информации при удаленном доступе пользователей к информационным системам.

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: 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: это 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.

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.

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, обеспечивающие создание и функционирование контейнеров.

Субъект доступа: пользователь, процесс или устройство, запрашивающее доступ к информации или ресурсам информационной системы.

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.

Low-code платформа: платформа для создания приложений с минимальным участием программистов. Вместо традиционного написания кода для создания большей части приложения и контента приложения используется визуальное моделирование, шаблоны, готовые компоненты и бизнес-логика, которую можно собрать из блоков, аналогично no-code платформам.

No-code платформа: платформа для разработки без написания кода. Она позволяет нетехническим пользователям создавать приложения, веб-сайты и автоматизированные потоки операций с помощью визуальных инструментов перетаскивания.

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, 2	+ 1,2
ИАФ.2	Идентификация устройств	+ 2	+ 2	+ 1
ИАФ.3	Аутентификация пользователей	+ 1а	+ 1б	+ 1в, 2, 6, 14
ИАФ.4	Аутентификация устройств			
2. Управление доступом (УПД)				
УПД.1	Реализация модели управления доступом	+ 1	+ 1, 2, 3	+ 1, 2, 3
УПД.2	Разграничение и контроль прав доступа	+ 1, 2	+ 1, 2, 3	+ 1, 2, 3, 4
УПД.3	Управление учетными записями	+	+ 1	+ 1, 2
УПД.4	Ограничение неуспешных и нерегламентированных попыток доступа в информационную систему	+	+ 1, 3, 5	+ 1, 2, 3, 4, 5, 6
УПД.5	Предупреждение пользователя при его доступе к информационной системе	+	+	+
УПД.6	Оповещение пользователя о предыдущем входе в информационную систему	+ 1	+ 1, 2, 5, 6	+ 1, 2, 4, 5, 6
УПД.7	Ограничение числа параллельных сеансов доступа		+	+ 1а
УПД.8	Блокирование сеанса доступа пользователя при неактивности	+ 1, 3, 4	+ 1, 2, 3, 4, 5	+ 1, 2, 3, 4, 5

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	+	+	+ 1
РСБ.3	Генерация временных меток при регистрации событий безопасности	+	+	+
РСБ.4	Требования к сбору, хранению и защите данных о событиях безопасности	+	+ 1	+ 1, 3
РСБ.5	Реагирование на сбои при регистрации событий безопасности	+	+	+ 1, 2
4. Защита виртуализации облачных технологий (ЗСВ)				
ЗСВ.1	Доверенная загрузка средства виртуализации и виртуальных машин	+	+ 1	+ 1, 2
ЗСВ.2	Контроль целостности средства виртуализации и виртуальных машин	+	+ 1, 2	+ 1, 2, 3, 4
ЗСВ.3	Регистрация событий безопасности в среде вирутализации	+	+	+
ЗСВ.4	Управление доступом в среде виртуализации	+	+	+
ЗСВ.5	Резервное копирование в среде виртуализации	+	+ 1	+ 1, 2
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 контейнерных сред и их оркестрации (ЗКО)				
ЗКС.1	Контроль целостности в контейнерных средах	+	+ 1, 2	+ 1, 2, 3, 4, 5, 6, 7
ЗКС.2	Регистрация событий безопасности в контейнерных средах	+	+ 1	+ 1
ЗКС.3	Управление доступом в контейнерных средах	+	+	+
ЗКС.4	Резервное копирование в контейнерных средах	+	+ 1	+ 1, 2
ЗКС.5	Изоляция контейнеров в контейнерной среде	+	+ 1	+ 1
ЗКС.6	Идентификация и аутентификация в контейнерной среде	+	+	+
ЗКС.7	Управление контейнерами и их образами (оркестрация)	+	+	+
ЗКС.8	Выявление уязвимостей в контейнерной среде	+	+ 1	+ 1
6. Защита сервисов электронной почты (ЗЭП)				
ЗЭП.1	Защита ящиков и сообщений электронной почты	+	+ 1, 2	+ 1, 2, 3
ЗЭП.2	Контроль доступа пользователей	+	+	+
ЗЭП.3	Защита от вредоносных вложений	+	+	+
ЗЭП.4	Защита от фишинга	+	+ 1	+ 1, 2, 3
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	+	+	+ 1
ЗВТ.2	Контроль доступа пользователей	+ 1	+ 1, 2	+ 1, 2
ЗВТ.3	Контроль и фильтрация трафика веб-приложений	+ 1	+ 1, 2	+ 1, 2, 3

ЗВТ.4	Регистрация событий безопасности в веб-приложениях и реагирование на них	+	+	+
ЗВТ.5	Проверка файлов веб-приложений на вредоносное программное обеспечение	+ 1	+ 1, 3	+ 1, 2, 3
ЗВТ.6	Защита систем управления контентом	+	+ 1, 2	+ 1, 2
8. Защита программных интерфейсов взаимодействия приложений API (ЗПИ)				
ЗПИ.1	Защита данных API	+ 1,2	+ 1, 2, 3	+ 1, 2, 3, 4
ЗПИ.2	Аутентификация и авторизация пользователей, устройств и приложений	+	+	+ 1
ЗПИ.3	Проверка на соответствие спецификации API	+ 1	+ 1, 2, 3	+ 1, 2, 4
9. Защита конечных устройств (ЗКУ)				
ЗКУ.1	Контроль доступа	+	+	+ 1
ЗКУ.2	Контроль целостности	+	+ 1	+ 2
ЗКУ.3	Антивирусная защита и обнаружение и предотвращение вторжений на конечных устройствах	+	+ 1, 2, 3	+ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10
ЗКУ.4	Мониторинг процессов и состояния устройства	+	+	+ 1, 2
ЗКУ.5	Контроль и фильтрация трафика на устройстве	+	+	+ 1, 2
ЗКУ.6	Регистрация, анализ и реагирование на события безопасности	+	+ 1, 2	+ 1, 2, 3
10. Защита мобильных устройств (ЗМУ)				
ЗМУ.1	Идентификация и аутентификация пользователей	+	+	+
ЗМУ.2	Контроль доступа	+	+	+
ЗМУ.3	Контроль целостности	+	+ 1, 2	+ 1, 2
ЗМУ.4	Защита данных	+ 1	+ 1, 2	+ 1, 2, 3, 4

ЗМУ.5	Антивирусная защита	+	+ 1	+ 1, 2
ЗМУ.6	Контроль приложений	+	+	+
ЗМУ.7	Ограничение и контроль функциональности	+	+	+
ЗМУ.8	Определение и контроль геопозиции	+	+ 1	+ 1
ЗМУ.9	Защита личных устройств	+	+	+
11. Защита устройств «Интернета вещей» (ЗИВ)				
ЗИВ.1	Идентификация и аутентификация	+	+	+
ЗИВ.2	Контроль доступа	+	+	+
ЗИВ.3	Защита данных	+	+ 1, 2	+ 1, 2, 3
ЗИВ.4	Контроль целостности	+	+	+ 1
12. Защита точек беспроводного доступа (ЗБД)				
ЗБД.1	Идентификация и аутентификация	+	+	+ 1, 2
ЗБД.2	Контроль доступа	+	+	+
ЗБД.3	Защита пользовательских данных	+	+	+
ЗБД.4	Контроль целостности			+
ЗБД.5	Ограничение уровней сигналов			+
13. Антивирусная защита (АВЗ)				
АВЗ.1	Антивирусная защита устройств и серверов	+	+	+
АВЗ.2	Антивирусная защита электронной почты	+	+ 1	+ 1
АВЗ.3	Антивирусная проверка сетевого трафика	+	+	+ 1
АВЗ.4	Применение замкнутой программной среды исполнения («песочницы»)		+	+ 1, 2, 3
14. Обнаружение и предотвращение вторжений на сетевом уровне (СОВ)				
СОВ.1	Обнаружение и предотвращение вторжений на периметре	+	+ 1, 2	+ 1, 2, 4, 5, 6, 7, 8, 9, 10
СОВ.2	Обнаружение и предотвращение вторжений в сегментах информационной системы	+	+ 1, 2	+ 1, 2
15. Сегментация и межсетевое экранирование (МСЭ)				

МСЭ.1	Сегментация сети	+ 1	+ 1	+ 1, 2, 3
МСЭ.2	Организация демилитаризованной зоны	+ 1	+ 1, 2, 3	+ 1, 2, 3
МСЭ.3	Контроль сетевого доступа и фильтрация трафика	+	+	+
МСЭ.4	Маскирование системы			
МСЭ.5	Создание ложных систем			
16. Защита от атак, направленных на отказ в обслуживании (ЗОО)				
ЗОО.1	Контроль и фильтрация входящего трафика	+	+	+ 1
ЗОО.2	Мониторинг состояния сервисов и интерфейсов	+	+	+ 1
ЗОО.3	Балансировка нагрузки	+	+	+ 1
ЗОО.4	Ограничение скорости	+	+	+
ЗОО.5	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	+ 1, 2	+ 1, 2	+ 1, 2, 3
ЗКС.2	Контроль атрибутов безопасности при сетевом взаимодействии	+	+	+
ЗКС.3	Обеспечение подлинности сетевых соединений	+	+	+
ЗКС.4	Контроль доступа к внешним ресурсам	+	+	+ 1
ЗКС.5	Контекстная проверка исходящего трафика			+
18. Защита систем искусственного интеллекта				
ЗИИ.1	Обеспечение безопасной разработки системы искусственного интеллекта	+	+	+
ЗИИ.2	Защита системы искусственного интеллекта в ходе эксплуатации	+	+	+

«+» - 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.