МИНИСТЕРСТВО СОЦИАЛЬНОЙ ПОЛИТИКИ СВЕРДЛОВСКОЙ ОБЛАСТИ

Территориальный отраслевой исполнительный орган государственной власти Свердловской области – Управление социальной политики Министерства социальной политики Свердловской области № 26

П Р И К А З

07.08.2020 № 55

г. Екатеринбург

Об утверждении положения по организации и проведению работ по обеспечению безопасности персональных данных в территориальном отраслевом исполнительном органе государственной власти Свердловской области – Управлении социальной политики Министерства социальной политики Свердловской области № 26

С целью обеспечения исполнения требований Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и организации работ по обеспечению безопасности персональных данных в территориальном отраслевом исполнительном органе государственной власти Свердловской области – Управлении социальной политики Министерства социальной политики Свердловской области № 26 (далее – Управление социальной политики № 26)

ПРИКАЗЫВАЮ

1. Утвердить положение по организации и проведению работ по обеспечению безопасности персональных данных в территориальном отраслевом исполнительном органе государственной власти Свердловской области –Управлении социальной политики № 26 (приложение № 1).

2. Руководителям структурных подразделений Управления социальной политики № 26 обеспечить соблюдение требований положения по организации и проведению работ по обеспечению безопасности персональных данных.

3. Настоящий приказ довести под подпись до всех сотрудников, осуществляющих обработку персональных данных в Управлении социальной политики № 26.

4. Считать утратившими силу приказы Управления социальной политики по Верх-Исетскому району города Екатеринбурга от 15.12.2017 № 124 «Об утверждении положения по организации и проведению работ по обеспечению безопасности персональных данных в территориальном отраслевом исполнительном органе государственной власти Свердловской области–Управлении социальной политики Министерства социальной политики Свердловской области по Верх-Исетскому району города Екатеринбурга» и Управления социальной политики по Железнодорожному району города Екатеринбурга от 14.02.2019 № 34 «Об утверждении положения по организации и проведению работ по обеспечению безопасности персональных данных в территориальном отраслевом исполнительном органе государственной власти Свердловской области – Управлении социальной политики Министерства социальной политики Свердловской области по Железнодорожному району города Екатеринбурга в новой редакции».

5. Контроль за выполнением требований настоящего приказа оставляю за собой.

Начальник управления Г.А. Воронкова

Приложение № 1 к приказу
территориального отраслевого
исполнительного органа
государственной власти
Свердловской области –
Управления социальной политики
Министерства социальной политики
Свердловской области № 26
от 07.08.2020 № 55

Положение
по организации и проведению работ по обеспечению безопасности персональных данных в территориальном отраслевом исполнительном органе государственной власти Свердловской области – Управлении социальной политики Министерства социальной политики Свердловской области № 26

Содержание

Глава 1. Общие положения

Положение по организации и проведению работ по обеспечению безопасности персональных данных в территориальном отраслевом исполнительном органе государственной власти Свердловской области– Управлении социальной политики Министерства социальной политики Свердловской области № 26 (далее – Положение) определяет порядок организации и проведения работ по обеспечению безопасности персональных данных и информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (далее – защищаемая информация) в территориальном отраслевом исполнительном органе государственной власти Свердловской области – Управлении социальной политики Министерства социальной политики Свердловской области № 26 (далее — Управление социальной политики № 26).

1. Положение разработано с целью:

1) организации и координации работ по обеспечению безопасности защищаемой информации на объектах информатизации (далее — ОИ) Управления социальной политики № 26;

2) регламентации порядка проведения работ по обеспечению безопасности защищаемой информации, обрабатываемой на ОИ Управления социальной политики № 26;

3) контроля состояния безопасности защищаемой информации, обрабатываемой на ОИ;

4) определения такого порядка обработки ПДн, при котором обеспечиваются законные права и интересы субъектов ПДн.

2. Настоящее Положение разработано на основании:

1) Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

2) Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

3) постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

4) постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными и правовыми актами, операторами, являющимися государственными или муниципальными органами»;

5) постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

6) приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении требований к защите информации,

не составляющей государственную тайну, содержащейся в государственных информационных системах»;

7) приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

8) приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;

9) «Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К)», утвержденных приказом Гостехкомиссии России от 30 августа 2002 г. № 282;

10) Методических рекомендаций по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных», утвержденные 13 декабря 2013 г. руководителем Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций;

11) Руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденного решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

3. Положение обязательно для исполнения всеми лицами, участвующими в обработке защищаемой информации в Управлении социальной политики № 26.

4. Список сокращений, используемых в настоящем Положении, приведен в приложении № 1, терминов и определений – в приложении № 2.

Глава 2. Администратор информационной безопасности

5. Администратор информационной безопасности осуществляет следующие мероприятия, направленные на обеспечение безопасности защищаемой информации, обрабатываемой на ОИ:

1) настройку и сопровождение системы защиты ОИ, в частности:

реализует полномочия доступа для каждого пользователя ОИ на основе утвержденного руководителем Управления социальной политики № 26 перечня лиц, имеющих доступ к защищаемой информации, обрабатываемой на ОИ;

удаляет учетные записи пользователей на ОИ при увольнении или перемещении сотрудника не позднее 3 рабочих дней, с момента получения информации ;

блокирует и производит разблокировку учетных записей пользователей ОИ при их уходе на больничный или в отпуск и при выходе с больничного или из отпуска;

периодически, но не реже одного раза в квартал, контролирует смену паролей пользователями для доступа на ОИ;

регистрирует новых пользователей ОИ;

регистрирует СЗИ;

периодически, но не реже одного раза в месяц, выполняет мероприятия по периодическому тестированию функционирования СЗИ в соответствии с документацией разработчика данных средств, регистрируя проведение данных мероприятий.

2) настройку и сопровождение подсистемы регистрации и учета ОИ:

проводит регулярный анализ системного журнала ОИ для выявления попыток НСД к защищаемым ресурсам с соответствующей регистрацией проверки;

информирует руководство о несанкционированных действиях персонала не позднее 1 рабочего дня с момента выявления и участвует в разбирательствах по фактам попыток НСД;

проводит резервное копирования информационных массивов ОИ.

3) сопровождение подсистемы обеспечения целостности ОИ:

осуществляет учет возникновения нештатных ситуаций;

осуществляет восстановление ОИ при возникновении сбоев;

4) контроль функционирования подсистемы антивирусной защиты ОИ:

обеспечивает поддержание установленного порядка и соблюдение правил антивирусной защиты;

периодически, но не реже одного раза в месяц, проводит антивирусные проверки всех жестких дисков ОИ;

регистрирует результаты антивирусных проверок;

5) осуществление контроля использования машинных носителей информации и ведение их учета;

6) сопровождение подсистемы межсетевого экранирования ОИ;

7) сопровождение подсистемы обнаружения вторжений ОИ;

8) организация обновлений программного обеспечения (далее — ПО) и средств защиты, выполнение профилактических работ, установки и модификации программных средств на ОИ;

9) проведение модернизации аппаратных компонентов;

10) проведение инструктажа сотрудников, имеющих право доступа к защищаемой информации;

11) осуществление контроля за соблюдением пользователями ОИ требований к защите информации;

12) осуществление контроля за обеспечением уровня защищенности ПДн на ОИ, а также контроля за соблюдением пользователями ОИ требований к защите ПДн;

13) участие в анализе ситуаций, касающихся функционирования СЗИ и проверки фактов НСД;

14) оказание методической помощи по вопросам обеспечения безопасности защищаемой информации;

15) организация разработки предложений и участие в проводимых работах по совершенствованию системы защиты информации, обрабатываемой на ОИ;

16) проведение внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн в Управлении социальной политики № 26.

6. Администратор информационной безопасности обязан:

обеспечивать функционирование и поддерживать работоспособность средств защиты ОИ, в пределах, возложенных на него функций;

в случае отказа работоспособности ТС и ПО, средств вычислительной техники, в том числе средств защиты ОИ, принимать меры по их восстановлению (не позднее 5 рабочих дней с момента выявления отказа работоспособности) и выявлению причин, которые вызвали отказ работоспособности;

информировать руководство о фактах нарушения установленного порядка работ, попытках и фактах НСД к защищаемой информации, обрабатываемой на ОИ Управления социальной политики № 26.

7. Администратор информационной безопасности несет ответственность за:

неисполнение (ненадлежащее исполнение) своих обязанностей, предусмотренных настоящим Положением в пределах, определенных законодательством Российской Федерации;

сохранность и работоспособное состояние ТС, ПО, средств защиты, входящих в состав ОИ.

8. Администратор информационной безопасности вправе:

контролировать работу пользователей ОИ;

требовать прекращения обработки информации, как в целом, так и на отдельных ОИ, в случае выявления нарушений требований по обработке и обеспечению безопасности защищаемой информации, обрабатываемой на ОИ Управления социальной политики № 26.

Глава 3. Пользователь ОИ

9. Пользователем ОИ является сотрудник, который в силу своих должностных обязанностей осуществляет обработку защищаемой информации на ОИ с использованием средств автоматизации и имеет доступ к информационным ресурсам, аппаратным средствам, ПО и средствам защиты ОИ.

10. Пользователь ОИ несет персональную ответственность за свои действия.

11. Пользователь ОИ в своей работе руководствуется нормативными правовыми актами в сфере защиты информации и локальными актами Управления социальной политики № 26, определяющих порядок организации и проведения работ, направленных на обеспечение безопасности защищаемой информации, обрабатываемой на ОИ.

В частности, при работе на ОИ, пользователь ОИ руководствуется нормативными правовыми актами в сфере ПДн и локальными актами Управления социальной политики № 26, определяющих порядок организации и проведения работ, направленных на обеспечение безопасности ПДн при их обработке.

12. Пользователь ОИ обязан:

1) соблюдать требования нормативных правовых актов в сфере защиты информации и локальных актов Управления социальной политики № 26, определяющих порядок организации и проведения работ, направленных на обеспечение безопасности защищаемой информации, обрабатываемой на ОИ;

2) выполнять на ОИ в отношении защищаемой информации, обрабатываемой на ОИ, только те процедуры, которые определены для него в

локальных актах Управления социальной политики № 26, определяющих порядок организации и проведения работ, направленных на обеспечение безопасности защищаемой информации, обрабатываемой на ОИ;

3) в случае отсутствия пользователя ОИ рядом с ОИ для предотвращения доступа к информации, находящейся на ОИ, минуя ввод пароля, пользователь ОИ во время перерыва в работе ОИ обязан осуществить блокирование операционной системы (далее — ОС) нажатием комбинации *Ctrl+Alt+Del* и кнопки «Блокировать» в появившемся меню или выключить ОИ. По окончании рабочего дня пользователь ОИ обязан выключить ОИ;

4) знать и соблюдать установленные требования по обработке и обеспечению безопасности защищаемой информации, обрабатываемой на ОИ;

5) соблюдать требования антивирусной защиты на ОИ;

6) соблюдать требования парольной защиты на ОИ;

7) соблюдать правила при работе в сетях общего доступа и (или) международного обмена, установленные настоящим положением.

13. Пользователю ОИ запрещается:

1) разглашать защищаемую информацию третьим лицам;

2) сообщать, передавать посторонним лицам личные ключи и атрибуты доступа к ресурсам ОИ;

3) сообщать (или передавать) посторонним лицам сведения о системе защиты ОИ;

4) обрабатывать защищаемую информацию в условиях, позволяющих осуществлять просмотр такой информации лицами, не имеющими к ним права доступа, а также при несоблюдении требований по обеспечению безопасности защищаемой информации;

5) оставлять включенный без присмотра ОИ, не активизировав средства защиты от НСД (временное блокирование ОС нажатием комбинации Ctrl+Alt+Del и кнопки «Блокировать» в появившемся меню);

6) самостоятельно вносить изменения в конфигурацию ПО и ТС ОИ, изменять установленный алгоритм функционирования технических и программных средств;

7) записывать и хранить защищаемую информацию, обрабатываемую на ОИ, на неучтенных установленным порядком машинных носителях информации;

8) использовать ОИ и другие ресурсы ОИ в неслужебных целях;

9) подключать к ОИ личные машинные носители информации и мобильные устройства;

10) отключать (блокировать) СЗИ;

11) привлекать посторонних лиц для ремонта или настройки ОИ без согласования с администратором информационной безопасности.

14. Пользователь ОИ несет ответственность за:

1) неисполнение (ненадлежащее исполнение) своих обязанностей, предусмотренных настоящим положением в пределах, определенных законодательством Российской Федерации;

2) сохранность защищаемой информации, к которой допущен пользователь в рамках исполнения должностных обязанностей;

3) соблюдение требований нормативных правовых актов в сфере защиты информации и локальных актов Управления социальной политики № 26, определяющих порядок организации и проведения работ, направленных на обеспечение безопасности защищаемой информации на ОИ.

15. Пользователь ОИ имеет следующие права:

1) осуществлять обработку защищаемой информации в пределах установленных полномочий;

2) обращаться к администратору информационной безопасности за оказанием технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, ТС ИС, а также с СЗИ.

Глава 4. Правила работы в сетях общего доступа и (или) международного обмена

16. Работа в сетях связи общего пользования и (или) сетях международного информационного обмена (далее — Сеть) на элементах ОИ должна проводиться при служебной необходимости.

17. При работе в Сети запрещается:

1) осуществлять работу при отключенных средствах защиты (антивирусное средство, межсетевой экран и другие);

2) скачивать из Сети ПО и другие файлы;

3) посещать сайты, непосредственно не связанные с исполнением служебных обязанностей.

18. Обо всех выявленных нарушениях требований по обработке и обеспечению безопасности защищаемой информации, обрабатываемой на ОИ, пользователь ОИ должен незамедлительно сообщать администратору информационной безопасности либо руководству.

19. Для получения консультаций по вопросам работы и настройке элементов ОИ пользователь ОИ должен обращаться к администратору информационной безопасности.

20. Пользователь ОИ обязан принимать меры по реагированию в случае возникновения нештатных либо аварийных ситуаций, с целью ликвидации их последствий в рамках, возложенных на него функций.

Глава 5. Первичный инструктаж лица, допущенного к работе с защищаемой информацией, обрабатываемой на ОИ

21. Первичный инструктаж лица, допущенного к работе с защищаемой информацией, обрабатываемой на ОИ, проводит администратор информационной безопасности после утверждения руководителем документа о наделении лица правом доступа к ОИ до непосредственного доступа этого лица к ОИ.

22. Лицо получает непосредственный доступ к защищаемой информации, содержащейся на ОИ, только после прохождения первичного инструктажа.

23. Лицо, допущенное к работе с ПДн на ОИ, должно быть ознакомлено с нормативными правовыми актами Российской Федерации в сфере защиты ПДн, а также с локальными актами Управления социальной политики № 26, регламентирующими вопросы защиты ПДн.

24. Лицо, являющееся пользователем ИС, должно иметь доступ только к тем функциям ОИ, которые необходимы для выполнения им его должностных обязанностей.

25. Администратор информационной безопасности, проводящий инструктаж лица, обязан разъяснить ему, какие действия на ОИ лицо имеет право совершать, а какие действия ему запрещены.

26. Лицо, допущенное к работе с защищаемой информацией, обрабатываемой на ОИ, должно быть предупреждено:

1) об обязанностях выполнения всех правил и требований, предусмотренных локальными актами Управления социальной политики № 26 в области защиты информации;

2) о проведении разбирательств по фактам совершения действий, связанных с доступом к защищаемой информацией, обрабатываемой на ОИ, и повлекших за собой негативные последствия, в соответствии с установленным порядком проведения разбирательств по фактам нарушения требований по обеспечению безопасности защищаемой информации.

27. Факт прохождения лицом первичного инструктажа регистрируется администратором информационной безопасности в соответствующем журнале учета пользователей, имеющих право доступа к ОИ.

Форма журнала учета пользователей, имеющих право доступа к ОИ приведена в приложении № 3.

Глава 6. Организация режима обеспечения безопасности помещений, в которых осуществляется обработка защищаемой информации

28. Помещения, в которых осуществляется обработка защищаемой информации, должны располагаться в пределах контролируемой зоны.

29. Доступ третьих лиц в помещения Управления социальной политики № 26, где осуществляется обработка защищаемой информации, разрешается только в присутствии лиц, имеющих право доступа в помещение.

30. Помещения, в которых осуществляется обработка защищаемой информации в ИС, должны обеспечивать сохранность информации, обрабатываемой на ОИ, и ТС, исключать возможность бесконтрольного проникновения в помещение и их визуального просмотра посторонними лицами.

31. Машинные носители, содержащие информацию, обрабатываемую на ОИ, (диски, флеш-карты) должны храниться в недоступном для посторонних лиц месте – в запираемых металлических шкафах (сейфах).

32. Помещения, в которых осуществляется обработка защищаемой информации, должны иметь прочные входные двери и замки, гарантирующие надежное закрытие помещений в нерабочее время.

33. Вскрытие и закрытие помещений, в которых ведется обработка защищаемой информации, производится сотрудниками Управления социальной политики № 26, имеющими право доступа в соответствующее помещение.

34. Перед закрытием помещений, в которых осуществляется обработка защищаемой информации, по окончании служебного дня сотрудники, имеющие

право доступа к защищаемой информации, обрабатываемым в соответствующем помещении, обязаны:

1) убрать машинные носители, содержащие защищаемую информацию (диски, флеш-карты) в запираемые шкафы, запереть шкафы на замок;

2) отключить ТС (кроме постоянно действующего оборудования) и электроприборы от сети, выключить освещение;

3) закрыть окна, двери.

35. Перед открытием помещений, в которых осуществляется обработка защищаемой информации, сотрудники обязаны:

1) провести внешний осмотр с целью установления целостности двери и замка;

2) открыть дверь и осмотреть помещение, проверить наличие и целостность замков на шкафах.

При обнаружении неисправности двери и запирающих устройств сотрудники обязаны:

1) не вскрывая помещение, в котором осуществляется обработка защищаемой информации, сообщить об этом руководителю;

2) в присутствии не менее двух сотрудников, включая руководителя, вскрыть помещение и осмотреть его;

3) составить акт о выявленных нарушениях и передать установленным порядком руководителю.

36. При работе с защищаемой информацией, двери помещений должны быть всегда закрыты.

37. Доступ в помещения, где осуществляется обработка защищаемой информации, вспомогательного и обслуживающего персонала (уборщиц, электромонтёров, сантехников и других лиц) разрешается только в присутствии лица, имеющего право доступа в соответствующее помещение, после принятия мер, исключающих визуальный просмотр документов, содержащих защищаемую информацию, обрабатываемую на ОИ, и экранов мониторов.

38. Внутренняя планировка и расположение ОИ в помещениях, где осуществляется обработка защищаемой информации, должны исключать визуальный просмотр обрабатываемой на ОИ защищаемой информации для сотрудников, не осуществляющих обработку таких сведений. Окна помещений, в которых осуществляется обработка защищаемой информации, должны быть оборудованы шторами (жалюзи).

39. На случай пожара, аварии или стихийного бедствия должны быть разработаны специальные инструкции, в которых предусматривается порядок вызова сотрудников, вскрытие помещений, где осуществляется обработка защищаемой информации, очередность и порядок эвакуации документов, материалов и изделий, содержащих данную информацию, а также порядок дальнейшего их хранения.

40. Ответственность за соблюдение порядка доступа в помещения, в которых осуществляется обработка защищаемой информации, возлагается на руководителей структурных подразделений, осуществляющих обработку защищаемой информации.

Глава 7. Контроль за соблюдением требований по обработке и обеспечению безопасности информации

41. Контроль за соблюдением требований по обработке и обеспечению безопасности защищаемой информации Управления социальной политики № 26 состоит из следующих направлений:

1) внешний контроль за соблюдением требований по обработке и обеспечению безопасности защищаемой информации;

2) внутренний контроль соответствия обработки защищаемой информации требованиям к защите информации.

42. Внешний контроль за выполнением требований законодательства по обеспечению безопасности информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, осуществляется:

1) Федеральной службой по техническому и экспортному контролю в пределах своих полномочий.

Внешний контроль за выполнением требований законодательства в области ПДн осуществляется:

1) Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор);

2) Федеральной службой безопасности РФ;

3) Федеральной службой по техническому и экспортному контролю в пределах своих полномочий.

43. Внутренний контроль соответствия обработки защищаемой информации требованиям к защите ПДн Управления социальной политики № 26 состоит из контроля за исполнением требований по обработке и обеспечению безопасности ПДн, в том числе в оценке соотношения вреда, который может быть причинен субъектам ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер.

44. Внутренний контроль соответствия обработки защищаемой информации требованиям к защите информации — это комплекс мероприятий, осуществляемых в целях:

1) соблюдения условий и принципов обработки защищаемой информации;

2) соблюдения требований по обработке и обеспечению безопасности, обрабатываемой на ОИ защищаемой информации;

3) предупреждения и пресечения возможности получения посторонними лицами защищаемой информации;

4) выявления и предотвращения утечки защищаемой информации по техническим каналам;

5) исключения или затруднения несанкционированного доступа к защищаемой информации;

6) предупреждения хищения ТС, входящих в состав ОИ, и машинных носителей, содержащих защищаемую информацию;

7) предотвращения программно-математических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности ОИ.

45. Основными задачами внутреннего контроля являются:

1) проверка соответствия локальных актов в области защиты информации действующему законодательству Российской Федерации;

2) проверка актуальности содержания локальных актов в области обеспечения безопасности защищаемой информации;

3) проверка соблюдения требований нормативных правовых актов, методических документов в сфере защиты информации;

4) проверка наличия необходимых согласий субъектов ПДн, чьи ПДн обрабатываются в Управлении социальной политики № 26;

5) учет и соблюдение требований к защите информации при подготовке организационно-распорядительной документации;

6) проверка организации и выполнения мероприятий по обеспечению безопасности защищаемой информации, обрабатываемой на ОИ;

7) проверка работоспособности применяемых СЗИ для защищаемой информации, обрабатываемой на ОИ, в соответствии с их эксплуатационной документацией;

8) проверка наличия эксплуатационной документации на технические и программные средства защиты ОИ;

9) оценка знаний и качества выполнения сотрудниками своих функциональных обязанностей в части обеспечения безопасности защищаемой информации, обрабатываемой на ОИ;

10) оперативное принятие мер по пресечению нарушений требований по обеспечению безопасности защищаемой информации.

46. Внутренний контроль соответствия обработки защищаемой информации на ОИ требованиям к защите информации осуществляется администратором информационной безопасности ежеквартально. О результатах проверки и мерах, необходимых для устранения выявленных нарушений, администратор информационной безопасности докладывает руководству и производит отметку в журнале учета проведения внутреннего контроля соответствия обработки защищаемой информации требованиям к обеспечению безопасности защищаемой информации.

Форма журнала учета проведения внутреннего контроля соответствия обработки защищаемой информации требованиям к обеспечению безопасности защищаемой информации приведена в приложении № 4.

Глава 8. Проведение проверок по инцидентам информационной безопасности

47. Инцидентом информационной безопасности является событие или комбинация событий, указывающая на свершившуюся, предпринимаемую или вероятную реализацию угрозы информационной безопасности, результатом которой являются:

1) нарушение или возможное нарушение работы средств защиты информации на ОИ;

2) нарушение или возможное нарушение требований законодательства Российской Федерации, нормативных актов и предписаний регулирующих и надзорных органов, внутренних документов Управления социальной политики № 26;

3) нарушение или возможное нарушение в выполнении технологических процессов обработки информации на ОИ.

48. Инциденты информационной безопасности классифицируются по значимости на:

1) инциденты I категории;

2) инциденты II категории.

49. К инцидентам I категории, к которым относятся инциденты, повлекшие за собой разглашение (утечку), уничтожение (искажение) защищаемой информации и/или утрату машинных носителей защищаемой информации, выведение из строя технических и программных средств, входящих в состав ОИ, а именно:

1) успешный подбор административного пароля;

2) несанкционированное внесение изменений в ОИ;

3) утрата или кража резервной копии базы, содержащей защищаемую информацию;

4) необоснованная передача информационных массивов ОИ;

5) организация утечки сведений по техническим каналам;

6) умышленное нарушение работоспособности ОИ;

7) умышленное заражение ОИ компьютерными вирусами;

8) проведение работ с ОИ, повлекших за собой необратимую потерю данных;

9) другие действия, попадающие под действия статей, приведенных в таблице 1.

Таблица 1

Номер статьи	Название статьи
1	2
Федеральный закон Российской Федерации № 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации»	
ст. 17	Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации
Федеральный закон Российской Федерации № 152-ФЗ от 27 июля 2006 года «О персональных данных»	
ст. 24	Ответственность за нарушение требований настоящего Федерального закона
Кодекс Российской Федерации об административных правонарушениях	
ст. 5.39	Отказ в предоставлении информации
ст. 13.11	Нарушение законодательства Российской Федерации в области персональных данных
ст. 13.11.1	Распространение информации о свободных рабочих местах или вакантных должностях, содержащей ограничения дискриминационного характера

Номер статьи	Название статьи
1	2
ст. 13.12	Нарушение правил защиты информации
ст. 13.14	Разглашение информации с ограниченным доступом
ст. 19.7	Непредставление сведений (информации)
Уголовный кодекс Российской Федерации	
ст. 137	Нарушение неприкосновенности частной жизни
ст. 140	Отказ в предоставлении гражданину информации
ст. 272	Неправомерный доступ к компьютерной информации
ст. 273	Создание, использование и распространение вредоносных компьютерных программ
ст. 274	Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей
Трудовой кодекс Российской Федерации	
ст. 90	Ответственность за нарушение норм, регулирующих обработку и защиту ПД сотрудника

50. К инцидентам II категории относятся инциденты, в результате которых возникают предпосылки к разглашению (утечке), уничтожению (искажению) защищаемой информации, утрате машинных носителей защищаемой информации, выведению из строя технических и программных средств, входящих в состав ОИ, а именно:

1) набор не назначенного пароля, более 3 раз подряд;
2) оставление ОИ включенным (незаблокированным) во время отсутствия на рабочем месте;
3) перезагрузка ОИ при сбоях в работе, в т.ч. аварийная (неоднократная) перезагрузка путем нажатия кнопки RESET;
4) утрата учтенного машинного носителя информации;
5) удачная попытка входа под чужим именем, паролем;
6) несанкционированная очистка журналов аудита;
7) несанкционированное копирование защищаемой информации на внешние носители информации;
8) несанкционированная установка (удаление) ПО на ОИ;
9) несанкционированное изменение конфигурации ПО на ОИ;
10) попытка получения прав администратора на ОИ (увеличения полномочий собственных прав, получение прав на отладку программ) удачная или неудачная;
11) попытка получения прав администратора в домене удачная и неудачная;
12) неумышленное заражение ОИ компьютерными вирусами;
13) несанкционированное использование сканирующего ПО;
14) несанкционированное использование анализаторов протоколов (снифферов);
15) несанкционированный просмотр защищаемой информации или вывод на печать;

16) периодическая попытка неудачного доступа к защищаемой информации, обрабатываемой на ОИ;

17) перевод времени на ОИ;

18) нецелевое использование корпоративных ресурсов (печать, Internet, mail, и т.п.);

19) выход из строя ТС ОИ.

51. Проверка проводится по всем категориям инцидентов, с отметкой в журнале учета инцидентов на ОИ. Форма журнала учета инцидентов на ОИ приведена в приложении № 5.

52. Об инцидентах I категорий и II категории, повлекших несанкционированный доступ к информации или нарушениям штатной работы ОИ, администратор информационной безопасности докладывает ответственному за организацию обработки ПДн.

53. Решение об инициализации служебной проверки принимает ответственный за организацию обработки ПДн.

54. Решение о назначении проведения служебной проверки принимает руководитель Управления социальной политики № 26.

Глава 9. Порядок приостановления обработки защищемой информации

55. При обнаружении нарушений I категории обработка защищаемой информации незамедлительно приостанавливается до выявления причин нарушений и устранения этих причин.

56. Принятие решения о приостановлении обработки защищаемой информации принимается руководителем Управления социальной политики № 26.

57. По факту нарушения требований по обеспечению безопасности, повлекшего приостановление обработки защищаемой информации, проводится служебная проверка.

Глава 10. Обезличивание ПДн

58. Обезличивание ПДн проводится:

1) в статистических или исследовательских целях;

2) по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

59. При обезличивании применяется один из следующих методов обезличивания:

1) метод введения идентификаторов (замена части сведений (значений ПДн) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным);

2) метод изменения состава или семантики (изменение состава или семантики ПДн путем замены результатами статистической обработки, обобщения или удаления части сведений);

3) метод декомпозиции (разбиение множества (массива) ПДн на несколько подмножеств (частей) с последующим раздельным хранением подмножеств);

4) метод перемешивания (перестановка отдельных записей, а также групп записей в массиве ПДн).

60. При использовании процедуры обезличивания не допускается совместное хранение ПДн и обезличенных данных.

61. Обезличивание ПДн субъектов должно производиться перед внесением их в информационную систему.

62. Управление социальной политики № 26 вправе обрабатывать на ОИ обезличенные данные, полученные от третьих лиц.

63. В процессе обработки обезличенных данных, при необходимости, может проводиться деобезличивание. После обработки ПДн, полученные в результате такого деобезличивания, уничтожаются.

64. Обработка ПДн до осуществления процедур обезличивания и после выполнения операций деобезличивания должна осуществляться в соответствии с действующим законодательством Российской Федерации с применением мер по обеспечению безопасности ПДн.

65. Обработка обезличенных данных должна осуществляться с использованием технических и программных средств, соответствующих форме представления и хранения данных.

66. Хранение и защита дополнительной (служебной) информации, содержащей параметры методов и процедур обезличивания/деобезличивания, обеспечивается в соответствии с внутренними процедурами обеспечения конфиденциальности, установленными в Управлении социальной политики № 26. При этом обеспечивается исполнение установленных правил доступа пользователей к хранимым данным, резервного копирования и возможности актуализации и восстановления хранимых данных.

67. Процедуры обезличивания/деобезличивания должны встраиваться в процессы обработки ПДн как их неотъемлемый элемент, а также максимально эффективно использовать имеющуюся у Управления социальной политики № 26 инфраструктуру, обеспечивающую обработку ПДн.

68. Обезличивание ПДн, обработка которых осуществляется с разными целями, может осуществляться разными методами.

Возможно объединение различных методов обезличивания в одну процедуру.

Для решения каждой задачи обработки определяются требуемые свойства обезличенных данных и метода обезличивания, которые зависят от набора действий, осуществляемых с ПДн (сбор, хранение, изменение, систематизация, осуществление выборки, поиск, передача и т.д.) в соответствии с принципом разумной достаточности (определяется минимально необходимый перечень свойств). Целесообразно предусмотреть возможность обработки обезличенных данных без предварительного деобезличивания.

69. При выборе метода и процедуры обезличивания учитываются:

1) объем ПДн, подлежащих обезличиванию (некоторые методы неэффективны на малых объемах);

2) форма представления данных (отдельные записи, файлы, таблицы баз данных и т.д.);

3) область обработки обезличенных данных (необходим ли другим операторам доступ к обезличиваемым данным);

4) способы хранения обезличенных данных (локальное хранение, распределенное хранение и т.д.);

5) применяемые в информационной системе меры по обеспечению безопасности данных.

В таблице 2 приведены рекомендации по выбору метода обезличивания в зависимости от класса решаемых задач. Рекомендованные методы ранжированы в порядке убывания эффективности их применения.

Таблица 2

№ п/п	Класс задач	Задачи обработки	Метод обезличивания
1	2	3	4
1.	Статистическая обработка и статистические исследования ПД	– осуществление выборки по заявленным параметрам; – проведение исследований по заданным параметрам субъектов.	– метод перемешивания; – метод декомпозиции; – метод изменения состава или семантики.
2.	Сбор и хранение ПД	– внесение ПДн субъектов в информационную систему на основе анкет, заявлений и прочих документов.	– метод декомпозиции; – метод перемешивания; – метод введения идентификаторов.
3.	Обработка поисковых запросов (поиск данных о субъектах и поиск субъектов по известным данным)	– поиск информации о субъектах; – печать и выдача субъектам документов в установленной форме, содержащих ПДн; – выдача справок, выписок, уведомлений по запросам субъектов или	– метод перемешивания; – метод декомпозиции; – метод введения идентификаторов.

1	2	3	4
		уполномоченных органов.	
4.	Актуализация ПД	– внесение изменений в существующие записи о субъектах на основе обращений субъектов, решений судов и других уполномоченных органов; – внесение изменений в существующие записи о субъектах на основе исследований, выполнения органом своих функций или требований законодательства РФ.	– метод перемешивания; – метод декомпозиции; – метод введения идентификаторов.
5.	Интеграция данных различных операторов	– поиск информации о субъектах; – передача данных смежным органам.	– метод перемешивания; – метод декомпозиции; – метод введения идентификаторов.
6.	Ведение учета субъектов ПД	– прием анкет, заявлений; – ведение учета ПДн в соответствии с функциями органа.	– метод декомпозиции; – метод перемешивания; – метод введения идентификаторов.

Глава 11. Уничтожение защищаемой информации

70. Уничтожение защищаемой информации должно проведено:

1) по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законодательством;

2) в случае отзыва субъектом ПДн согласия на обработку его ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн;

3) в случае выявления фактов неправомерной обработки ПДн (в том числе при обращении субъекта ПДн) и обеспечить их правомерность не предоставляется возможным.

71. Перед уничтожением защищаемой информации необходимо:

1) убедиться в правовых основаниях уничтожения защищаемой информации;

2) убедиться в том, что уничтожается именно та защищаемая информация, которая предназначена для уничтожения;

3) уничтожить защищаемую информацию подходящим способом, указанным в соответствующем требовании или распорядительном документе;

4) проверить необходимость уведомления об уничтожении ПДн субъекта ПДн, или его представителя, или третьих лиц в предусмотренном случае.

72. Уничтожение защищаемой информации осуществляется одним из следующих способов:

1) физическим уничтожением носителя защищаемой информации;

2) уничтожением защищаемой информации с носителя защищаемой информации.

Для физического уничтожения бумажного носителя защищаемой информации используются два вида уничтожения — уничтожение через шредирование (измельчение и гидрообработка) и уничтожение через термическую обработку (сжигание).

73. Уничтожение информации на машинных носителях необходимо осуществлять путем стирания информации с использованием ПО с гарантированным уничтожением. Уничтожение защищаемой информации осуществляется во всех копиях базы данных, если иное не установлено действующим законодательством Российской Федерации.

74. Если защищаемая информация хранятся на машинном носителе, пришедшем в негодность, отслужившем установленный срок или утратившем практическое значение, такой машинный носитель подлежит физическому уничтожению. Перед уничтожением машинного носителя на нем производится стирание защищаемой информации путем использования ПО с гарантированным уничтожением информации.

После стирания защищаемой информации машинный носитель уничтожается одним из следующих способов: разрезание, сжигание, механическое уничтожение, сдача предприятию по утилизации вторичного сырья или иными методами, исключающими возможность восстановления содержания защищаемой информации.

По факту уничтожения защищаемой информации с носителя делается отметка в журнале учета машинных носителей информации. Форма журнала учета машинных носителей информации приведена в приложении №6.

По факту уничтожения машинных носителей информации составляется Акт уничтожения машинных носителей информации. Форма Акт уничтожения машинных носителей информации приведена в приложении № 7.

Глава 12. Порядок управления доступом субъектов доступа к объектам доступа на ОИ

75. Предоставление доступа или изменение прав доступа сотрудников Управления социальной политики № 26 к ОИ осуществляется на основании служебной записки руководителя структурного подразделения сотрудника.

76. Доступ к защищаемым информационным ресурсам ОИ предоставляется администратором информационной безопасности.

77. С целью организации учета лиц, имеющих право доступа к информации, обрабатываемой на ОИ, ведется журнал учета пользователей, имеющих право доступа к ОИ.

Форма журнал учета пользователей, имеющих право доступа к ОИ приведена в приложении № 3.

78. Основанием для прекращения права доступа сотрудника к информации, обрабатываемой на ОИ, является служебная записка руководителя структурного подразделения, увольнение сотрудника, изменение его должностных обязанностей или длительное отсутствие (например, отпуск по уходу за ребенком).

Глава 13. Организация парольной защиты на ОИ

79. Цель применения и реализации парольной защиты заключается в исключении утечки защищаемой информации, обрабатываемой на ОИ, а также ее несанкционированной модификации или уничтожения.

80. Правила парольной защиты регламентируют организационно-техническое обеспечение процессов выдачи, смены и прекращения действия паролей на ОИ, а также контроль над действиями пользователей ОИ при работе с паролями.

81. Организационное и техническое обеспечение процессов выдачи, использования, смены и прекращения действия паролей во всех подсистемах ОИ и контроль действий пользователей при работе с паролями возлагается на администратора информационной безопасности.

82. Защите паролем подлежит доступ к:

1) базовой системе ввода-вывода ОИ;
2) настройке ОС;
3) настройке сетевого оборудования;
4) настройке СЗИ;
5) входу в ПО, предназначенное для обработки защищаемой информации.

83. Личные пароли доступа пользователей ОИ генерируются и распределяются централизованно или выдаются администратором информационной безопасности, или выбираются пользователями ОИ самостоятельно с учетом следующих требований:

1) длина пароля должна быть не менее 8 (Восьми) буквенно-цифровых символов;

2) пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера

телефонов, автомобилей, адреса места жительства, наименование ТС, входящих в состав ОИ, общепринятые сокращения (например, ЭВМ, ЛВС, USER, ADMINISTRATOR и т.д.) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе ОИ;

3) не допускается использование в качестве пароля одного и того же повторяющегося символа или повторяющейся комбинации из нескольких символов;

4) не допускается использование в качестве пароля комбинации символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

5) при смене пароля новое значение должно отличаться от предыдущего;

6) в числе символов пароля, обязательно должны присутствовать латинские буквы в верхнем и нижнем регистрах, а также цифры и символы;

7) не допускается использование ранее использованных паролей.

84. Сотрудники, использующие пароли, обязаны:

1) четко знать и строго выполнять требования по парольной защите;

2) своевременно сообщать администратору информационной безопасности обо всех нештатных ситуациях, возникающих при работе с паролями.

85. При организации парольной защиты запрещается:

1) записывать и хранить свои пароли в очевидных местах (например, на мониторе, на обратной стороне клавиатуры и т.д.);

2) сообщать другим лицам свои пароли, а также сведения о применяемой системе защиты от НСД.

86. Полная плановая смена паролей должна проводиться не реже одного раза в 3 месяца.

Удаление (в том числе внеплановая смена) личного пароля любого пользователя должна производиться в следующих случаях:

1) при подозрении на компрометацию пароля;

2) по завершении срока действия пароля;

3) в случае увольнения, длительного отсутствия (более месяца);

4) по указанию администратора информационной безопасности;

5) в случае увольнения, перехода на другую работу администратора информационной безопасности.

87. Для предотвращения доступа к информации, находящейся на ОИ, минуя ввод пароля, пользователь ОИ во время перерыва в работе обязан осуществлять блокирование системы нажатием комбинации Ctrl+Alt+Del и кнопки «Блокировать» в появившемся меню или выключить ОИ.

88. Факт выдачи пароля пользователю ОИ фиксируется в журнале учета выдачи паролей для доступа к ОИ.

Форма журнала учета выдачи паролей для доступа к ОИ приведена в приложении № 8.

89. Ответственность за организацию парольной защиты возлагается на администратора информационной безопасности.

Глава 14. Организация антивирусной защиты на ОИ

90. Целью антивирусной защиты ОИ является предотвращение и нейтрализация негативных воздействий вредоносного ПО на информационные ресурсы, содержащие защищаемую информацию, и ПО, предназначенного для обработки такой информации.

91. Порядок организации антивирусной защиты определяет требования к организации защиты ОИ от разрушающего воздействия вредоносного ПО и устанавливают ответственность за их выполнение.

92. К использованию на ОИ допускаются только лицензионные и сертифицированные ФСТЭК России и ФСБ РФ по требованиям безопасности информации средства антивирусной защиты.

93. Установка и начальная настройка средств антивирусной защиты на ОИ может осуществляться администратором информационной безопасности, а также представителями организации-лицензиата ФСТЭК России и ФСБ РФ.

94. Администратор информационной безопасности должен организовывать осуществление периодического обновления сигнатур средств защиты от вредоносного ПО и контроль их работоспособности не реже 1 (Одного) раза в неделю.

95. При работе пользователи ОИ, обязаны руководствоваться следующими положениями:

1) Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), защищаемая информация, обрабатываемая на ОИ и содержащаяся на машинных носителях (жесткие магнитные диски, оптические носители информации (*CD*-, *DVD*-диски), флеш-накопители *USB*). Антивирусный контроль информации необходимо осуществлять перед архивированием или записью на машинный носитель. Файлы, помещаемые в электронный архив, в обязательном порядке должны пройти антивирусный контроль. Устанавливаемое (изменяемое) ПО должно быть предварительно проверено на отсутствие вредоносного ПО. После установки (изменения) ПО на ОИ должна быть осуществлена антивирусная проверка ОИ.

2) При возникновении подозрения на наличие вредоносного ПО (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь ОИ самостоятельно (или совместно с администратором информационной безопасности), должен провести внеочередной антивирусный контроль ОИ.

В случае обнаружения вредоносного ПО при проведении антивирусной проверки пользователь ОИ обязан:

приостановить работу ОИ;

немедленно поставить в известность о факте обнаружения вредоносного ПО администратора информационной безопасности, а также других пользователей ОИ, использующих зараженные файлы в работе;

совместно с владельцем зараженных вредоносным ПО файлов провести анализ возможности их дальнейшего использования;

провести «лечение» или удаление зараженных файлов.

3) Периодически, но не реже 1 (Одного) раза в неделю, администратором информационной безопасности должна проводиться антивирусная проверка жестких дисков ОИ.

4) Антивирусные проверки подлежат регистрации в журнале учета антивирусных проверок ОИ. Форма журнала учета антивирусных проверок ОИ приведена в приложении № 9.

5) Ответственность за проведение мероприятий антивирусной защиты и контроля, соблюдения требований антивирусной защиты на ОИ возлагается на администратора информационной безопасности.

Глава 15. Организация учета машинных носителей информации

96. Все машинные носители информации, содержащие защищаемую информацию, а именно:

1) жесткие диски, находящиеся в системных блоках серверов;
2) жесткие диски, находящиеся во внешних RAID-массивах серверов;
3) жесткие диски, находящиеся в системных блоках и кассеты со стриммерными лентами, находящиеся в стриммерных устройствах;
4) USB-носители, находящиеся у пользователей ОИ и содержащие резервные копии;
5) CD-R, CD-RW, DVD-R и/или DVD-RW-носители,

подлежат регистрации и учету.

97. Регистрация машинных носителей информации осуществляется администратором информационной безопасности.

Форма журнала учета машинных носителей информации приведена в приложении № 6.

98. На рабочих местах пользователей ОИ не должны находиться неучтенные машинные носители информации, содержащие защищаемую информацию.

99. Запрещается копирование защищаемой информации пользователями ОИ с целью их передачи другим сотрудникам или посторонним лицам.

100. Сотрудник, получивший носитель для работы с защищаемой информацией, обязан обеспечить его недоступность для третьих лиц (посторонних лиц и сотрудников, не имеющих допуск к защищаемой информации).

101. Полученные извне машинные носители информации должны:

1) проверяться на наличие вредоносных программных продуктов;
2) учитываться в соответствии с настоящим положением.

102. Хранение машинных носителей информации осуществляется в условиях, исключающих утрату их функциональности и хранимой информации из-за влияния внешних полей, излучений и иных неблагоприятных факторов, а также НСД к информации.

Машинные носители информации должны храниться в недоступном для посторонних лиц месте — в металлических шкафах, оборудованных замками (сейфах).

103. Выдача учтенных машинных носителей информации пользователям ОИ производится под подпись в журнале учета машинных носителей информации администратором информационной безопасности.

Передача машинных носителей информации для ремонта или утилизации запрещена.

104. Все машинные носители информации, потерявшие актуальность, передаются администратору информационной безопасности.

Уничтожение учтенных машинных носителей информации осуществляется администратором информационной безопасности. Перед уничтожением носителя производится уничтожение информации с носителя, за исключением случая, когда носитель вышел из строя и удаление информации невозможно. Выбранный способ уничтожения должен полностью исключать возможность последующего восстановления информации. По результатам уничтожения информации с машинного носителя информации делается отметка в журнале учета машинных носителей информации, с указанием способа уничтожения.

Уничтожение учтенных машинных носителей информации осуществляется по акту уничтожения машинных носителей информации с внесением изменений в журнал регистрации. Форма акта уничтожения машинных носителей информации приведена в приложении № 7.

Глава 16. Организация резервирования и восстановления информации на ОИ

105. С целью обеспечения возможности незамедлительного восстановления защищаемой информации на ОИ, модифицированной или уничтоженной вследствие НСД или возникновения нештатных ситуаций, повлекших за собой потерю данных, организуется резервирование и восстановление информации на ОИ.

106. Резервному копированию подлежат следующие информационные ресурсы:

1) файлы, каталоги, БД ОИ, содержащие информацию, обрабатываемую на ОИ;

2) системные и конфигурационные файлы ОС и специального ПО серверов;

3) конфигурационные файлы сетевого оборудования;

4) системные и конфигурационные файлы СЗИ.

107. Резервное копирование защищаемой информации, обрабатываемой на ОИ, должно осуществляться ЕЖЕМЕСЯЧНО на машинные носители информации, создавая тем самым резервный электронный архив. Факт резервного копирования подлежит обязательной регистрации в соответствующем журнале резервного копирования информационных массивов ОИ. Форма журнала резервного копирования информационных массивов ОИ приведена в приложении № 10.

Машинные носители информации, на которые осуществляется резервное копирование защищаемой информации, должны быть поставлены на соответствующий учет и зарегистрированы в журнале учета машинных носителей информации.

Перед резервным копированием машинный носитель информации (жесткий магнитный диск, оптический носитель информации (CD-, DVD-диск), флеш-накопитель USB) проверяется на отсутствие вредоносного ПО. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

Машинные носители информации с обновлениями ПО маркируют датой их получения (датой выхода обновления).

Качество записи резервных копий на машинных носителях информации должно проверяться непосредственно после изготовления копии.

Надежность и правильность записи критической информации следует периодически проверять использованием контрольных процедур восстановления.

108. В случае возникновения нештатной ситуации, вызвавшей полную или частичную потерю работоспособности ОИ, должно быть обеспечено ее восстановление из резервной копии.

109. При восстановлении работоспособности ПО сначала осуществляется резервное копирование информационных ресурсов, содержащих защищаемую информацию, затем производится полное уничтожение некорректно работающего ПО.

Восстановление ПО производится путем его установки с использованием эталонных дистрибутивов (установочных дисков).

110. Восстановление СЗИ производится с использованием дистрибутива. При восстановлении работоспособности СЗИ необходимо выполнить их настройку в соответствии с требованиями безопасности информации. После настройки СЗИ выполняется резервное копирование настроек данных СЗИ с помощью встроенных в них функций на учтенный машинный носитель информации.

111. При работе на ОИ рекомендуется использовать источники бесперебойного питания с целью предотвращения повреждения ТС, входящих в состав ОИ, и (или) защищаемой информации, обрабатываемой на ОИ, в результате сбоев в сети электропитания.

Ответственность за организацию резервного копирования, проведения мероприятий по восстановлению работоспособности информационных ресурсов, технических и программных средств, входящих в состав ОИ, возлагается на администратора информационной безопасности.

Глава 17. Порядок работы с электронными журналами протоколирования и анализа (аудита) значимых событий

112. Правила и порядок протоколирования и анализа (аудита) значимых событий на ОИ направлены на превентивную фиксацию и изучение действий субъектов и объектов на ОИ, а также на своевременное выявление фактов НСД к защищаемой информации.

113. Все события, происходящие в ОС, других критических приложениях и СЗИ должны протоколироваться в специальные электронные журналы аудита.

114. Проверке подлежат следующие электронные журналы:

1) журнал событий, формируемых СЗИ;
2) журнал событий, формируемых СУБД;
3) журналы, формируемые ОС и прикладным ПО.

На ОИ, на которых установлены СЗИ от НСД, проверка соответствующего электронного журнала событий, формируемых данными СЗИ, производится в соответствии с прилагаемой к ним технической и эксплуатационной документацией.

Аудит событий, зафиксированных в электронных журналах, должен анализироваться в плановом порядке на постоянной основе не реже 1 (Одного) раза в неделю администратором информационной безопасности с обязательной регистрацией в журнале проверки электронных журналов ОИ. Форма журнале проверки электронных журналов ОИ приведена в приложении № 11.

Глава 18. Порядок обращения со средствами защиты информации

115. Под СЗИ в настоящем разделе понимается СЗИ, не являющееся средствами криптографической защиты.

116. Процедура установки СЗИ сопровождается оформлением акта установки СЗИ.

Форма акта установки СЗИ приведена в приложении № 12.

117. Процедура деинсталляции СЗИ сопровождается оформлением акта деинсталляции СЗИ.

Форма акта деинсталляции СЗИ приведена в приложении № 13.

118. Инсталлирующие СЗИ носители, установленные СЗИ, эксплуатационная и техническая документация к СЗИ подлежат поэкземплярному учету в журнале поэкземплярного учета средств защиты информации, эксплуатационной и технической документации к ним. Форма журнала поэкземплярного учета средств защиты информации, эксплуатационной и технической документации к ним приведена в приложении № 14.

119. Администратор информационной безопасности должен осуществлять один раз в месяц тестирование СЗИ с отметкой в журнале учета периодического тестирования средств защиты информации.

Форма журнала учета периодического тестирования средств защиты информации приведена в Приложении № 15.

120. СЗИ доставляются фельдъегерской (в том числе ведомственной) связью или со специально выделенными сотрудниками при соблюдении мер, исключающих бесконтрольный доступ к СЗИ во время доставки.

При пересылке СЗИ помещаются в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия. Эксплуатационная и техническая документация к СЗИ пересылается заказными, ценными почтовыми отправлениями или доставляется специально выделенными сотрудники.

При пересылке СЗИ, эксплуатационной и технической документации к ним подготавливается сопроводительное письмо, в котором указывается: что посылается и в каком количестве, учетные номера изделий или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Сопроводительное письмо вкладывается в одну из упаковок.

Полученные упаковки вскрываются только лицом, для которого они предназначены.

Если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать — их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то получателем составляется акт, который высылается отправителю. Полученные с такими отправлениями СЗИ до получения указаний от отправителя применять не разрешается.

При обнаружении бракованных СЗИ один экземпляр бракованного изделия возвращается отправителю для установления причин происшедшего и их устранения в дальнейшем, а оставшиеся экземпляры хранятся до поступления дополнительных указаний от отправителя.

Получение СЗИ, эксплуатационной и технической документации к ним подтверждается отправителю в соответствии с порядком, указанным в сопроводительном письме.

121. СЗИ уничтожаются (утилизируются) по решению руководителя. Намеченные к уничтожению (утилизации) СЗИ изымаются из аппаратных средств, с которыми они функционировали. При этом СЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СЗИ процедура удаления программного обеспечения СЗИ и они полностью отсоединены от аппаратных средств.

Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения используются после уничтожения СЗИ без ограничений.

122. Уничтожение большого объема инсталлирующих СЗИ носителей оформляется актом. Уничтожение по акту производится комиссией в составе не менее трех человек из числа лиц, допущенных к работе с СЗИ. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых инсталлирующих СЗИ носителей. Исправления в тексте акта оговариваются и заверяются подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки в журнале поэкземплярного учета средств защиты информации информационных систем, эксплуатационной и технической документации к ним.

123. Эксплуатационная и техническая документация к СЗИ уничтожается путем сжигания или с помощью любых бумагорезательных машин. Факт уничтожения эксплуатационной и технической документации к СЗИ оформляется в журнале поэкземплярного учета средств защиты информации информационных систем, эксплуатационной и технической документации к ним.

124. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СЗИ, должны обеспечивать сохранность ПДн, СЗИ, исключать возможность неконтролируемого проникновения или пребывания в помещениях, где установлены СЗИ, посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

Для предотвращения просмотра извне помещений, где установлены СЗИ, их окна должны быть оборудованы шторами или жалюзи. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

125. При оборудовании помещений, где установлены СЗИ, должны выполняться требования к размещению и монтажу СЗИ, а также другого оборудования, функционирующего с СЗИ.

126. Инсталлирующие СЗИ носители, эксплуатационная и техническая документация к СЗИ должна храниться в металлических хранилищах (ящиках, шкафах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

Глава 19. Порядок обеспечения информационной безопасности ОИ при модернизации (обновлении) аппаратных и программных компонентов

127. Настоящие правила и порядок модернизации (обновления) аппаратных компонентов, ПО в целях информационной безопасности направлены на защиту ресурсов от:

1) нарушения штатной работы информационных ресурсов и сервисов ОИ;
2) нарушения штатного функционирования оборудования;
3) несанкционированной модификации;
4) несанкционированного копирования.

128. Установке нового оборудования должно предшествовать тестирование инфраструктуры ОИ и критических приложений на отсутствие негативных воздействий вновь устанавливаемого оборудования.

При обнаружении негативного воздействия устанавливаемого оборудования на инфраструктуру ОИ, функционирующие в штатном режиме, такое оборудование не устанавливается. В этом случае разрабатывается план дополнительных мероприятий, направленных на устранение негативного воздействия устанавливаемого оборудования.

129. Установке новых версий ПО или внесению изменений и дополнений в действующее ПО предшествует тестирование информационной инфраструктуры на отсутствие негативных воздействий устанавливаемого ПО.

130. Тестирование нового оборудования и обновлений ПО не должно осуществляться на ресурсах действующей информационной инфраструктуры.

Глава 20. Контроль и надзор за эксплуатацией аттестованного ОИ

131. Государственный контроль и надзор за проведением аттестации ОИ по требованиям безопасности информации, а также за соблюдением правил эксплуатации аттестованного ОИ и эффективностью принятых мер защиты

некриптографическими методами, проводится ФСТЭК России и ее территориальными органами.

132. Государственный контроль и надзор за соблюдением правил аттестации включает проверку правильности и полноты проводимых мероприятий по аттестации ОИ, проверку правильности оформления отчётных документов и протоколов аттестационных испытаний, проверку своевременности внесения изменений в организационно-распорядительные документы по обеспечению безопасности информации, а также контроль за эксплуатацией аттестованного ОИ.

Глава 21. Ответственность за нарушение требований законодательства

133. Лица, виновные в нарушении норм законодательства в сфере защиты информации, несут ответственность в порядке, предусмотренном законодательством Российской Федерации.

Приложение № 1

Список сокращений и обозначений

АРМ	Автоматизированное рабочее место
БД	База данных
ИСПДн	Информационная система персональных данных
НСД	Несанкционированный доступ
ОИ	Объект информатизации
ОС	Операционная система
ПДн	Персональные данные
ПО	Программное обеспечение
СЗИ	Средство защиты информации
ТС	Техническое средство

Приложение № 2

Термины и определения

1**. Автоматизированная система (далее — АС)** — система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

2. **Безопасность информации (данных) —** состояние защищенности информации (данных), при котором обеспечиваются ее (их) конфиденциальность, доступность и целостность.

3. **Вредоносная программа** — программа, предназначенная для осуществления несанкционированного доступа (далее — НСД) к информации и (или) воздействия на информацию или ресурсы АС.

4. **Доступ к информации** — возможность получения информации и ее использования.

5. **Защита информации от НСД** — защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации правил или правил разграничения доступа к защищаемой информации. Заинтересованными субъектами, осуществляющими НСД к защищаемой информации могут быть: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

6. **Защищаемая информация** — информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Собственником информации может быть - государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

7. **Защищаемый объект информатизации (далее — ОИ)** — ОИ, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.

8. **Информация** — сведения (сообщения, данные) независимо от формы их представления.

9. **Информационная система** (далее — ИС) — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

10. **ИС персональных данных (далее — ПДн)** — совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

11. **Информационная технология** — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

12. **Компьютерный вирус** — вредоносная программа, способная создавать свои копии и (или) другие вредоносные программы.

13. **Конфиденциальность информации** — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

14. **Норма эффективности защиты информации** – значение показателя эффективности защиты информации, установленное нормативными и правовыми документами.

15. **Обезличивание ПДн** — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

16. **Объект доступа (в автоматизированной ИС) — е**диница ресурса автоматизированной ИС, доступ к которой регламентируется правилами разграничения доступа.

17. **ОИ** — совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

18. **Оператор** — государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку ПДн, а также определяющие цели и содержание обработки ПДн.

19. **ПДн** — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).

20. **Предоставление информации** — действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

21. **Программное воздействие** — несанкционированное воздействие на ресурсы автоматизированной ИС, осуществляемое с использованием вредоносных программ.

22. **Распространение информации -** действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

23. **Средство защиты информации** – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

24. **Субъект доступа (в автоматизированной ИС) —** лицо или единица ресурса автоматизированной ИС, действия которой по доступу к ресурсам автоматизированной ИС регламентируются правилами разграничения доступа.

25. **Требование по защите информации** – установленное правило или норма, которая должна быть выполнена при организации осуществлении защиты информации, или допустимое значение показателя эффективности защиты информации.

26. **Уязвимость ИС** — свойство ИС, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

27. **Целостность (информации (ресурсов автоматизированной информационной системы) —** состояние информации (ресурсов автоматизированной ИС), при котором ее (их) изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Приложение № 3

ЖУРНАЛ
учета пользователей, имеющих право доступа к объектам информатизации

Начат с _____20___г.
Окончен _____20___г.

На _____листах
Срок хранения _____ лет

№ п/п	Дата	ФИО пользователя	Подпись пользователя объекта информатизации о прохождении первичного инструктажа, об ознакомлении с положениями о порядке защиты информации	ФИО и подпись администратора информационной безопасности	Примечание
1	2	3	4	5	6

Шаблон оформления журнала учета пользователей, имеющих право доступа к объектам информатизации

Приложение № 4

ЖУРНАЛ

учета проведения внутреннего контроля соответствия обработки защищаемой информации требованиям к обеспечению безопасности защищаемой информации

Начат с _____20___г.
Окончен _____20___г.

На _____листах
Срок хранения _____ лет

№ п/п	Дата	Содержание проверки	Реквизиты документа, содержащего отчет о результатах проверки	Ф.И.О. и подпись лица, проводившего проверку	Примечание
1	2	3	4	5	6

Шаблон оформления журнала учета проведения внутреннего контроля соответствия обработки защищаемой информации требованиям к обеспечению безопасности защищаемой информации

Приложение № 5

ЖУРНАЛ
учета инцидентов на объектах информатизации

Начат с _____20___г.
Окончен _____20___г.

На _____листах
Срок хранения _____ лет

№ п/п	Краткое описание инцидента	Дата обнаружения	Предпринятые меры по устранению инцидента		Примечание
			описание мероприятий	дата завершения мероприятий, роспись лица, проводившего мероприятия	
1	2	3	4	5	6

Шаблон оформления журнала учета инцидентов на объектах информатизации

Приложение № 6

ЖУРНАЛ
учета машинных носителей информации

Начат с _____20___г.
Окончен _____20___г.

На _____листах
Срок хранения _____ лет

№ п/п	Регистра-ционный номер носителя	Дата регист-рации	Тип, емкость носителя инфор-мации	№ экз.	Информация о движении носителя			Отметка об уничтожении (стирании) информации (указываются способ уничтожения, дата, расписка)	Отметка об унич-тожении носителя (№ и дата акта об уничтожении носителя)	При-мечание
					Ф.И.О. получателя / место установки	Дата, расписка о				
						получении/ установке	возврате			
1	2	3	4	5	6	7	8	9	10	11

Шаблон оформления журнала учета машинных носителей информации

Приложение № 7

УТВЕРЖДАЮ

_____
(должность)

_____
(фамилия, имя, отчество)

«___» _____ 20__ г.

М.П.

АКТ № _____
уничтожения машинных носителей информации

Комиссия в составе:

– председатель комиссии _____
(должность, Фамилия Имя Отчество)

– члены комиссии _____
(должность, Фамилия Имя Отчество)

_____
(должность, Фамилия Имя Отчество)

Основание уничтожения: _____
Настоящий акт составлен о том, что отобраны к уничтожению.

№ п/п	Регистрационный номер носителя	Тип, емкость носителя информации	Номер экземпляра	Способ уничтожения	Примечание

Всего подлежат уничтожению _____
(количество цифрами и прописью)

На указанных носителях информация уничтожена путем _____.

Председатель комиссии _____ /_____/
(Фамилия Имя Отчество) *(подпись)*

Члены комиссии _____ /_____/
(Фамилия Имя Отчество) *(подпись)*

_____ /_____/
(Фамилия Имя Отчество) *(подпись)*

Шаблон оформления проекта акта уничтожения машинных носителей информации

Приложение № 8

ЖУРНАЛ
учета выдачи паролей для доступа к объектам информатизации

Начат с _____20___г.
Окончен _____20___г.

На _____листах
Срок хранения _____ лет

№ п/п	Ф.И.О. и подпись пользователя объекта информатизации	Дата	Ф.И.О. и подпись администратора информационной безопасности	Примечание
1	2	3	4	5

Шаблон оформления журнала учета выдачи паролей для доступа к объектам информатизации

Приложение № 9

ЖУРНАЛ
учета антивирусных проверок объектов информатизации

Начат с _____20___г.
Окончен _____20___г.

На _____листах
Срок хранения _____ лет

Дата и время проверки	Имя технического средства	Наименование события	Примечание (принятые меры)
1	2	3	4

Шаблон оформления журнала учета антивирусных проверок объектов информатизации

Приложение № 10

ЖУРНАЛ
резервного копирования информационных массивов объектов информатизации

Начат с _____20___г.
Окончен _____20___г.

На _____листах
Срок хранения _____ лет

№ п/п	Дата проведения резервного копирования	Наименование информационного массива объекта информатизации	Регистрационный (учетный, серийный) номер машинного носителя информации	Тип носителя	Ф.И.О. и подпись администратора информационной безопасности	Приме-чание
1	2	3	4	5	6	7

Шаблон оформления журнала резервного копирования информационных массивов объектов информатизации

Приложение № 11

ЖУРНАЛ
проверки электронных журналов объектов информатизации

Начат с _____20___г.
Окончен _____20___г.

На _____листах
Срок хранения _____ лет

№ п/п	Дата проверки	Наименование, серийный номер технического средства	Наименование проверяемого журнала	Выявленные нарушения требований безопасности	Ф.И.О. и подпись администратора информационной безопасности	Примечание
1	2	3	4	5	6	7

Шаблон оформления журнала проверки электронных журналов объектов информатизации

Приложение № 12

ФОРМА АКТА
установки средства защиты информации

№ _____ «___» _____ 20__ г.

Рабочая группа в составе:

_____ _____
(должность) *(Фамилия, Имя, Отчество)*

_____ _____
(должность) *(Фамилия, Имя, Отчество)*

составила настоящий акт о том, что на основании
_____
(№, дата документа)
проведены работы по установке и настройке средств защиты информации (далее - СЗИ) на технические средства и системы, приведенные в таблице 1. Комплектация СЗИ соответствует приведенной в таблице 2.

Таблица 1.

№ п/п	Вид оборудования	Тип	Учетный (заводской) номер
1	2	3	4
1	*Приводятся сведения о техническом средстве (например, системный блок, моноблок), на жесткий диск которого установлено СЗИ*		
2	*Приводятся сведения о жестком диске, на который установлено СЗИ*		

Таблица 2.

№ п/п	Наименование
1	2
1	*Сообщаются сведения о наименовании СЗИ*
1.1	*Сообщаются сведения о специальном защитном знаке, размещенном на установочном компакт-диске с программным обеспечением и эксплуатационной документацией*
1.2	*Сообщаются сведения о формуляре на СЗИ*
1.3	*Сообщаются сведения о сертификате соответствия на СЗИ*

Технические средства и системы, размещенные в помещении № _____, расположенном по адресу _____
Начальные установки параметров СЗИ выполнены в соответствии с требованиями нормативных документов по безопасности информации, а также в соответствии с руководствами по настройке программных продуктов, и представлены в приложении к настоящему акту.

По завершении установки и настройки СЗИ на корпусах технических средств и систем размещены пломбы (номерные наклейки) _____ .

По завершении установки и настройки СЗИ рабочей группой проведены проверки работоспособности основных функций СЗИ и реализованных механизмов защиты. Пользователь технических средств и систем с правилами работы СЗИ ознакомлен.

По результатам проверок, замечаний к работоспособности средств защиты информации и их настройке не выявлено.

Лицо, проводившее установку: _____
(должность, подпись, расшифровка подписи)

Пользователь СЗИ: _____
(должность, подпись, расшифровка подписи)

\

Шаблон оформления проекта акта установки средства защиты информации

Приложение № 13

ФОРМА АКТА
деинсталляции средства защиты информации

№ _____ «___» _____ 20__ г.

Рабочая группа в составе:

_____ _____
(должность) *(Фамилия, Имя, Отчество)*

_____ _____
(должность) *(Фамилия, Имя, Отчество)*

составила настоящий акт о том, что на основании заявки/служебной записки _____
_____
(№, дата документа на инсталляцию СЗИ)

с технических средств и систем, приведенных в таблице 1, и находящихся в пользовании _____
(должность, фамилия, имя, отчество пользователя СЗИ)

произведена деинсталляция средства защиты информации (далее — СЗИ) _____
(наименование, версия СЗИ)

следующим способом:[1]_____ .

Таблица 1.

Технические средства и системы, размещенные в помещении № _____,
расположенном по адресу _____

№ п/п	Вид оборудования	Тип	Учетный (заводской) номер
1	2	3	4
1	*Приводятся сведения о техническом средстве (например, системный блок, моноблок), с жесткого диска которого деинсталлировано СЗИ*		
2	*Приводятся сведения о жестком диске, с которого деинсталлировано СЗИ*		

Лицо, проводившее деинсталляцию: _____
(должность, подпись, расшифровка подписи)

Пользователь СЗИ: _____
(должность, подпись, расшифровка подписи)

[1] К способам уничтожения относятся переформатирование, удаление программного обеспечения СЗИ, физическое уничтожение носителей информации.

Шаблон оформления проекта акта деинсталляции средства защиты информации

Приложение № 14

ЖУРНАЛ

поэкземплярного учета средств защиты информации, эксплуатационной и технической документации к ним

Начат с _____20___г.
Окончен _____20___г.

На _____листах
Срок хранения _____ лет

ФОРМА ЖУРНАЛА
поэкземплярного учета средств защиты информации, эксплуатационной и технической документации к ним

№ п/п	Наименование средства защиты информации, эксплуатационной и технической документации к ним	Серийный (заводской) номер	Номер специального защитного знака	Номер и срок действия сертификата соответствия на средства защиты	Ф.И.О., должность установившего средство защиты информации, дата установки (наименование организации, установившей средство защиты информации), дата установки	Место установки (наименование и серийный номер технического средства)/ место хранения	Примечание
1	2	3	4	5	6	7	8

Шаблон оформления журнала поэкземплярного учета средств защиты информации, эксплуатационной и технической документации к ним

Приложение № 15

ЖУРНАЛ
учета периодического тестирования средств защиты информации

Начат с _____20___г.
Окончен _____20___г.

На _____листах
Срок хранения _____ лет

№ п/п	Наименование средства защиты информации	Серийный (заводской) номер средства защиты информации	Дата тестирования	Ф.И.О. и подпись администратора информационной безопасности/ название организации, проводившего(ей) тестирование	Наименование теста, используемые средства для проведения теста	Результат тестирования (успешный/ неуспешный), комментарий	Дата очередного тестирования
1	2	3	4	5	6	7	8

Шаблон оформления журнала учета периодического тестирования средств защиты информации