

**ФЕДЕРАЛЬНАЯ СЛУЖБА**

**ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ**

**(ФСТЭК России)**

# П Р И К А З

« » \_\_\_\_\_\_\_ 2025 г. Москва № \_\_\_\_\_

**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. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и подпунктами 3 и 9.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085,
**П Р И К А З Ы В А Ю:**

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

2. Признать утратившими силу:

приказ ФСТЭК России от 13 февраля 2013 г. №  17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (зарегистрирован Минюстом России 31 мая 2013 г., регистрационный № 28608);

приказ ФСТЭК России от 15 февраля 2017 г. №  27 «О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 13 февраля 2013 г. №  17» (зарегистрирован Минюстом России 14 марта 2017 г., регистрационный № 45933);

приказ ФСТЭК России от 13 сентября 2019 г. №  106 «О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 13 февраля 2013 г. №  17» (зарегистрирован Минюстом России 13 сентября 2019 г., регистрационный № 55924).

3. Настоящий приказ вступает в силу с 1 сентября 2025 г., за исключением пункта 52 Требований, утвержденных настоящим приказом, который вступает в силу с 1 сентября 2027 г. До вступления в силу настоящего приказа для защиты информации, содержащейся в иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, применяются Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 13 февраля 2013 г. № 17.

**ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ**

**ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ**

**В.СЕЛИН**

УТВЕРЖДЕНЫ

приказом ФСТЭК России

от «\_\_\_» \_\_\_\_\_\_\_\_ 2025 г. № \_\_\_

**Требования**

**о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений**

I. Общие положения

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

2. В случае передачи информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации (далее — информация ограниченного доступа, конфиденциальная информация), из государственной информационной системы в иные информационные системы, информационная система в которую передается информация ограниченного доступа, должна соответствовать настоящим Требованиям[[1]](#footnote-1). Состав передаваемой информации ограниченного доступа, цели ее защиты и уровень защищенности в соответствии с настоящими Требованиями должны определяться договором или иным документом, предусматривающим передачу информации ограниченного доступа из государственной информационной системы в иную информационную систему.

3. Настоящие 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 и Федеральной службы безопасности Российской Федерации.

4. В муниципальных информационных системах защита информации обеспечивается в соответствии с настоящими Требованиями, если иное не установлено законодательством Российской Федерации о местном самоуправлении.

5. При обработке и хранении в информационных системах информации, содержащей сведения, составляющие государственную тайну, ее защита должна обеспечиваться в соответствии с нормами и требованиями по технической защите информации, содержащей сведения, составляющие государственную тайну, установленными ФСТЭК России[[2]](#footnote-2).

6. При обработке в информационных системах информации, содержащей персональные данные, должны применяться настоящие Требования и Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

7. В случае если информационные системы являются значимым объектом критической информационной инфраструктуры Российской Федерации, защита содержащейся в них информации должна обеспечиваться в соответствии с требованиями, установленными в соответствии с Федеральным законом от 27 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

8. В случае использования для защиты информации, содержащейся в информационных системах, шифровальных (криптографических) средств защиты информации должны применяться настоящие Требования и Требования о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств, утвержденные приказом ФСБ России от 24 октября 2022 г. № 524[[3]](#footnote-3).

9.  Функционирование информационных систем на базе информационно-телекоммуникационной инфраструктуры[[4]](#footnote-4) допускается при условии защиты информационно-телекоммуникационной инфраструктуры в соответствии с настоящими Требованиями.

II. Требования к организации деятельности по защите информации

и управлению данной деятельностью

10.  Оператор информационных систем (далее — оператор) должен организовывать деятельность по защите информации и управлять ею в соответствии с настоящими Требованиями.

11. Организация деятельности по защите информации должна предусматривать:

а) утверждение политики защиты информации;

б) определение лиц, ответственных за защиту информации;

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

г) разработку и утверждение внутренних стандартов и регламентов по защите информации;

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

12. Политика защиты информации должна охватывать все информационные системы оператора, а также информационно-телекоммуникационную инфраструктуру, если информационные системы функционируют на базе информационно-телекоммуникационной инфраструктуры. Положения политики защиты информации обязательны для исполнения всеми подразделениями (работниками) оператора.

13. Политика защиты информации должна содержать:

а) область действия политики;

б) цели и задачи защиты информации;

в) принципы защиты информации;

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

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

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

ж)  ответственность работников за нарушения требований о защите информации и установленных оператором правил обработки информации.

Политика защиты информации утверждается руководителем оператора или уполномоченным руководителем оператора лицом (далее — ответственное лицо), и доводится до работников оператора.

14. Основными целями защиты информации должны являться:

а) недопущение (исключение, снижение возможности) наступления негативных последствий (событий) от нарушения конфиденциальности, целостности, доступности информации (далее — нарушение безопасности информации);

б) недопущение (исключение, снижение возможности) наступления негативных последствий (событий) от нарушения функционирования информационных систем вследствие реализации (возникновения) угроз безопасности информации.

Иные цели защиты информации определяются оператором в зависимости от ожидаемых результатов от проведения мероприятий и принятия мер по защите информации. Определяемые оператором задачи защиты информации должны обеспечивать достижение целей защиты информации.

15. Организации, которым на основании договора или иного документа передается информация, предоставляется доступ к информационным системам оператора 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 указана в договоре или ином документе, на основании которого передается информация, предоставляется доступ к информационным системам оператора или содержащейся в них информации.

16. Защиту информации организует руководитель оператора или по его решению ответственное лицо.

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 должны быть включены в должностной регламент (инструкцию) ответственного лица. Состав обязанностей (функций) и полномочий (прав) по организации защиты информации ответственного лица должен быть достаточен для организации и управления защитой информации в соответствии с настоящими Требованиями, а также организации контроля за данной деятельностью у оператора.

17. Руководитель оператора, ответственное лицо создает, определяет структурное подразделение или назначает отдельных специалистов, на которых возлагаются обязанности (функции) по защите информации (далее соответственно — структурное подразделение, специалисты по защите информации).

Функции и полномочия (права) по защите информации структурного подразделения определяются в положении о структурном подразделении или ином документе, в соответствии с которым функционирует структурное подразделение. Обязанности (функции) и полномочия (права) специалистов по защите информации по проведению мероприятий и принятию мер по защите информации определяются в их должностных регламентах (инструкциях). Состав обязанностей (функций) и полномочий (прав) по защите информации структурного подразделения, специалистов по защите информации должен быть достаточен для проведения мероприятий и принятия мер по защите информации в соответствии с настоящими Требованиями.

В случае наличия у оператора структурного подразделения, на которое возложены функции по обеспечению информационной безопасности[[5]](#footnote-5), защита информации обеспечивается указанным подразделением.

18. Работники структурного подразделения, специалисты по защите информации должны обладать компетенциями, необходимыми для выполнения возложенных на них обязанностей (функций) по защите информации в соответствии с настоящими Требованиями.

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

20. Подразделения (работники), применяющие информационные системы, должны участвовать в проведении мероприятий и принятии мер по защите информации в объеме, установленном оператором 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, ремонта информационных систем и иных видов эксплуатационных работ, обучения пользователей информационных систем (далее – пользователи), являющихся работниками оператора (далее – внутренние пользователи), в объеме, установленном оператором во внутренних стандартах и регламентах по защите информации.

21.  Структурным подразделением, специалистами по защите информации должны применяться программные, программно-аппаратные средства, обеспечивающие 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.

22. По решению руководителя оператора, ответственного лица для проведения мероприятий и принятия мер по защите информации могут привлекаться организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации[[6]](#footnote-6) (далее – организации-лицензиаты). Состав проводимых организациями-лицензиатами мероприятий и принимаемых ими мер по защите информации, используемых при этом программных, программно-аппаратных средств, предназначенных для защиты информации, определяется оператором в договорах или иных документах, на основании которых такие организации-лицензиаты привлекаются к защите информации.

Специалисты по защите информации должны осуществлять контроль проводимых организациями-лицензиатами мероприятий и принимаемых ими мер по защите информации.

23. Оператором должны быть разработаны и утверждены внутренние стандарты по защите информации, устанавливающие требования к реализации мер по защите информации применительно к особенностям деятельности оператора и эксплуатации информационных систем.

Оператором должны быть разработаны и утверждены внутренние регламенты по защите информации, содержащие порядок проведения мероприятий или описание реализуемых процессов по защите информации применительно к особенностям деятельности оператора и функционирования информационных систем. Область действия внутренних стандартов и регламентов по защите информации определяется оператором.

24. Внутренние стандарты по защите информации должны содержать:

а) требования к первичной идентификации пользователей;

б) требования к применяемым моделям доступа пользователей;

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

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

д) требования к конфигурациям и настройкам программных, программно-аппаратных средств, предназначенных для обеспечения доступа пользователей к информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»);

е) требования к конфигурациям и настройкам программных, программно-аппаратных средств, предназначенных для обеспечения удаленного доступа внутренних пользователей, включая требования к обеспечению безопасной дистанционной работы;

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

з) требования к защите физических и виртуальных устройств внутренних пользователей, имеющих постоянный доступ к сети «Интернет» (далее — конечные устройства (точки));

и) требования к защите мобильных устройств, планшетных, переносных компьютеров, используемых для доступа внутренних пользователей к информационным системам при выполнении своих обязанностей (функций) (далее — мобильные устройства);

к) требования к непрерывности функционирования информационных систем;

л) требования к резервному копированию информации и программного обеспечения в информационных системах;

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

н) требования к защите информации в подключаемых информационных системах и каналах передачи данных при взаимодействии с такими информационными системами.

25. Внутренние регламенты по защите информации должны содержать:

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

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

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

г) порядок предоставления удаленного доступа к информационным системам внутренним пользователям, а также при необходимости пользователям, не являющимся работниками оператора (далее — внешние пользователи);

д) порядок и условия предоставления подрядным организациям доступа к информационным системам и (или) передачи им информации и контроля за таким доступом, передачей;

е) порядок предоставления пользователям иных информационных систем доступа к информационным системам оператора и (или) передачи информации в иные информационные системы и контроля за такими доступом, передачей (в случае взаимодействия с иными информационными системами);

ж) порядок предоставления пользователям информационных систем доступа в сеть «Интернет» и ее использования (в случае взаимодействия с сетью «Интернет»);

з) порядок повышения уровня знаний и информированности работников подразделений оператора по вопросам защиты информации;

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

к)  порядок получения, оценки, тестирования и применения обновлений программного обеспечения (далее — управление обновлениями);

л) порядок обработки и обращения с информацией ограниченного доступа;

м) порядок обеспечения физической защиты информационных систем;

н) порядок разработки безопасного программного обеспечения[[7]](#footnote-7) в случае его разработки оператором;

о) порядок вывода в контур эксплуатации сервисов, доступ к которым осуществляется с использованием сети «Интернет» в случае наличия таких сервисов;

п) порядок мониторинга информационной безопасности[[8]](#footnote-8) информационных систем в случае их взаимодействия с сетью «Интернет»;

р) порядок восстановления штатного функционирования информационных систем и тестирования процессов восстановления;

с) порядок контроля за обеспечением уровня защищенности информации, содержащейся в информационных системах.

26. Внутренние стандарты и регламенты по защите информации утверждаются руководителем оператора или ответственным лицом и доводятся до работников, а также подрядных организаций в части, их касающейся.

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

Обязанность подрядной организации по выполнению внутренних стандартов и регламентов по защите информации должна быть указана в договоре или ином документе, на основании которого передается информация, предоставляется доступ к информационным системам оператора или содержащейся в них информации.

27. Руководитель оператора, ответственное лицо обеспечивает выделение организационных, материально-технических и иных обеспечивающих ресурсов для проведения мероприятий и принятия мер по защите информации, для привлечения при необходимости дополнительных сил и средств для защиты информации в соответствии с настоящими Требованиями на всех этапах жизненного цикла информационных систем.

Структурное подразделение, специалисты по защите информации должны разрабатывать и представлять руководителю оператора, ответственному лицу обоснованные предложения по 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, ущерба), наступление которых прогнозируется в случае отсутствия ресурсов.

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

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 могут привести к нарушению целей защиты информации, установленных в политике защиты информации (далее — угрозы безопасности информации или актуальные угрозы);

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

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

Мероприятия по защите информации должны предусматривать реализацию оператором последовательности действий или процессов, обеспечивающих достижение целей защиты информации.

Меры по защите информации должны предусматривать реализацию в каждой информационной системе организационно-технических и технических мер, обеспечивающих блокирование (нейтрализацию) актуальных для информационной системы угроз безопасности информации.

В зависимости от целей защиты информации мероприятия и меры по защите информации должны обеспечивать:

а) исключение утечки конфиденциальной информации;

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

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

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

д) предотвращение несанкционированного удаления информации и программного обеспечения, своевременное 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 нарушение функционирования (работоспособности) информационных систем;

и) недопущение распространения с использованием информационных систем противоправной информации;

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

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

а) показателя, характеризующего текущее состояние защиты информации от базового уровня угроз безопасности информации (далее — показатель защищенности Кзи);

б) показателя, который определяет достаточность и эффективность проведения мероприятий по защите информации (далее — показатель уровня зрелости Пзи).

Показатель защищенности Кзи и показатель уровня зрелости Пзи являются показателями деятельности по защите информации оператора.

Для определения значений и расчета показателя защищенности Кзи и показателя уровня зрелости Пзи должныприменяться методические документы, утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о ФСТЭК России (далее — методические документы
ФСТЭК России)[[9]](#footnote-9).

32. Расчет и оценка показателя защищенности Кзи должны проводиться оператором не реже одного раза в шесть месяцев. Расчет и оценка показателя уровня зрелости Пзи должны проводиться оператором не реже одного раза в два года.

О полученных по результатам оценки значениях показателя защищенности Кзи и показателя уровня зрелости Пзи в случае их несоответствия нормированным значениям информируется руководитель оператора для принятия решения о необходимости проведения мероприятий по совершенствованию защиты информации и принятия мер по повышению уровня защищенности информации, содержащейся в информационных системах.

Результаты оценки показателя защищенности Кзи и показателя уровня зрелости Пзи в срок не позднее 5 рабочих дней после их расчета должны направляться оператором в ФСТЭК России в целях мониторинга текущего состояния технической защиты информации и оценки эффективности деятельности по технической защите информации[[10]](#footnote-10).

33. В случае если полученные по результатам расчета значения показателя защищенности Кзи и показателя уровня зрелости Пзи не достигают нормированных значений, указанных в методических документах ФСТЭК России, оператором должны проводиться мероприятия, направленные на совершенствование защиты информации, и приниматься меры по повышению уровня защищенности информации, содержащейся в информационных системах.

По решению руководителя оператора, ответственного лица структурным подразделением, специалистами по защите информации с участием подразделений (работников), применяющих информационные системы, подразделений (работников), обеспечивающих эксплуатацию информационных систем, разрабатывается план мероприятий по совершенствованию защиты информации, содержащейся в информационных системах.

В плане указываются наименования мероприятий, сроки их выполнения, подразделения (работники), ответственные за реализацию каждого мероприятия. План утверждается руководителем оператора, ответственным лицом и доводится до подразделений (работников) оператора в части, их касающейся. Результатом реализации мероприятий плана должно быть достижение значений показателя защищенности Кзи и показателя уровня зрелости Пзи не ниже нормированных значений, указанных в методических документах ФСТЭК России.

III. Требования к проведению мероприятий и принятию

мер по защите информации

34. Для достижения целей защиты информации оператором 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 и обращении с информацией ограниченного доступа;

е)  обеспечение защиты информации при использовании конечных устройств (точек);

ж)  обеспечение защиты информации при использовании мобильных устройств;

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

и)  обеспечение защиты информации при предоставлении пользователям доступа к информационным системам, предусматривающего возможность выполнения, изменения, записи, удаления программ и (или) данных в информационных системах (далее - привилегированный доступ);

к) обеспечение мониторинга информационной безопасности;

л) обеспечение разработки безопасного программного обеспечения;

м)  обеспечение физической защиты информационных систем;

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

о) повышение уровня знаний и информированности работников оператора по вопросам защиты информации;

п) обеспечение защиты информации при взаимодействии с подрядными организациями;

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

с) обеспечение защиты информации при использовании искусственного интеллекта[[11]](#footnote-11);

т) обеспечение доверия[[12]](#footnote-12) при взаимодействии в информационных системах субъектов и объектов доступа;

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

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

Достаточность и эффективность проводимых мероприятий (реализованных процессов) оценивается по результатам определения показателя уровня зрелости Пзи в соответствии с пунктом 31 настоящих Требований.

35. Мероприятия по выявлению и оценке угроз безопасности информации должны предусматривать определение в ходе создания информационных систем актуальных угроз и разработку в случаях установленных нормативным правовым актом Правительства Российской Федерации[[13]](#footnote-13) 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, ответственным лицом.

В ходе эксплуатации информационных систем должны быть обеспечены поиск данных и признаков, идентифицирующих актуальные угрозы, проведена приоритизация выявленных угроз, осуществлено оповещение подразделений (работников) оператора о выявленных актуальных угрозах. При наличии признаков реализации опасных угроз должны быть приняты меры по их блокированию (нейтрализации).

36.  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 своевременное обнаружение фактов несанкционированных изменений и выявление причин изменений.

Контроль конфигураций информационных систем должен осуществляться на основе анализа результатов учета ИТ-активов[[14]](#footnote-14) 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.

37. Мероприятия по управлению уязвимостями должны предусматривать 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 должно обеспечиваться применением компенсирующих мер:

в отношении уязвимостей критического уровня опасности[[15]](#footnote-15) - в срок не более 24 часов;

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 информационных систем.

При выявлении уязвимостей информационных систем, сведения о которых отсутствуют в банке данных угроз безопасности информации[[16]](#footnote-16), оператор в срок не более 5 рабочих дней с даты такого выявления должен направить информацию об уязвимости в ФСТЭК России для ее оценки необходимости включения в банк данных угроз безопасности информации ФСТЭК России.

38. Мероприятия по управлению обновлениями должны предусматривать проведение проверки подлинности и целостности обновлений, тестирование обновлений программного обеспечения до их применения в информационных системах, выдачу разрешения подразделениям (работникам) оператора на применение обновлений программного обеспечения в информационных системах с использованием безопасных настроек и конфигураций, установленных во внутренних стандартах по защите информации.

Сроки применения обновлений программного обеспечения, 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.

39. Мероприятия по защите информации при обработке 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 такая информация не предназначена.

Контроль обработки, хранения информации ограниченного доступа в программно-аппаратных средствах и ее передачи должен обеспечиваться в соответствии со 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, ответственное лицо.

40. Мероприятия по обеспечению защиты информации при использовании конечных устройств (точек) информационных систем должны исключать возможность несанкционированного доступа к конечным устройствам (точкам) или воздействия на них через интерфейсы и физические порты, взаимодействующие с сетью «Интернет».

Защита конечных устройств (точек) информационных систем должна предусматривать в том числе проведение на них мониторинга и анализа событий и процессов, а также предупреждение о событиях безопасности. Контроль использования конечных устройств (точек) должен осуществляться в соответствии с внутренними стандартами и регламентами по защите информации.

41. Мероприятия по обеспечению защиты информации при использовании мобильных устройств должны исключать возможность несанкционированного доступа (или воздействия) к информационным системам и к взаимодействующими с ними мобильными устройствами через каналы передачи мобильных данных, мобильные сервисы, интерфейсы и физические порты мобильных устройств (за исключением мобильных устройств, предназначенных для доступа к сайтам сети «Интернет» и иным публичным веб-ресурсам).

В мобильных устройствах вычислительная среда, используемая для исполнения функций по защите информации, должна быть изолирована от вычислительной среды, используемой для работы с иными приложениями, сервисами.

Доступ к информационным системам для обработки содержащейся в них информации с использованием мобильных устройств должен осуществляться только с применением виртуальных частных сетей, функционирующих на основе сертифицированных шифровальных (криптографических) средств защиты информации. При хранении в мобильных устройствах информации ограниченного доступа ее защита должна обеспечиваться с использованием сертифицированных шифровальных (криптографических) средств защиты информации.

Использование для доступа к информационным системам и содержащейся в них информации личных мобильных устройств не допускается. Контроль использования мобильных устройств должен осуществляться в соответствии с внутренними стандартами и регламентами по защите информации.

42. Мероприятия по обеспечению защиты информации при удаленном доступе внутренних пользователей должны исключать возможность несанкционированного доступа к информационным системам или воздействий на них за счет доступа к каналам передачи данных и удаленно подключаемым программно-аппаратным средствам или их подмены.

Удаленный доступ внутренних пользователей к информационным системам должен осуществляться с использованием программно-аппаратных средств, выделенных оператором. По согласованию со структурным подразделением, специалистами по защите информации допускается предоставление удаленного доступа к информационным системам с использованием личных программно-аппаратных средств внутреннего пользователя (за исключением личных мобильных устройств) при условии применения для удаленного доступа сертифицированных средств обеспечения безопасной дистанционной работы и средств антивирусной защиты.

Удаленный доступ должен осуществляться только с сетевых адресов, закрепленных за сетями связи, собственники или иные владельцы которых имеют номер автономной системы[[17]](#footnote-17) и с применением сертифицированных шифровальных (криптографических) средств защиты информации, обеспечивающих защиту канала передачи данных.

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

43.  Мероприятия по обеспечению защиты информации при предоставлении привилегированного доступа должны исключать 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, которые должны быть закреплены за соответствующими ролями пользователей. Привилегированные учетные записи должны иметь права доступа, минимально необходимые для выполнения пользователями возложенных 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 и иметь только локальный доступ.

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. 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.

Контроль использования привилегированных учетных записей должен осуществляться в соответствии с внутренними стандартами и регламентами по защите информации.

44. Мероприятия по осуществлению мониторинга информационной безопасности должны предусматривать сбор данных о событиях безопасности, их обработку и анализ, 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 информационных систем, имеющих взаимодействие с сетью «Интернет».

Мероприятия по мониторингу информационно безопасности должны осуществляться в соответствии с разделом 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[[18]](#footnote-18).

Оператор ежегодно в срок, установленный внутренним регламентом по защите информации, разрабатывает отчет о результатах мониторинга в прошедшем году, который представляется руководителю оператора. Отчет о результатах мониторинга за прошедший год после его представления руководителю оператора направляется оператором в ФСТЭК России в целях мониторинга текущего состояния технической защиты информации[[19]](#footnote-19).

45. Мероприятия по разработке безопасного программного обеспечения должны быть направлены на предотвращение появления, выявление и устранение уязвимостей в разрабатываемом оператором программном обеспечении.

В случае самостоятельной разработки оператором программного обеспечения, предназначенного для использования в информационных системах, должны быть реализованы меры, предусмотренные разделом 5 ГОСТ Р 56939 -2024.

В случае разработки программного обеспечения подрядной организацией на основании заключенного с оператором договора по решению руководителя, ответственного лица допускается включение в техническое задание на разработку программного обеспечения требований по разработке безопасного программного обеспечения, предусмотренных разделом 5 ГОСТ Р 56939 -2024. Подтверждением выполнения подрядной организацией мер по разработке безопасного программного обеспечения является наличие у нее сертификата соответствия, выданного ФСТЭК России в соответствии с Порядком проведения сертификации процессов безопасной разработки программного обеспечения средств защиты информации, утвержденным приказом ФСТЭК России от 1 декабря 2023 г. № 240[[20]](#footnote-20).

46. Мероприятия по обеспечению физической защиты информационных систем должны исключать возможность несанкционированного физического доступа к программно-аппаратным средствам обработки и хранения информации.

Доступ посторонних лиц в помещения (зоны помещений), в которых установлены программно-аппаратные средства обработки и хранения информации, и проведение в таких помещениях работ должны осуществляться только в сопровождении работников оператора, ответственных за контроль доступа в помещения (зоны помещений) по согласованию со структурным подразделением, специалистами по защите информации.

В случае отсутствия возможности исключения несанкционированного физического доступа к средствам обработки и хранения информации, защита информации ограниченного доступа, содержащейся в таких средствах, должна обеспечиваться с использованием шифровальных (криптографических) средств защиты информации.

Контроль физического доступа к программно-аппаратным средствам обработки и хранения информации ограниченного доступа и (или) в помещения (зоны помещений), 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.

Не допускается использовать в информационных системах какие-либо съемные машинные носители информации, кроме выдаваемых оператором. В случае обнаружения работником оператора 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 дальнейшего уничтожения. Подключение обнаруженного съемного машинного носителя информации к информационным системам запрещается.

47. Мероприятия по обеспечению непрерывности функционирования информационных систем при возникновении нештатных ситуаций должны позволять восстановить выполнение функций (процессов, видов работ) информационных систем, для которых оператором или обладателем информации установлены требования к непрерывному режиму функционирования, в пределах интервалов времени восстановления, установленных внутренними стандартами и регламентами по защите информации.

Интервалы времени восстановления функционирования информационных систем устанавливаются оператором в соответствии с актами, на основании которых осуществляется создание, эксплуатация информационных систем, или требованиями обладателя информации с учетом значимости функций для обеспечения его деятельности 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 дней с момента обнаружения нарушения функционирования;

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

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

Оператором 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 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, исключающих несанкционированный доступ к резервным копиям информации.

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

Оператор должен проводить периодические 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 с превышение 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.

48. Мероприятия по повышению уровня знаний и информированности работников оператора по вопросам защиты информации должны включать:

а) доведение до работников оператора 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 с целью оценки устойчивости работников к методам социальной инженерии;

г) проведение тренировок с работниками по практической отработки мероприятий по защите информации, предусмотренных внутренними регламентами по защите информации.

Применяемые оператором способы повышения уровня знаний работников по вопросам защиты информации, периодичность и формы оценки уровня знаний должны определяться во внутренних регламентах по защите информации.

Оценка уровня знаний работников по вопросам защиты информации осуществляется в ходе периодического тестирования, проводимого работниками, ответственными за организацию и проведение повышения уровня знаний, в соответствии с внутренними регламентами. Для работников, показавших по результатам тестирования неудовлетворительный уровень знаний по вопросам защиты информации, организуется повторное прохождение обучающих курсов по вопросам защиты информации.

49. Мероприятия по защите информации при взаимодействии оператора с подрядными организациями должны исключать 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.

В договорах или иных документах, на основании которых подрядным организациям предоставлен доступ к информационным системам оператора или передана содержащаяся в них информация, должны быть установлены обязанность подрядных организаций по обеспечению защиты информации, к которой получен доступ, а также ответственность за невыполнение этой обязанности.

Не допускается копирование подрядными организациями информации, к которой им предоставлен доступ, если такое копирование не предусмотрено в договорах или иных документах, 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 на основании настоящих Требований во внутренних стандартах и регламентах по защите информации.

 Разработка (развитие) и (или) тестирование программного обеспечения подрядными организациями непосредственно в эксплуатируемых информационных системах оператора 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. Контроль доступа подрядных организаций к стендам разработки (развития) и (или) тестирования должен осуществляться в соответствии с внутренними регламентами по защите информации.

50. Мероприятия по организации и проведению защиты от атак, направленных на отказ в обслуживании, должны исключать возможность блокирования авторизованным пользователям доступа к информационным системам и (или) содержащейся в них информации в следствии несанкционированных воздействий на физические порты, интерфейсы и сервисы, к которым должен быть обеспечен постоянный доступ из сети «Интернет».

Оператором должно быть обеспечено взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации[[21]](#footnote-21), а также взаимодействие в автоматизированном режиме с Центром мониторинга и управления сетью связи общего пользования[[22]](#footnote-22).

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 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 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 матрицей коммуникаций информационной системы с сетью «Интернет».

51. Мероприятия по обеспечению защиты информации при использовании для функционирования информационных систем искусственного интеллекта[[23]](#footnote-23) должны исключать возможность 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[[24]](#footnote-24), применяемые модели искусственного интеллекта[[25]](#footnote-25) и их параметры[[26]](#footnote-26), процессы и сервисы по обработке данных и поиску решений[[27]](#footnote-27).

В информационно-коммуникационной инфраструктуре оператора, на базе которой функционируют технологии искусственного интеллекта[[28]](#footnote-28), должны быть реализованы мероприятия и приняты меры по защите информации в соответствии с настоящими Требованиями.

При необходимости передачи лицу, разработавшему модель искусственного интеллекта, данных, содержащихся в информационных системах, в том числе для улучшения функционирования модели искусственного интеллекта, передача конфиденциальной информации не допускается.

При взаимодействии пользователей информационных систем с искусственным интеллектом посредством направления запроса и получения ответа должно 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 шаблонам;

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

определены для направляемых в искусственный интеллект запросы 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 форматам и допустимым тематикам;

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

д)   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 должно быть исключено нерегламентированное влияние искусственного интеллекта на параметры модели искусственного интеллекта и на функционирование информационных систем. В составе информационных систем должны использоваться доверенные технологии искусственного интеллекта[[29]](#footnote-29).

52. Мероприятия по обеспечению доверия при взаимодействии субъектов и объектов доступа в распределенных информационных системах 1 класса защищенности, имеющих доменную архитектуру, должны включать:

а) первичную идентификацию пользователей и персональных электронных вычислительных машин, серверов, к которым осуществляется доступ пользователей;

б) строгую аутентификацию внутренних пользователей и персональных электронных вычислительных машин, серверов, к которым осуществляется доступ, с использованием сертификатов безопасности, выдаваемых центром сертификации оператора (далее — корпоративный центр сертификации);

в) проверку аутентичности и целостности устанавливаемого программного обеспечения и его обновлений с использованием сертификатов безопасности, выданных разработчиком программного обеспечения и корпоративным центром сертификации;

г) доверенную загрузку программного обеспечения персональных электронно-вычислительных машин и серверов, страной происхождения которых является Российская Федерация, с использованием аппаратных модулей безопасности этих средств, обеспечивающих безопасное хранение закрытых ключей и сертификатов безопасности.

Строгая аутентификация с использованием аппаратного модуля безопасности должна применяться для всех персональных электронных вычислительных машин и серверов, страной происхождения которых является Российская Федерация и которые подлежат включению в состав информационных систем после 1 января 2029 г.

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.

Оператором должны быть обеспечены доступность корпоративного центра сертификации для пользователей и программных, программно-аппаратных средств информационных систем и его функционирование на специально предназначенных для этого программно-аппаратных средствах.

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

а) реализацию базового набора мер защиты информационных систем и содержащейся в них информации соответствующих классов защищенности, устанавливаемых оператором в соответствии с приложением № 1 к настоящим Требованиям;

б) адаптацию базового набора мер защиты информационных систем и содержащейся в них информации применительно к архитектуре информационных систем, применяемым информационным технологиям, особенностям эксплуатации системы;

в) верификацию адаптированного базового набора мер защиты информационных систем и содержащейся в них информации в соответствии с актуальными угрозами и возможностями нарушителей, при необходимости их дополнение и (или) усиление.

В информационных системах должны быть реализованы следующие базовые меры:

а) идентификация и аутентификация;

б) управление доступом;

в) регистрация событий безопасности;

г) защита виртуализации и облачных технологий;

д) защита технологий контейнерных сред и их оркестрации[[30]](#footnote-30);

е) защита сервисов электронной почты;

ж) защита веб-технологий;

з) защита программных интерфейсов взаимодействия приложений;

и) защита конечных устройств (точек);

к) защита мобильных устройств;

л) защита устройств «интернета вещей»;

м) антивирусная защита;

н) обнаружение и предотвращение вторжений на сетевом уровне;

о) сегментация и межсетевое экранирование;

п) защита от атак, направленных на отказ в обслуживании;

р) защита каналов связи и сетевого взаимодействия.

Меры защиты информационных систем и содержащейся в них информации, подлежащие реализации, должны 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 возможностями.

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

 С целью подтверждения достаточности и эффективности принятых мер защиты информационных систем и содержащейся в них информации до начала обработки и (или) хранения информации в информационных системах должна быть проведена их аттестация на соответствие настоящим 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. №  77[[31]](#footnote-31).

54. Мероприятия по проведению контроля уровня защищенности информации, содержащейся в информационных системах, должны включать проведение 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 и экспертная оценка 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 с учетом реализованных организационных мер и применяемых средств защиты информации;

г) 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.

По результатам проведения контроля уровня защищенности информации разрабатывается отчет, который подписывается лицами, проводившими контроль. Отчет должен быть представлен руководителю оператора, ответственному лицу для принятия при необходимости решения о выделении дополнительных ресурсов с целью повышения уровня защищенности информации. Отчет направляется оператором в ФСТЭК России в целях мониторинга текущего состояния технической защиты информации[[32]](#footnote-32).

55. Мероприятия и меры по защите информации, предусмотренные настоящими Требованиями, должны реализовываться оператором с использованием методических документов ФСТЭК России.

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

57. Технические меры по защите информации должны применяться на аппаратном, системном, прикладном уровнях, а также в информационно-телекоммуникационной инфраструктуре (при 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 обеспечивается применением встроенных в прикладное программное обеспечение средств защиты информации и (или) применением наложенных и сетевых средств защиты информации.

58.  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. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

59.  Применяемые сертифицированные средства защиты информации должны соответствовать:

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

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.

Классы защиты и уровни доверия определяются в соответствии с нормативными правовыми актами ФСТЭК России[[33]](#footnote-33).

60. На стадиях жизненного цикла государственных информационных систем меры по защите информации должны применяться в соответствии с Требованиями к порядку создания, развития 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. № 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»[[34]](#footnote-34).

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 «\_\_\_» \_\_\_\_\_\_\_\_ 2025 г. № \_\_\_\_

Определение класса защищенности информационной системы

1. Оператором 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 (К1), второй класс (К2), третий класс (К3)) определяется в зависимости от уровня значимости информации (УЗ), обрабатываемой в этой информационной системе, и масштаба информационной системы.

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

2. Уровень значимости информации определяется степенью возможного 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.

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

где степень возможного ущерба определяется обладателем информации или оператором в соответствии с таблицей:

|  |  |
| --- | --- |
| **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 |

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

Информации, которая отнесена к информации ограниченного распространения и для которой установлена ограничительная пометка «для служебного пользования», имеет высокий уровень значимости (УЗ 1).

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

3. Информационная система имеет федеральный масштаб, если она предназначена для решения задач на всей территории Российской Федерации или в пределах двух и более субъектов Российской Федерации.

Информационная система имеет региональный масштаб, если она предназначена для решения задач в пределах одного субъекта Российской Федерации.

Информационная система имеет объектовый масштаб, если она предназначена для решения задач в пределах объекта (объектов) одного государственного органа, муниципального образования, организации.

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

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

5.При определении класса защищенности информационной системы должен учитываться класс защищенности информационно-телекоммуникационной инфраструктуры, на базе которой функционирует информационная система. Классы защищенности информационных систем, функционирующих на базе информационно-телекоммуникационной инфраструктуры, не должны быть выше класса защищенности этой информационно-телекоммуникационной инфраструктуры.

6. Результаты классификации оформляются актом, который утверждается оператором. Акт классификации должен содержать наименование классифицируемой системы, уровень значимости информации, масштаб информационной системы, присвоенный класс защищенности. Допускается оформление единого акта классификации на несколько информационных систем, одного оператора.

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

1. Часть 81 статьи 14 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». [↑](#footnote-ref-1)
2. Подпункт 91 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. №  1085 (далее — Положение о ФСТЭК России). [↑](#footnote-ref-2)
3. Зарегистрирован Минюстом России 23 ноября 2022 г., регистрационный № 71073. [↑](#footnote-ref-3)
4. 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. № 900. [↑](#footnote-ref-4)
5. Пункт 1 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». [↑](#footnote-ref-5)
6. Пункт 5 часть 1 статьи 12 Федерального закона от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности». [↑](#footnote-ref-6)
7. Пункт 3.2 национального стандарта Российской Федерации ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования». Утвержден и введен в действие приказом Росстандарта от 24 октября 2024 г. № 1504-ст (М., ФГБУ «РСТ», 2024) (далее – ГОСТ Р 56939-2024). [↑](#footnote-ref-7)
8. 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. № 656-ст (М., ФГБУ «РСТ», 2021) (далее – ГОСТ Р 59547-2021). [↑](#footnote-ref-8)
9. Абзац пункта 5 Положения о ФСТЭК России. [↑](#footnote-ref-9)
10. Подпункты 6.1 и 6.5 пункта 8 Положения о ФСТЭК России. [↑](#footnote-ref-10)
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. №  490 (далее – Национальная стратегия развития искусственного интеллекта). [↑](#footnote-ref-11)
12. Пункт 3.16 национального стандарта Российской Федерации ГОСТ Р 58833 — 2020 Защита информации. Идентификация и аутентификация. Общие положения. Утвержден и введен в действие приказом Росстандарта от 10 апреля 2020 г. № 159-ст (М., ФГБУ «РСТ», 2020). [↑](#footnote-ref-12)
13. Подпункт «г» пункта 12 и 3 Требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденных постановлением Правительства Российской Федерации от 6 июля 2015 г. № 676. [↑](#footnote-ref-13)
14. Пункт 3 Положения об учете ИТ-активов, используемых для осуществления деятельности по цифровой трансформации системы государственного (муниципального) управления, утвержденное постановлением Правительства Российской Федерации от 1 июля 2024 г. № 900. [↑](#footnote-ref-14)
15. Пункт 5.2.18 национального стандарта Российской Федерации ГОСТ Р 56545 — 2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей». Утвержден и введен в действие приказом Росстандарта от 19 августа 2015 г. № 1180-ст. (М., ФГБУ «РСТ», 2021). [↑](#footnote-ref-15)
16. Подпункт 21 пункта 8 Положения о ФСТЭК России. [↑](#footnote-ref-16)
17. Часть 1 статьи 56.1 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи». [↑](#footnote-ref-17)
18. Подпункт «ц» пункта 5 Национальной стратегии развития искусственного интеллекта. [↑](#footnote-ref-18)
19. Подпункт 6.1 пункта 8 Положения о ФСТЭК России. [↑](#footnote-ref-19)
20. Зарегистрирован Минюстом России 16 апреля 2024 г., регистрационный № 77896. [↑](#footnote-ref-20)
21. Подпункт «б» пункта 2 Указа Президента Российской Федерации от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». [↑](#footnote-ref-21)
22. Пункт 5 приказа Роскомнадзора от 31 июля 2019 г. № 225 «Об утверждении Положения о Центре мониторинга и управления сетью связи общего пользования» (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). [↑](#footnote-ref-22)
23. Подпункт «а» пункта 5 Национальной стратегии развития искусственного интеллекта. [↑](#footnote-ref-23)
24. Подпункт «д» пункта 5 Национальной стратегии развития искусственного интеллекта. [↑](#footnote-ref-24)
25. Подпункт «р» пункта 5 Национальной стратегии развития искусственного интеллекта. [↑](#footnote-ref-25)
26. Подпункт «т» пункта 5 Национальной стратегии развития искусственного интеллекта. [↑](#footnote-ref-26)
27. Подпункт «а» пункта 5 Национальной стратегии развития искусственного интеллекта. [↑](#footnote-ref-27)
28. Подпункт «б» пункта 5 Национальной стратегии развития искусственного интеллекта. [↑](#footnote-ref-28)
29. Подпункт «ц» пункта 5 Национальной стратегии развития искусственного интеллекта. [↑](#footnote-ref-29)
30. 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 Росстандарта от 28 августа 2023 г. № 700-ст. (М., ФГБУ «Институт стандартизации», 2023). [↑](#footnote-ref-30)
31. Зарегистрирован Минюстом России 10 августа 2021 г., регистрационный № 64589. [↑](#footnote-ref-31)
32. Подпункт 6.1 пункта 8 Положения о ФСТЭК России. [↑](#footnote-ref-32)
33. Подпункт 13.1 пункта 8 Положения о ФСТЭК России. [↑](#footnote-ref-33)
34. Утвержден и введен в действие приказом Росстандарта от 28 января 2014 г. № 3-ст (М., ФГУП «Стандартинформ», 2014). [↑](#footnote-ref-34)