Зарегистрировано в Минюсте России 16 июня 2025 г. N 82619

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ПРИКАЗ

от 11 апреля 2025 г. N 117

ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ О ЗАЩИТЕ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ, ИНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ ГОСУДАРСТВЕННЫХ ОРГАНОВ, ГОСУДАРСТВЕННЫХ УНИТАРНЫХ ПРЕДПРИЯТИЙ, ГОСУДАРСТВЕННЫХ УЧРЕЖДЕНИЙ

В соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", пунктом 2 и подпунктом 9(1) пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085, приказываю:

1. Утвердить прилагаемые Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений.

2. Признать утратившими силу:

приказ ФСТЭК России от 11 февраля 2013 г. N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" (зарегистрирован Минюстом России 31 мая 2013 г., регистрационный N 28608);

приказ ФСТЭК России от 15 февраля 2017 г. N 27 "О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17" (зарегистрирован Минюстом России 14 марта 2017 г., регистрационный N 45933);

приказ ФСТЭК России от 28 мая 2019 г. N 106 "О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17" (зарегистрирован Минюстом России 13 сентября 2019 г., регистрационный N 55924);

приказ ФСТЭК России от 27 апреля 2020 г. N 61 "О внесении изменения в приказ ФСТЭК России от 28 мая 2019 г. N 106 "О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17" (зарегистрирован Минюстом России 12 мая 2020 г., регистрационный N 58322);

пункт 1 изменений, которые вносятся в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17, и в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. N 239, утвержденных приказом ФСТЭК России от 28 августа 2024 г. N 159 (зарегистрирован Минюстом России 24 октября 2024 г., регистрационный N 79900).

3. Установить, что аттестаты соответствия на государственные информационные системы и иные информационные системы, выданные до дня вступления в силу настоящего приказа, считаются действительными.

4. Настоящий приказ вступает в силу с 1 марта 2026 г.

Директор

Федеральной службы по техническому

и экспортному контролю

В. СЕЛИН

УТВЕРЖДЕНЫ

приказом ФСТЭК России

от 11 апреля 2025 г. N 117

ТРЕБОВАНИЯ О ЗАЩИТЕ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ, ИНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

ГОСУДАРСТВЕННЫХ ОРГАНОВ, ГОСУДАРСТВЕННЫХ УНИТАРНЫХ ПРЕДПРИЯТИЙ, ГОСУДАРСТВЕННЫХ УЧРЕЖДЕНИЙ

I. Общие положения

1. Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений (далее - Требования), применяются для обеспечения защиты (некриптографическими методами) информации, предотвращения несанкционированного доступа к информации, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения, блокирования доступа к информации, содержащейся в функционирующих на территории Российской Федерации государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений (далее соответственно - защита информации, информационные системы).

2. В случае передачи из государственной информационной системы информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации (далее - информация ограниченного доступа), информационная система, в которую передается информация ограниченного доступа, должна соответствовать требованиям о защите информации, установленным в соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" <1>. Состав передаваемой информации ограниченного доступа, цели ее защиты и уровень защищенности в соответствии с Требованиями должны устанавливаться обладателем информации, заказчиком, заключившим контракт на создание информационных систем, оператором информационных систем (далее - оператор (обладатель информации).

<1> Часть 8.1 статьи 14 Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

3. В муниципальных информационных системах защита информации обеспечивается в соответствии с Требованиями, если иное не установлено законодательством Российской Федерации.

4. При обработке и хранении в информационных системах информации, содержащей сведения, составляющие государственную тайну, ее защита должна обеспечиваться в соответствии с требованиями по технической защите информации, содержащей сведения, составляющие государственную тайну <2>.

<2> Подпункт 9(1) пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085 (далее - Положение о ФСТЭК России).

5. При обработке в информационных системах информации, содержащей персональные данные, должны применяться Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119, и Требования.

6. В случае если информационная система является значимым объектом критической информационной инфраструктуры Российской Федерации, защита содержащейся в ней информации должна обеспечиваться в соответствии с нормативными правовыми актами, принятыми на основании статьи 6 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации", и Требованиями.

7. В случае использования для защиты информации, содержащейся в информационных системах, шифровальных (криптографических) средств защиты информации должны применяться требования о защите информации, установленные ФСБ России в соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", и Требования.

8. Функционирование информационных систем на базе информационно-телекоммуникационной инфраструктуры <3> допускается при условии защиты информационно-телекоммуникационной инфраструктуры в соответствии с Требованиями.

<3> 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.

9. Оператор (обладатель информации) должен обеспечивать защиту информации в соответствии с Требованиями на всех стадиях (этапах) обработки и хранения информации, создания и развития (модернизации), эксплуатации и вывода из эксплуатации информационных систем в рамках функций, выполняемых ими в соответствии с Федеральным законом от 27 июля 2007 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

10. Оператор (обладатель информации) должен обеспечивать защиту информации, обрабатываемую в информационных системах, в целях:

а) недопущения (снижения возможности) наступления негативных последствий (событий) от нарушения конфиденциальности, целостности, доступности информации (далее - нарушение безопасности информации);

б) недопущения (снижения возможности) наступления негативных последствий (событий) от нарушения функционирования информационных систем вследствие реализации (возникновения) угроз безопасности информации.

11. Оператор (обладатель информации) должен определить цели защиты информации в зависимости от ожидаемых результатов от проведения мероприятий и принятия мер по защите информации. Негативные последствия (события) определяются оператором (обладателем информации) на основе информации, содержащейся в банке данных угроз безопасности информации ФСТЭК России <4>. Посредством выполнения оператором (обладателем информации) задач защиты информации должны быть достигнуты цели защиты

информации.

<4> Подпункт 21 пункта 8 Положения о ФСТЭК России.

12. Требования не распространяются на информационные системы Администрации Президента Российской Федерации, аппарата Совета Безопасности Российской Федерации, Федерального Собрания Российской Федерации, Аппарата Правительства Российской Федерации, Конституционного Суда Российской Федерации, Верховного Суда Российской Федерации, а также на информационные системы государственных органов, осуществляющих разведывательную и контрразведывательную деятельность, информационные системы, обеспечивающие управление вооружением, военной и специальной техникой.

II. Организация деятельности по защите информации и управление данной деятельностью

13. Оператор (обладатель информации) должен организовывать деятельность по защите информации и управлять ею в соответствии с Требованиями.

14. Организация деятельности по защите информации должна включать:

а) разработку и утверждение политики защиты информации, содержащей в том числе:

область действия политики, включая перечень информации, информационных систем, компонентов информационно-телекоммуникационной инфраструктуры, подлежащих защите в соответствии с Требованиями;

цели и задачи защиты информации;

принципы защиты информации;

перечни объектов защиты, включая программные, программно-аппаратные средства, информационные системы, сети и подсети, образующие информационно-телекоммуникационную инфраструктуру;

категории лиц, участвующих в защите информации, их обязанности (функции) и полномочия;

состав организационной системы управления деятельностью по защите информации и схему взаимодействия ее элементов;

ответственность работников за нарушение требований о защите информации и установленных оператором (обладателем информации) правил обработки информации;

б) определение лиц, ответственных за защиту информации;

в) применение программных, программно-аппаратных средств, предназначенных для защиты информации;

г) разработку и утверждение внутренних стандартов по защите информации, содержащих в

том числе:

требования к первичной идентификации лиц, обладающих правами доступа к информационным системам и (или) содержащейся в них информации и их использованию (далее - пользователи);

требования к применяемым моделям доступа пользователей;

перечень разрешенного и (или) запрещенного для использования программного обеспечения;

требования к типовым конфигурациям и настройкам программных, программно-аппаратных средств;

требования к конфигурациям и настройкам программных, программно-аппаратных средств, предназначенных для обеспечения доступа пользователей из информационных систем к информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет");

требования к конфигурациям и настройкам программных, программно-аппаратных средств, предназначенных для обеспечения удаленного доступа пользователей к информационным системам и содержащейся в них информации, включая требования к обеспечению безопасной дистанционной работы;

ограничения и запреты действий для пользователей при использовании и обеспечении эксплуатации ими информационных систем;

требования к защите физических и виртуальных устройств информационных систем, имеющих постоянный доступ к сети "Интернет" (далее - конечные устройства);

требования к защите мобильных устройств, планшетных, переносных компьютеров, применяемых пользователями для доступа к информационным системам (за исключением мобильных устройств, предназначенных для доступа к сайтам сети "Интернет" и иным публичным веб-ресурсам) (далее - мобильные устройства);

требования к непрерывности функционирования информационных систем;

требования к резервному копированию информации, программного обеспечения и его конфигураций;

требования к сбору, регистрации и анализу событий, связанных с возможным нарушением безопасности информации, нарушением функционирования информационных систем, реализацией угроз безопасности информации (далее - события безопасности);

требования к защите информации при подключении к информационным системам иных информационных систем, включая требования к каналам передачи данных при взаимодействии с такими информационными системами;

д) разработку и утверждение внутренних регламентов по защите информации, содержащих в том числе:

порядок создания, учета, изменения и блокирования, контроля, удаления учетных записей;

порядок создания, учета, изменения и блокирования, контроля, удаления привилегированных учетных записей;

порядок создания, изменения, блокирования, контроля, удаления аутентификационной информации и средств аутентификации;

порядок предоставления пользователям удаленного доступа к информационным системам и содержащейся в них информации;

порядок и условия 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;

порядок 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);

порядок предоставления пользователям доступа из информационных систем в сеть "Интернет" и контроля ее использования;

порядок повышения уровня знаний и информированности пользователей по вопросам защиты информации;

порядок выявления, оценки и устранения уязвимостей информационных систем (далее - управление уязвимостями);

порядок получения, оценки, тестирования и применения обновлений программных, программно-аппаратных средств (далее - управление обновлениями);

порядок обработки, хранения и обращения с информацией ограниченного доступа;

порядок обеспечения физической защиты информационных систем;

порядок разработки безопасного программного обеспечения <5> в случае его самостоятельной разработки оператором (обладателем информации);

<5> Пункт 3.2 национального стандарта Российской Федерации ГОСТ Р 56939-2024 "Защита информации. Разработка безопасного программного обеспечения. Общие требования", утвержденного и введенного в действие приказом Росстандарта от 24 октября 2024 г. N 1504-ст (М., ФГБУ "РСТ", 2024) (далее - ГОСТ Р 56939-2024).

порядок вывода в контур промышленной эксплуатации сервисов, доступ к которым осуществляется с использованием сети "Интернет", в случае наличия таких сервисов;

порядок мониторинга информационной безопасности <6> информационных систем;

<6> Пункт 3.7 национального стандарта Российской Федерации ГОСТ Р 59547-2021 "Защита информации. Мониторинг информационной безопасности. Общие положения", утвержденного и введенного в действие приказом Росстандарта от 27 июля 2021 г. N 656-ст (М., ФГБУ "РСТ", 2021) (далее - ГОСТ Р 59547-2021).

порядок восстановления штатного функционирования информационных систем и тестирования процессов восстановления;

порядок контроля уровня защищенности информации, содержащейся в информационных системах;

е) выделение организационных, технических и иных ресурсов, необходимых для защиты информации.

15. При разработке политики защиты информации должны учитываться все информационные системы оператора (обладателя информации), а также информационно-телекоммуникационная инфраструктура, если информационные системы функционируют на базе информационно-телекоммуникационной инфраструктуры. Политика защиты информации утверждается руководителем оператора (обладателя информации) или уполномоченным руководителем оператора (обладателя информации) лицом (далее - ответственное лицо) и обязательна для исполнения всеми подразделениями (работниками) оператора (обладателя информации) в части, их касающейся.

16. Организации, которым 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), должны быть ознакомлены с политикой защиты информации в части, их касающейся.

Обязанность подрядной организации по выполнению политики защиты информации должна быть определена в документах оператора (обладателя информации), на основании которых в том числе передается информация, предоставляется доступ к информационным системам оператора (обладателя информации) или содержащейся в них информации.

17. Защиту информации должен организовывать руководитель оператора (обладателя информации) или по его решению ответственное лицо.

18. Обязанности (функции) и полномочия ответственного лица по организации деятельности по защите информации, управлению защитой информации, а также по организации контроля за данной деятельностью у оператора (обладателя информации) должны быть включены в должностные обязанности (трудовые функции) ответственного лица. Состав обязанностей (функций) и полномочий ответственного лица должен быть достаточен для организации деятельности по защите информации и управления этой деятельностью в соответствии с Требованиями, а также организации контроля за данной деятельностью у оператора (обладателя информации).

19. Руководитель оператора (обладателя информации), ответственное лицо должны создать (определить) структурное подразделение или назначает отдельных специалистов, на которых возлагаются обязанности (функции) по защите информации (далее - структурное подразделение (специалисты) по защите информации).

Функции и полномочия по защите информации структурного подразделения по защите информации определяются в положении о структурном подразделении или ином документе, в соответствии с которым функционирует структурное подразделение <7>. Обязанности (функции) и полномочия специалистов по защите информации по проведению мероприятий и принятию мер по защите информации должны быть установлены в их должностных обязанностях (трудовых функциях). Состав обязанностей (функций) и полномочий по защите информации структурного подразделения (специалистов) по защите информации должен быть достаточен для проведения мероприятий и принятия мер по защите информации в соответствии с Требованиями.

<7> Типовое положение о структурном подразделении органа (организации),

обеспечивающем информационную безопасность органа (организации), утвержденное постановлением Правительства Российской Федерации от 15 июля 2022 г. N 1272.

В случае наличия у оператора (обладателя информации) структурного подразделения, на которое возложены функции по обеспечению информационной безопасности <8>, защита информации может быть возложена на указанное подразделение.

<8> Подпункт "б" пункта 1 Указа Президента Российской Федерации от 1 мая 2022 г. N 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации".

20. Работники структурного подразделения (специалисты) по защите информации должны обладать компетенциями, необходимыми для выполнения возложенных на них обязанностей (функций) по защите информации в соответствии с Требованиями. Не менее 30 процентов работников структурного подразделения по защите информации должны иметь профессиональное образование по специальности или направлению подготовки в области информационной безопасности или пройти обучение по программе профессиональной переподготовки в области информационной безопасности.

21. Структурное подразделение (специалисты) по защите информации должно (должны) обеспечивать защиту информации во взаимодействии с подразделениями (работниками), использующими информационные системы, и подразделениями (работниками), обеспечивающими эксплуатацию информационных систем.

22. Подразделения (работники), использующие информационные системы, должны участвовать в проведении мероприятий и принятии мер по защите информации в объеме, установленном оператором (обладателем информации) во внутренних стандартах и регламентах по защите информации.

Подразделения, обеспечивающие эксплуатацию информационных систем, должны проводить мероприятия и принимать меры по защите информации в ходе сопровождения, обслуживания информационных систем, поставки комплектующих и иных видов работ по эксплуатации информационных систем в объеме, установленном оператором (обладателем информации) во внутренних стандартах и регламентах по защите информации.

23. Структурным подразделением (специалистами) по защите информации должны применяться программные, программно-аппаратные средства, позволяющие обеспечить выполнение возложенных на них обязанностей (функций) по защите информации, в том числе по выявлению угроз безопасности информации, обнаружению и предотвращению вторжений, проведению контроля уровня защищенности информации, содержащейся в информационных системах, мониторингу информационной безопасности информационных систем, выявлению уязвимостей, контролю настроек и конфигураций информационных систем, а также средства и системы, предназначенные для автоматизации и аналитической поддержки деятельности по защите информации.

Состав программных, программно-аппаратных средств, необходимых структурному подразделению (специалистам) по защите информации для выполнения возложенных на них обязанностей (функций), определяется во внутренних стандартах и регламентах по защите информации.

24. Для проведения мероприятий и принятия мер по защите информации оператором

(обладателем информации) могут привлекаться организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации <9> (далее - специализированные организации). Состав проводимых специализированными организациями мероприятий и принимаемых ими мер по защите информации, используемых при этом программных, программно-аппаратных средств, предназначенных для защиты информации, определяется оператором (обладателем информации). Работники структурного подразделения (специалисты) по защите информации оператора (обладателя информации) должны привлекаться к приемке результатов работ и услуг, выполняемых (оказываемых) специализированными организациями.

<9> Пункт 5 части 1 статьи 12 Федерального закона от 4 мая 2011 г. N 99-ФЗ "О лицензировании отдельных видов деятельности".

25. Оператором (обладателем информации) должны быть разработаны и утверждены:

внутренние стандарты по защите информации, устанавливающие требования к реализации мер по защите информации применительно к особенностям деятельности оператора (обладателя информации) и функционирования информационных систем;

внутренние регламенты по защите информации, содержащие порядок проведения мероприятий или описание реализуемых процессов по защите информации применительно к особенностям деятельности оператора (обладателя информации) и функционирования информационных систем.

Внутренние стандарты и регламенты по защите информации утверждаются руководителем оператора (обладателя информации) или ответственным лицом.

Область действия внутренних стандартов и регламентов по защите информации определяется оператором (обладателем информации).

26. Внутренние стандарты и регламенты по защите информации доводятся до пользователей, а также подрядных организаций в части, их касающейся.

Внутренние стандарты и регламенты по защите информации подлежат исполнению пользователями в части, их касающейся.

Обязанность подрядной организации по выполнению внутренних стандартов и регламентов по защите информации должна быть определена в документах оператора (обладателя), на основании которых передается информация, предоставляется доступ к информационным системам оператора (обладателя информации) или содержащейся в них информации.

27. Структурное подразделение (специалисты) по защите информации должно (должны) разрабатывать и представлять руководителю оператора (обладателя информации), ответственному лицу обоснованные предложения по организационным, материально-техническим и иным обеспечивающим ресурсам, необходимым для проведения мероприятий и принятия мер по защите информации, с указанием сведений о целях защиты информации, на достижение которых требуются ресурсы, и перечня негативных последствий (событий), наступление которых прогнозируется в случае отсутствия ресурсов.

Руководитель оператора (обладателя информации), ответственное лицо на основе представленных предложений и в пределах имеющихся средств предусматривает выделение организационных, материально-технических и иных обеспечивающих ресурсов для

проведения мероприятий и принятия мер по защите информации, привлечения при необходимости дополнительных сил и средств для защиты информации в соответствии с Требованиями на всех этапах жизненного цикла информационных систем.

28. Управление деятельностью по защите информации должно осуществляться в рамках функционирующей организационной системы управления, возглавляемой руководителем оператора (обладателя информации) или по его решению ответственным лицом. Управление деятельностью по защите информации должно включать:

а) разработку и планирование мероприятий и мер по защите информации;

б) проведение мероприятий и принятие мер по защите информации;

в) проведение оценки состояния защиты информации;

г) совершенствование мероприятий и мер по защите информации.

29. При разработке и планировании мероприятий и мер по защите информации должны быть:

а) определены события в информационных системах, наступление которых может привести к нарушению целей защиты информации, установленных в политике защиты информации;

б) определены информационные системы, программные, программно-аппаратные средства, несанкционированный доступ к которым и (или) воздействие на которые могут привести к нарушению целей защиты информации, установленных в политике защиты информации;

в) выявлены и оценены угрозы безопасности информации, реализация (возникновение) которых может привести к нарушению целей защиты информации, установленных в политике защиты информации (далее - угрозы безопасности информации);

г) определены состав и сроки проведения мероприятий и принятия мер по защите информации и оценены необходимые для этого ресурсы.

30. Проводимые мероприятия и принимаемые меры по защите информации должны быть направлены на блокирование (нейтрализацию) актуальных для информационной системы угроз безопасности информации (далее - актуальные угрозы) в соответствии с целями защиты информации, определенными в политике защиты информации.

В зависимости от целей защиты информации мероприятия и меры по защите информации должны быть направлены на:

а) исключение утечки информации ограниченного доступа и иной конфиденциальной информации;

б) предотвращение несанкционированного доступа к информационным системам и содержащейся в них информации, обнаружение фактов несанкционированного доступа и реагирование на них;

в) предотвращение несанкционированной модификации информации, обнаружение фактов несанкционированной модификации и реагирование на них;

г) предотвращение несанкционированной подмены информации, обнаружение фактов несанкционированной подмены и реагирование на них;

д) предотвращение несанкционированного удаления информации и программного обеспечения, обнаружение фактов несанкционированного удаления и реагирование на них;

е) исключение или существенное затруднение отказа в обслуживании авторизованным пользователям информационных систем;

ж) недопущение использования информационных систем и содержащейся в них информации не по назначению;

з) исключение или существенное затруднение нарушения функционирования (работоспособности) информационных систем;

и) недопущение распространения с использованием информационных систем противоправной информации;

к) обеспечение возможности восстановления в установленные оператором (обладателем информации) сроки доступа авторизованных пользователей к информационным системам и содержащейся в них информации, заблокированной вследствие реализации (возникновения) угроз безопасности информации;

л) обеспечение возможности восстановления в установленные оператором (обладателем информации) сроки информации, модифицированной или уничтоженной вследствие реализации (возникновения) угроз безопасности информации.

31. Оценка состояния защиты информации должна проводиться на основе определения оператором (обладателем информации):

а) показателя, характеризующего текущее состояние защиты информации от базового уровня угроз безопасности информации (далее - показатель защищенности $К_{зи}$);

б) показателя, который определяет достаточность и эффективность проведения мероприятий по защите информации (далее - показатель уровня зрелости $П_{зи}$).

Для определения значений и расчета показателя защищенности $К_{зи}$ и показателя уровня зрелости $П_{зи}$ должны применяться методические документы, утвержденные ФСТЭК России в соответствии с абзацем вторым пункта 5 и подпунктом 4 пункта 8 Положения о ФСТЭК России (далее - методические документы ФСТЭК России).

32. Расчет и оценка показателя защищенности $К_{зи}$ должны проводиться оператором (обладателем информации) не реже одного раза в шесть месяцев. Расчет и оценка показателя уровня зрелости $П_{зи}$ должны проводиться оператором (обладателем информации) не реже одного раза в два года.

О полученных по результатам оценки значениях показателя защищенности $К_{зи}$ и показателя уровня зрелости $П_{зи}$ в случае их несоответствия нормированным значениям, указанным в методических документах ФСТЭК России, в течение 3 календарных дней со дня завершения такой оценки информируется руководитель оператора (обладателя информации) для принятия решения о проведении мероприятий по совершенствованию защиты информации и принятии мер по повышению уровня защищенности информации, содержащейся в информационных системах.

Результаты оценки показателя защищенности $К_{зи}$ и показателя уровня зрелости $П_{зи}$ в срок не позднее 5 рабочих дней после дня их расчета должны направляться оператором (обладателем информации) в ФСТЭК России в целях мониторинга текущего состояния технической защиты информации и оценки эффективности деятельности по технической защите информации <10>.

<10> Подпункты 6(1) и 6(5) пункта 8 Положения о ФСТЭК России.

33. По решению руководителя оператора (обладателя информации), ответственного лица структурным подразделением (специалистами) по защите информации с участием подразделений (работников), использующих информационные системы, подразделений (работников), обеспечивающих эксплуатацию информационных систем, разрабатывается план мероприятий по совершенствованию защиты информации, содержащейся в информационных системах, в котором в том числе указываются наименования мероприятий, сроки их выполнения, подразделения (работники), ответственные за реализацию каждого мероприятия.

План утверждается руководителем оператора (обладателя информации), ответственным лицом и доводится до подразделений (работников) оператора (обладателя информации) в части, их касающейся. Результатом реализации мероприятий плана должно быть достижение значений показателя защищенности $К_{зи}$ и показателя уровня зрелости $П_{зи}$ не ниже нормированных значений, указанных в методических документах ФСТЭК России.

III. Проведение мероприятий и принятие мер по защите информации

34. Для достижения целей защиты информации оператором (обладателем информации) должны проводиться следующие мероприятия:

а) выявление и оценка угроз безопасности информации;

б) контроль конфигураций информационных систем;

в) управление уязвимостями;

г) управление обновлениями;

д) обеспечение защиты информации при обработке, хранении и обращении с информацией ограниченного доступа;

е) обеспечение защиты информации при применении конечных устройств;

ж) обеспечение защиты информации при применении мобильных устройств;

з) обеспечение защиты информации при удаленном доступе пользователей к информационным системам;

и) обеспечение защиты информации при беспроводном доступе пользователей к информационным системам;

к) обеспечение защиты информации при предоставлении пользователям доступа к информационным системам, предусматривающего чтение, выполнение, изменение, запись, удаление программ и (или) данных в информационных системах (далее - привилегированный доступ);

л) обеспечение мониторинга информационной безопасности;

м) обеспечение разработки безопасного программного обеспечения;

н) обеспечение физической защиты информационных систем;

о) обеспечение непрерывности функционирования информационных систем при возникновении нештатных ситуаций;

п) повышение уровня знаний и информированности пользователей по вопросам защиты информации;

р) обеспечение защиты информации при взаимодействии с подрядными организациями;

с) обеспечение защиты от компьютерных атак, направленных на отказ в обслуживании;

т) обеспечение защиты информации при использовании искусственного интеллекта <11>;

<11> Подпункт "а" пункта 5 Национальной стратегии развития искусственного интеллекта на период до 2030 года, утвержденной Указом Президента Российской Федерации от 10 октября 2019 г. N 490 (далее - Национальная стратегия развития искусственного интеллекта).

у) реализация в информационных системах мер по их защите и защите содержащейся в них информации;

ф) проведение контроля уровня защищенности информации, содержащейся в информационных системах;

х) обеспечение непрерывного взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

35. Достаточность и эффективность проводимых мероприятий (реализованных процессов) оцениваются оператором по результатам определения показателя уровня зрелости $П_{зи}$ в соответствии с пунктами 32 и 33 Требований.

36. Мероприятия по выявлению и оценке угроз безопасности информации должны предусматривать определение в ходе создания информационных систем актуальных угроз и разработку в случаях, установленных требованиями к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденными постановлением Правительства Российской Федерации от 6 июля 2015 г. N 676, моделей угроз безопасности информации, а также своевременное выявление актуальных угроз и их оценку в ходе эксплуатации информационных систем.

Модель угроз безопасности информации в случае ее разработки должна использоваться в качестве исходных данных для разработки и внедрения мер по защите информации, а также для выбора средств защиты информации и их функциональных возможностей в ходе создания (развития) подсистем защиты информации информационных систем. Решение о необходимости разработки модели угроз безопасности информации в ходе создания негосударственных информационных систем принимается руководителем оператора (обладателя информации), ответственным лицом.

В ходе эксплуатации информационных систем должен быть обеспечен поиск данных и признаков, идентифицирующих наличие актуальных угроз, проведена приоритизация выявленных угроз безопасности информации, осуществлено оповещение подразделений

(работников) оператора (обладателя информации) о выявленных актуальных угрозах. При наличии признаков реализации (возникновения) актуальных угроз должны быть приняты меры по их блокированию (нейтрализации).

37. Мероприятия по контролю конфигураций информационных систем должны исключать несанкционированное изменение состава программных, программно-аппаратных средств информационных систем, их настроек и конфигураций, установленных во внутренних стандартах по защите информации, а также обеспечивать обнаружение фактов несанкционированных изменений и выявление причин изменений.

Контроль конфигураций информационных систем должен осуществляться на основе анализа результатов учета ИТ-активов <12> и (или) сведений, содержащихся в автоматизированных системах хранения и управления данными об информационных системах и их конфигурациях (при наличии систем инвентаризации ИТ-активов). Структурному подразделению (специалистам) по защите информации должен быть обеспечен доступ к указанным сведениям.

<12> 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.

38. Мероприятия по управлению уязвимостями должны включать выявление уязвимостей информационных систем, оценку их критичности, определение методов и приоритетов устранения уязвимостей, а также контроль за устранением уязвимостей.

Устранение уязвимостей, которые могут быть использованы нарушителями, или исключение возможности их использования за счет применения компенсирующих мер должно проводиться оператором (обладателем информации):

в отношении уязвимостей критического уровня опасности <13> - в срок не более 24 часов;

<13> Пункт 5.2.18 национального стандарта Российской Федерации ГОСТ Р 56545-2015 "Защита информации. Уязвимости информационных систем. Правила описания уязвимостей", утвержденного и введенного в действие приказом Росстандарта от 19 августа 2015 г. N 1180-ст (М., ФГБУ "РСТ", 2021).

в отношении уязвимостей высокого уровня опасности - в срок не более 7 календарных дней.

В отношении уязвимостей среднего и низкого уровней опасности сроки и порядок их устранения определяются во внутреннем регламенте по защите информации исходя из особенностей функционирования информационных систем.

При выявлении уязвимостей информационных систем, сведения о которых отсутствуют в банке данных угроз безопасности информации ФСТЭК России, оператор (обладатель информации) в срок не более 5 рабочих дней с даты такого выявления должен направить информацию об уязвимости в ФСТЭК России для оценки необходимости включения выявленной уязвимости в банк данных угроз безопасности информации ФСТЭК России <14>.

<14> Подпункт 21 пункта 8 Положения о ФСТЭК России.

39. Мероприятия по управлению обновлениями должны включать проведение проверки подлинности и целостности обновлений программных, программно-аппаратных средств, тестировании обновлений до их применения в контурах промышленной эксплуатации информационных систем, выдаче разрешения подразделениям (работникам) оператора (обладателя информации) на применение обновлений программных, программно-аппаратных средств в контурах промышленной эксплуатации информационных систем с использованием безопасных настроек и конфигураций, установленных во внутренних стандартах по защите информации. Бесконтрольная установка 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.

40. Мероприятия по защите информации при обработке, хранении и обращении с информацией ограниченного доступа должны исключать:

неправомерное распространение информации ограниченного доступа вне зависимости от формы ее представления, в том числе с использованием информационно-телекоммуникационных сетей и сети "Интернет";

доступ к информации ограниченного доступа лиц, для которых информация не предназначена и (или) для которых такой доступ запрещен.

Проводимые мероприятия должны включать определение информации ограниченного доступа и предназначенных для ее хранения программно-аппаратных средств, а также контроль и регистрацию всех фактов доступа пользователей к программно-аппаратным средствам, в которых хранится информация ограниченного доступа.

Контроль обработки, хранения информации ограниченного доступа в программно-аппаратных средствах и ее передачи должен осуществляться в соответствии с внутренним регламентом по защите информации. О фактах неправомерного распространения информации ограниченного доступа и (или) доступа к средствам ее обработки и хранения должен быть незамедлительно проинформирован руководитель оператора (обладателя информации), ответственное лицо.

41. Мероприятия по обеспечению защиты информации при применении конечных устройств информационных систем должны исключать возможность 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".

Защита конечных устройств информационных систем должна включать реализацию в них в соответствии с Требованиями мер по защите информации от несанкционированного доступа и проведении на них мониторинга и анализа процессов и событий с целью выявления актуальных угроз, а также предупреждении о произошедших событиях безопасности. Контроль использования конечных устройств должен осуществляться в соответствии с внутренними стандартами и регламентами по защите информации.

42. Посредством проведения мероприятий по обеспечению защиты информации при применении мобильных устройств должна быть исключена возможность 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.

При применении пользователями мобильных устройств для доступа к информационным системам и содержащейся в них информации в целях выполнения своих обязанностей (функций) оператор (обладатель информации) должен принимать меры по защите информационных систем и содержащейся в них информации, в том числе:

обеспечивать защиту каналов передачи данных;

осуществлять доступ пользователей с применением строгой аутентификации <15>.

<15> Пункт 3.54 национального стандарта Российской Федерации ГОСТ Р 58833-2020 "Защита информации. Идентификация и аутентификация. Общие требования", утвержденного и введенного в действие приказом Росстандарта от 10 апреля 2020 г. N 159-ст (М., ФГБУ "Институт стандартизации", 2020).

Пользователем должен быть исключен несанкционированный доступ к мобильному устройству.

43. Применение пользователями личных мобильных устройств для доступа к информационным системам и содержащейся в них информации с целью выполнения своих обязанностей (функций) допускается в случае соответствия мобильных устройств Требованиям и наличия у оператора (обладателя информации) возможности контроля использования мобильных устройств.

44. Контроль использования мобильных устройств должен осуществляться в соответствии с внутренними стандартами и регламентами по защите информации.

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

46. Посредством проведения мероприятий по обеспечению защиты информации при удаленном доступе пользователей должна быть исключена возможность 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.

При удаленном доступе пользователей к информационным системам и содержащейся в них информации в целях выполнения своих обязанностей (функций) оператором (обладателем информации) должны приниматься меры по защите информационных систем и содержащейся в них информации, обеспечиваться защита каналов передачи данных и программно-аппаратных средств, с использованием которых осуществляется удаленный

доступ, исключаться несанкционированный доступ к удаленно подключаемому программно-аппаратному средству пользователя.

Удаленный доступ пользователей в целях выполнения своих обязанностей (функций) должен осуществляться с использованием программно-аппаратных средств, выделенных оператором (обладателем информации) и соответствующих Требованиям. По согласованию со структурным подразделением (специалистами) по защите информации допускается предоставление удаленного доступа к информационным системам с использованием личных программно-аппаратных средств пользователя оператора (обладателя информации) при условии применения для удаленного доступа сертифицированных средств обеспечения безопасной дистанционной работы <16>, средств антивирусной защиты и иных средств защиты информации, исключающих угрозы безопасности информации, связанные с удаленным доступом.

<16> Приказ ФСТЭК России от 16 февраля 2021 г. N 32 (зарегистрирован Минюстом России 15 июня 2021 г., регистрационный N 63867).

Удаленный доступ пользователей к информационным системам в целях выполнения своих обязанностей (функций) должен осуществляться с использованием сетей связи, расположенных на территории Российской Федерации, посредством применения средств защиты канала передачи данных, и строгой аутентификации пользователей.

При удаленном доступе пользователей к информационным системам и содержащейся в них информации, не связанном с выполнением пользователями своих обязанностей (функций), в том числе при доступе к общедоступной информации, оператором (обладателем информации) должны приниматься меры по защите информационных систем и содержащейся в них информации и, при необходимости, обеспечиваться защита каналов передачи данных, используемых для осуществления удаленного доступа.

Контроль удаленного доступа пользователей к информационным системам должен осуществляться в соответствии с внутренними стандартами и регламентами по защите информации.

47. Посредством проведения мероприятий по обеспечению защиты информации при беспроводном доступе пользователей к информационным системам должна быть исключена возможность 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.

При беспроводном доступе пользователей к информационным системам и содержащейся в них информации в целях выполнения своих обязанностей (функций) оператором (обладателем информации) должны приниматься меры по защите информационных систем и содержащейся в них информации, обеспечиваться защита беспроводных каналов передачи данных и программно-аппаратных средств, с использованием которых осуществляется беспроводной доступ. Посредством формирования конфигурации и настроек, уровней сигналов точек беспроводного доступа, используемых для подключения пользователей к информационным системам в целях выполнения своих обязанностей (функций), должна быть исключена возможность подключения к ним лиц, не имеющих прав доступа к информационным системам. Указанные точки беспроводного доступа должны быть однозначно идентифицированы в информационных системах, а также определены места их

размещения.

Точки беспроводного доступа и построенные на их основе беспроводные сети связи, используемые для доступа пользователей к информационным системам и содержащейся в них информации в целях выполнения ими своих обязанностей (функций), должны быть изолированы от беспроводных сетей связи, предназначенных для доступа к сети "Интернет" и (или) общедоступной информации оператора (обладателя информации).

48. Посредством проведения мероприятий по обеспечению защиты информации при предоставлении привилегированного доступа должна быть исключена возможность получения привилегированного доступа к информационным системам лицами, для которых такой доступ должен быть исключен, а также использования повышенных прав доступа с нарушением внутренних стандартов и регламентов по защите информации.

Для получения привилегированного доступа должны быть созданы привилегированные учетные записи. Привилегированные учетные записи должны иметь права доступа, минимально необходимые для выполнения пользователями возложенных на них обязанностей (функций), в соответствии с принятыми в информационных системах моделями доступа пользователей. Привилегированные учетные записи, имеющие права по созданию других привилегированных учетных записей, должны быть персонифицированными.

Привилегированный доступ должен осуществляться с применением строгой аутентификации, а в случае технической невозможности применения строгой аутентификации - с использованием усиленной многофакторной аутентификации.

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.

Неиспользуемые привилегированные учетные записи должны быть заблокированы и удалены в соответствии с внутренними стандартами и регламентами по защите информации.

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.

Все действия по доступу пользователей с использованием привилегированных учетных записей подлежат регистрации. Контроль использования привилегированных учетных записей должен осуществляться в соответствии с внутренними стандартами и регламентами по защите информации.

49. Мероприятия по осуществлению мониторинга информационной безопасности должны предусматривать сбор данных о событиях безопасности, их обработке и анализе, а также выявление признаков реализации угроз безопасности информации и (или) нарушений требований внутренних стандартов и регламентов по защите информации. Мероприятия по осуществлению мониторинга информационной безопасности должны проводиться в отношении всех информационных систем, за исключением локальных и изолированных информационных систем, в которых должен обеспечиваться контроль журналов регистрации событий безопасности.

Мероприятия по мониторингу информационной безопасности должны осуществляться в соответствии с разделами 4 и 5 ГОСТ Р 59547-2021.

В ходе проведения мониторинга информационной безопасности для анализа зафиксированных событий безопасности и выявленных в них признаков реализации актуальных угроз допускается использование доверенных технологий искусственного интеллекта <17>.

<17> Подпункт "ц" пункта 5 Национальной стратегии развития искусственного интеллекта.

Структурное подразделение (специалисты) по защите информации оператора (обладателя информации) с периодичностью и в сроки, установленные внутренним регламентом по защите информации, должно (должны) разработать и представить руководителю оператора (обладателя информации), ответственному лицу отчет о результатах мониторинга, который в том числе должен содержать типы событий безопасности, обнаруженные по результатам мониторинга, и связанные с ними компьютерные инциденты (при их наличии), а также рекомендации по их анализу и (или) устранению. Последний в текущем году отчет о результатах мониторинга или итоговый отчет за текущий год (в случае его разработки) после представления руководителю оператора (обладателя информации) направляется оператором (обладателем информации) в ФСТЭК России в целях мониторинга текущего состояния технической защиты информации <18>.

<18> Подпункт 6(1) пункта 8 Положения о ФСТЭК России.

50. Мероприятия по разработке безопасного программного обеспечения должны быть направлены на предотвращение появления, выявление и устранение уязвимостей в разрабатываемом оператором (обладателем информации) программном обеспечении. Мероприятия по разработке безопасного программного обеспечения проводятся в случае осуществления оператором (обладателем информации) самостоятельной разработки программного обеспечения, применяемого в информационных системах.

В случае самостоятельной разработки оператором (обладателем информации) программного обеспечения, предназначенного для использования в информационных системах, 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.

51. Посредством проведения мероприятий по обеспечению физической защиты информационных систем должна быть исключена возможность несанкционированного физического доступа к программно-аппаратным средствам обработки и хранения информации.

Физический доступ к программно-аппаратным средствам информационных систем, предназначенным для обработки и хранения информации, должен быть предоставлен пользователям, которым указанный доступ 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.

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 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.

52. Посредством проведения мероприятий по обеспечению непрерывности функционирования информационных систем при возникновении нештатных ситуаций должна быть обеспечена возможность 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.

53. 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, классов защищенности информационных систем, устанавливаемых оператором (обладателем информации) в соответствии с приложением к Требованиям, и должны составлять:

для информационных систем 1 класса защищенности - не более 24 часов с момента обнаружения нарушения функционирования;

для информационных систем 2 класса защищенности - не более 7 календарных дней с момента обнаружения нарушения функционирования;

для информационных систем 3 класса защищенности - не более 4 недель с момента обнаружения нарушения функционирования.

54. Программные, программно-аппаратные средства, позволяющие обеспечить выполнение значимых функций, должны быть развернуты в отказоустойчивой конфигурации, обеспечивающей восстановление выполнения значимых функций в установленный оператором (обладателем информации) во внутренних стандартах и регламентах по защите информации интервал времени восстановления.

55. Оператором (обладателем информации) должно быть обеспечено:

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

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

Периодичность резервного копирования, количество, типы носителей, места хранения резервных копий и уровень критичности резервируемой информации определяются во внутренних стандартах и регламентах по защите информации.

Оператор (обладатель информации) должен проводить периодические, но не реже одного раза в два года, проверки, в том числе в форме тренировок, 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 обеспечиваться возможность выполнения пользователями значимых функций, в том числе в неавтоматизированном режиме, в соответствии с внутренними регламентами по защите информации.

56. Мероприятия по повышению уровня знаний и информированности пользователей информационных систем по вопросам защиты информации должны включать:

а) доведение до пользователей информационных материалов, в том числе в форме памяток, баннеров, буклетов, по актуальным вопросам защиты информации;

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

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

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

57. 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, у которых отсутствуют знания по вопросам защиты информации, должно быть организовано повторное прохождение обучающих курсов по вопросам защиты информации.

58. Посредством проведения мероприятий по защите информации при взаимодействии оператора (обладателя информации) с подрядными организациями должна быть исключена

возможность 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.

Оператором (обладателем информации) в отношении подрядной организации должны быть установлены требования по обеспечению защиты информации, к которой получен доступ.

Не допускается копирование подрядными организациями информации, к которой им предоставлен доступ, если такое копирование не предусмотрено в документах оператора (обладателя информации), на основании которых подрядным организациям предоставлен доступ к информационным системам.

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. 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 (обладателем информации) на основании Требований во внутренних стандартах и регламентах по защите информации.

Разработка (развитие) и (или) тестирование программного обеспечения подрядными организациями непосредственно в эксплуатируемых информационных системах оператора (обладателя информации) не допускается. Для проведения работ по разработке (развитию) и (или) тестированию программного обеспечения работникам подрядных организаций должен быть предоставлен доступ к 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.

59. Посредством проведения мероприятий по организации и проведению защиты от компьютерных атак, направленных на отказ в обслуживании, должна быть исключена возможность блокирования авторизованным пользователям 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".

Оператором (обладателем информации) должно быть обеспечено взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также взаимодействие в автоматизированном режиме с Центром мониторинга и управления сетью связи общего пользования <19>.

<19> Пункт 5 Положения о Центре мониторинга и управления сетью связи общего пользования, утвержденного приказом Роскомнадзора от 31 июля 2019 г. N 225 (зарегистрирован Минюстом России 22 ноября 2019 г., регистрационный N 56583), с изменениями, внесенными приказом Роскомнадзора от 24 апреля 2024 г. N 73 (зарегистрирован Минюстом России 6 июня 2024 г., регистрационный N 78486).

Мероприятия, предусмотренные настоящим пунктом, должны осуществляться 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. Программно-аппаратные средства, используемые для контроля, фильтрации и блокирования сетевых запросов, обладающих признаками атак, направленных на отказ в обслуживании, должны быть расположены на территории Российской Федерации.

Обеспечение доступности из сети "Интернет" интерфейсов и сервисов информационных систем, подлежащих защите от компьютерных атак, направленных на отказ в обслуживании, должно осуществляться в соответствии с внутренними регламентами по защите информации по согласованию со структурным подразделением (специалистами) по защите информации после принятия мер по контролю и фильтрации исходящего и входящего сетевого трафика в соответствии с перечнем ресурсов сети "Интернет", с которыми может взаимодействовать информационная система, включающим исходящий и входящий сетевые потоки, их характеристики и используемые протоколы.

60. Посредством проведения мероприятий по обеспечению защиты информации при использовании для функционирования информационных систем искусственного интеллекта <20> должна быть обеспечена возможность исключения 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 наборы данных <21>, применяемые модели искусственного интеллекта <22> и их параметры <23>, процессы и сервисы по обработке данных и поиску решений <24>.

<20> Подпункт "а" пункта 5 Национальной стратегии развития искусственного интеллекта.
<21> Подпункт "д" пункта 5 Национальной стратегии развития искусственного интеллекта.

<22> Подпункт "р" пункта 5 Национальной стратегии развития искусственного интеллекта.

<23> Подпункт "т" пункта 5 Национальной стратегии развития искусственного интеллекта.

<24> Подпункт "а" пункта 5 Национальной стратегии развития искусственного интеллекта.

Не допускается передача лицу, разработавшему модель искусственного интеллекта, информации ограниченного доступа, содержащейся в информационных системах, в том числе для улучшения функционирования модели искусственного интеллекта.

61. При взаимодействии пользователей в целях выполнения ими своих обязанностей (функций) с сервисами на основе искусственного интеллекта посредством направления запроса и получения ответа должны быть:

а) при взаимодействии в формате строго заданных шаблонов запросов и ответов:

определены шаблоны запросов пользователей, направляемых в искусственный интеллект, и обеспечен контроль соответствия запросов установленным шаблонам;

определены шаблоны ответов искусственного интеллекта и обеспечен контроль соответствия ответов установленным оператором (обладателем информации) шаблонам;

б) при взаимодействии в формате свободной текстовой формы запросов и ответов:

определены для направляемых в искусственный интеллект запросов пользователей допустимые тематики и обеспечен контроль соответствия запросов допустимым тематикам;

определены форматы ответов искусственного интеллекта в соответствии с допустимыми тематиками и обеспечен контроль соответствия ответов установленным оператором (обладателем информации) форматам и допустимым тематикам;

в) разработаны статистические критерии для выявления недостоверных ответов искусственного интеллекта для последующего сбора и анализа недостоверных ответов;

г) обеспечено реагирование на недостоверные ответы искусственного интеллекта посредством ограничения области принимаемых решений и (или) реализации функций информационной системы на основе недостоверных ответов искусственного интеллекта.

При использовании в информационных системах искусственного интеллекта или сервисов на основе искусственного интеллекта должно быть исключено нерегламентированное влияние искусственного интеллекта на параметры модели искусственного интеллекта и на функционирование информационных систем.

Непосредственно в состав информационных систем должны включаться доверенные технологии искусственного интеллекта <25> или их компоненты.

<25> Подпункт "ц" пункта 5 Национальной стратегии развития искусственного интеллекта.

62. Мероприятия по реализации в информационных системах мер по их защите и содержащейся в них информации должны включать:

1) реализацию базовых мер защиты информационных систем и содержащейся в них информации соответствующих классов защищенности, устанавливаемых оператором (обладателем информации);

2) адаптацию базовых мер защиты информационных систем и содержащейся в них информации применительно к архитектуре информационных систем, применяемым информационным технологиям, особенностям функционирования информационных систем;

3) верификацию адаптированных базовых мер защиты информационных систем и содержащейся в них информации в соответствии с актуальными угрозами и возможностями нарушителей, их дополнение и (или) усиление.

63. В информационных системах должны быть реализованы следующие базовые меры защиты информационных систем и содержащейся в них информации:

а) идентификация и аутентификация;

б) управление доступом;

в) регистрация событий безопасности;

г) защита виртуализации и облачных вычислений <26>;

<26> Подпункт "и" пункта 4 Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. N 203.

д) защита технологий контейнерных сред и их оркестрации <27>;

<27> Пункт 3.10 национального стандарта Российской Федерации ГОСТ Р 70860-2023 "Информационные технологии. Облачные вычисления. Общие технологии и методы", утвержденного и введенного в действие приказом Госстандарта от 28 августа 2023 г. N 700-ст (М., ФГБУ "Институт стандартизации", 2023).

е) защита сервисов электронной почты;

ж) защита веб-технологий;

з) защита программных интерфейсов взаимодействия приложений;

и) защита конечных устройств;

к) защита мобильных устройств;

л) защита технологий интернета вещей <28>;

<28> Подпункт "в" пункта 4 Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. N 203.

м) защита точек беспроводного доступа;

н) антивирусная защита;

о) обнаружение и предотвращение вторжений на сетевом уровне;

п) сегментация и межсетевое экранирование;

р) защита от компьютерных атак, направленных на отказ в обслуживании;

с) защита каналов передачи данных и сетевого взаимодействия.

64. Реализация мер по защите информационных систем и содержащейся в них информации, подлежащие реализации, должна обеспечивать защиту от нарушителей со следующими уровнями возможностей:

в информационных системах 3 класса защищенности - от нарушителей с базовым уровнем возможностей;

в информационных системах 2 класса защищенности - от нарушителей с повышенным уровнем возможностей;

в информационных системах 1 класса защищенности - от нарушителей с высоким уровнем возможностей.

Оператором (обладателем информации) может быть принято решение о применении мер защиты информационных систем и содержащейся в них информации от нарушителей с более высоким уровнем возможностей.

65. С целью подтверждения достаточности принятых мер защиты информационных систем и содержащейся в них информации до начала обработки и (или) хранения информации в государственных информационных системах должна быть проведена их аттестация <29> на

соответствие Требованиям в соответствии с Порядком организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденным приказом ФСТЭК России от 29 апреля 2021 г. N 77 <30>.

<29> Подпункт 13(3) пункта 8 Положения о ФСТЭК России.
<30> Зарегистрирован Минюстом России 10 августа 2021 г., регистрационный N 64589.

Решение о необходимости аттестации иных информационных систем государственных органов, государственных унитарных предприятий, государственных учреждений принимается руководителем оператора (обладателя информации), ответственным лицом.

66. Мероприятия по контролю уровня защищенности информации, содержащейся в информационных системах, должны обеспечивать включение проведения оценки возможностей нарушения безопасности информации и (или) нарушения функционирования информационных систем внешними и внутренними нарушителями.

Контроль уровня защищенности информации должен проводиться в соответствии с внутренними регламентами по защите информации одним или совокупностью следующих методов:

а) 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;

б) выявление несанкционированных подключений устройств к информационным системам;

в) тестирование информационных систем путем моделирования реализации актуальных угроз с целью оценки возможностей несанкционированного доступа к ним (воздействий на них) или повышения привилегий при реализованных мероприятиях и мерах по защите информационных систем и содержащейся в них информации;

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

67. Контроль уровня защищенности информации должен проводиться не реже одного раза в три года или после компьютерного инцидента, произошедшего у оператора (обладателя информации). Методы контроля уровня защищенности информации и периодичность его проведения определяются оператором (обладателем информации) во внутреннем регламенте.

По результатам проведения контроля уровня защищенности информации разрабатывается отчет, который подписывается лицами, проводившими контроль. Отчет должен быть представлен в течение 3 рабочих дней с даты завершения контроля уровня защищенности информации руководителю оператора (обладателя информации), ответственному лицу для принятия при необходимости решения руководителя оператора (обладателя информации) о выделении ресурсов с целью повышения уровня защищенности информации. Отчет направляется оператором (обладателем информации) в ФСТЭК России в течение 5 рабочих дней с даты завершения контроля уровня защищенности информации в целях мониторинга текущего состояния технической защиты информации.

68. Мероприятия и меры по защите информации, предусмотренные Требованиями, должны реализовываться оператором (обладателем информации) с использованием методических документов ФСТЭК России.

69. При отсутствии возможности реализации отдельных мероприятий и (или) принятия мер по защите информации в соответствии с Требованиями оператором (обладателем информации) должны быть разработаны и внедрены компенсирующие меры, позволяющие обеспечить блокирование (нейтрализацию) актуальных угроз. При этом оператором (обладателем информации) должно быть обосновано применение компенсирующих мер на этапе создания информационных систем, а при аттестации информационных систем - подтверждена их эффективность для блокирования (нейтрализации) актуальных угроз.

70. Технические меры по защите информации должны приниматься на аппаратном, системном, прикладном уровнях, а также в информационно-телекоммуникационной инфраструктуре при ее наличии. На аппаратном и системном уровнях защита информации должна обеспечиваться посредством применения встроенных в аппаратное обеспечение и системное программное обеспечение средств защиты информации. На прикладном и сетевом (инфраструктурном) уровнях защита информации должна обеспечиваться применением встроенных в прикладное программное обеспечение средств защиты информации и (или) применением наложенных и сетевых средств защиты информации.

71. Для защиты информации должны применяться сертифицированные средства защиты информации в соответствии с инструкциями (правилами) по их эксплуатации, установленными разработчиками в эксплуатационной документации. Применяемые средства защиты информации должны быть обеспечены со стороны их разработчиков поддержкой безопасности на территории Российской Федерации, включая выпуск и применение обновлений программного обеспечения, обеспечивающих устранение выявленных уязвимостей, дефектов и недостатков.

Средства защиты информации должны применяться с соблюдением запретов, установленных пунктом 6 Указа Президента Российской Федерации от 1 мая 2022 г. N 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации".

72. Применяемые сертифицированные средства защиты информации должны соответствовать:

для защиты информационных систем 1 класса защищенности - не ниже чем 4 классу защиты и уровню доверия <31>;

<31> Пункт 2, подпункт 13(1) пункта 8 Положения о ФСТЭК России.

для защиты информационных систем 2 класса защищенности - не ниже чем 5 классу защиты и уровню доверия;

для защиты информационных систем 3 класса защищенности - 6 классу защиты и уровню доверия.

73. На стадиях жизненного цикла государственных информационных систем меры по защите информации должны приниматься заказчиками, операторами в соответствии с Требованиями к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах

данных информации, утвержденными постановлением Правительства Российской Федерации от 6 июля 2015 г. N 676, на стадиях жизненного цикла иных информационных систем - в соответствии с разделом 5 национального стандарта Российской Федерации ГОСТ Р 51583-2014 "Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие требования.", утвержденного и введенного в действие приказом Росстандарта от 28 января 2014 г. N 3-ст (М., ФГУП "Стандартинформ", 2014).

Приложение

к Требованиям о защите информации,

содержащейся в государственных

информационных системах, иных

информационных системах государственных

органов, государственных унитарных

предприятий, государственных учреждений,

утвержденным приказом ФСТЭК России

от 11 апреля 2025 г. N 117

ТРЕБОВАНИЯ К ОПРЕДЕЛЕНИЮ КЛАССА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

1. Оператором (обладателем информации) устанавливаются три класса защищенности информационных систем, определяющие уровни защищенности содержащейся в них информации.

Самый низкий класс - третий, самый высокий - первый. Класс защищенности информационной системы (первый класс (далее - К1), второй класс (далее - К2), третий класс (далее - К3) определяется в зависимости от уровня значимости информации (далее - УЗ), обрабатываемой в этой информационной системе, и масштаба информационной системы.

2. Уровень значимости информации определяется в зависимости от степени возможных негативных последствий (ущерба) для обладателя информации и (или) оператора от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации. Негативные последствия (ущерб) определяются в том числе на основе перечня негативных последствий, включенных в банк данных угроз безопасности информации ФСТЭК России.

Степень возможного ущерба определяется обладателем информации или оператором (обладателем информации) в соответствии с таблицей 1:

Таблица 1

Степень возможного ущерба	Возможный ущерб от нарушения безопасности информации и (или) функционирования информационной системы
Высокая	Возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор, обладатель информации не могут выполнять возложенные на них функции
Средняя	Возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор, обладатель информации не могут выполнять хотя бы одну из возложенных на них функций
Низкая	Возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор, обладатель информации могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств

3. Высокий уровень значимости (далее - УЗ 1) должен устанавливаться, если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба.

Средний уровень значимости (далее - УЗ 2) должен устанавливаться, если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба.

Низкий уровень значимости (далее - УЗ 3) должен устанавливаться, если для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определены низкие степени ущерба.

4. Для информации, которая отнесена к информации ограниченного распространения и для носителей которой установлена ограничительная пометка "для служебного пользования", должен быть установлен УЗ 1.

5. При обработке в информационной системе двух и более видов информации УЗ определяется отдельно для каждого вида информации. Итоговый УЗ, обрабатываемой в информационной системе, устанавливается по наивысшим значениям степени возможного ущерба, определенным для конфиденциальности, целостности, доступности информации каждого вида информации.

6. Для информационной системы должен быть определен федеральный масштаб, если она предназначена для решения задач на всей территории Российской Федерации или в пределах двух и более субъектов Российской Федерации.

Для информационной системы должен быть определен региональный масштаб, если она предназначена для решения задач в пределах одного субъекта Российской Федерации.

Для информационной системы должен быть определен объектовый масштаб, если она предназначена для решения задач в пределах объекта (объектов) одного государственного органа, муниципального образования, организации.

7. Класс защищенности информационной системы определяется в соответствии с таблицей 2:

Таблица 2

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

8. Классы защищенности информационных систем, функционирующих на базе информационно-телекоммуникационной инфраструктуры, не должны быть выше класса защищенности этой информационно-телекоммуникационной инфраструктуры.

9. Допускается присвоение отдельным сегментам информационной системы разных классов защищенности. В этом случае меры по защите информации сегментов информационной системы и содержащейся в них информации должны приниматься в соответствии с присвоенными им классами защищенности.

10. Результаты классификации оформляются актом, который утверждается оператором (обладателем информации). Акт классификации должен содержать наименование классифицируемой системы и сегментов информационной системы при их наличии, УЗ или УЗ в сегментах информационной системы при их наличии, масштаб информационной системы и (или) сегментов информационной системы при их наличии, присвоенный класс защищенности информационной системе или сегментам информационной системы при их наличии. Допускается оформление единого акта классификации на несколько сегментов информационной системы одного оператора (обладателя информации).

11. Класс защищенности информационной системы (сегментов информационной системы) подлежит пересмотру при изменении масштаба информационной системы (сегментов информационной системы) или значимости содержащейся в ней информации (в сегментах информационной системы).