АДМИНИСТРАЦИЯ СЫСЕРТСКОГО ГОРОДСКОГО ОКРУГА
П О С Т А Н О В Л Е Н И Е

от 16.05.2024 № 1789-ПА
г. Сысерть

Об утверждении положения об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Руководствуясь Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований к защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказом Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных», методическими рекомендациями по применению приказа Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных», утвержденными 13.12.2013 руководителем Роскомнадзора, ГОСТ Р 59853-2021. Национальный стандарт Российской Федерации. Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения, утвержденным и введенным в действие приказом Росстандарта от 19.11.2021 № 1520-ст, ГОСТ Р 50.1.053-2005 «Информационные технологии. Основные термины и определения в области технической защиты информации», утвержденным и введенным в действие приказом Ростехрегулирования от 06.04.2005 № 77-ст, ГОСТ Р 51275-2006. Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения, утвержденным и введенным в действие приказом Ростехрегулирования от 27.12.2006 № 374-ст, ГОСТ Р 50922-2006.

Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения, утвержденным и введенным в действие приказом Ростехрегулирования от 27.12.2006 № 373-ст,

ПОСТАНОВЛЯЮ:

1. Утвердить положение об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа (прилагается).

2. Начальнику отдела информационных технологий муниципального казенного учреждения «Управление хозяйственного и транспортного обслуживания Сысертского городского округа» О.Л. Соломеину довести настоящее постановление под подпись до работников Администрации Сысертского городского округа, ответственных за организацию и проведение работ по защите информации.

Исполняющий обязанности
Главы Сысертского
городского округа С.О. Воробьёв

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 4E70B9BFC13181EE0107980F09751A52
Владелец **Воробьёв Сергей Олегович**
Действителен с 28.02.2024 по 23.05.2025

УТВЕРЖДЕНО
постановлением Администрации
Сысертского городского округа
от 16.05.2024 № 1789-ПА
«Об утверждении положения об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа»

Положение об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Часть 1. Термины и определения

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

Вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа (далее – НСД) к информации и (или) воздействия на информацию или ресурсы информационной системы.

Доступ к информации – возможность получения информации и ее использования.

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.

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.

Информация – сведения (сообщения, данные) независимо от формы их представления.

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

ИС персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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

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

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

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Объект доступа (в автоматизированной ИС) – единица ресурса автоматизированной ИС, доступ к которой регламентируется правилами разграничения доступа.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Программное воздействие – несанкционированное воздействие на ресурсы автоматизированной ИС, осуществляемое с использованием вредоносных программ.

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

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

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

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

Уязвимость ИС – свойство ИС, обусловливающее возможность реализации угроз безопасности, обрабатываемой в ней информации.

Часть 2. Общие положения

Настоящее Положение об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа (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) при ее обработке в Администрации Сысертского городского округа (далее – Оператор).

Положение разработано с целью:

1) организации и координации работ по обеспечению безопасности защищаемой информации в ИС, взаимодействующих с федеральными государственными ИС и с региональными государственными ИС;

2) регламентации порядка проведения работ по обеспечению безопасности защищаемой информации, обрабатываемой в ИС и ИС персональных данных Администрации Сысертского городского округа;

3) контроля состояния безопасности защищаемой информации, обрабатываемой в ИС;

4) определение такого порядка обработки персональных данных, при котором обеспечиваются законные права и интересы субъектов персональных данных.

Положение обязательно для исполнения всеми лицами, участвующими в обработке защищаемой информации.

Часть 3. Пользователь ИС

3.1. Пользователем ИС является работник, который в силу своих должностных обязанностей осуществляет обработку защищаемой информации с использованием средств автоматизации и имеет доступ к информационным ресурсам, аппаратным средствам, программному обеспечению и средствам защиты информации.

3.2. Пользователь ИС несет персональную ответственность за свои действия.

3.3. Пользователь ИС в своей работе руководствуется нормативными правовыми актами в сфере персональных данных и локальными актами Оператора, определяющими порядок организации и проведения работ, направленных на обеспечение безопасности защищаемой информации при ее обработке.

3.4. Пользователь ИС обязан:

1) соблюдать требования нормативных правовых актов в сфере защиты информации и локальных актов Оператора, определяющих порядок организации и проведения работ, направленных на обеспечение безопасности защищаемой информации при их обработке в ИС;

2) выполнять на автоматизированном рабочем месте (далее – АРМ) в отношении защищаемой информации только те процедуры, которые определены для него в локальных актах Оператора, определяющих порядок организации и проведения работ, направленных на обеспечение безопасности защищаемой информации при ее обработке в ИС;

3) в случае временного отсутствия на рабочем месте для предотвращения доступа к информации, находящейся на АРМ, минуя ввод пароля, пользователь ИС во время перерыва в работе обязан осуществить блокирование системы нажатием комбинации Ctrl+Alt+Del и кнопки «Блокировать» в появившемся меню или выключить АРМ. По окончании рабочего дня пользователь ИС обязан выключить АРМ;

4) знать и соблюдать установленные требования по обработке и обеспечению безопасности персональных данных;

5) соблюдать требования антивирусной защиты в ИС;

6) соблюдать требования парольной защиты в ИС;

7) соблюдать правила при работе в сетях общего доступа и (или) международного обмена;

8) контролировать доступ посторонних лиц в помещения, в которых расположены компоненты ИС;

9) контролировать наличие и целостность пломб на корпусах технических средств в составе ИС.

3.5. Работа в сетях связи общего пользования и (или) сетях международного информационного обмена (далее – Сеть) на элементах ИС должна проводиться при служебной необходимости.

3.6. При работе в Сети запрещается:

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

2) скачивать из Сети программное обеспечение и другие файлы, непосредственно не связанных с исполнением служебных обязанностей, непосредственно не связанных с исполнением служебных обязанностей;

3) посещение сайтов, непосредственно не связанных с исполнением служебных обязанностей;

4) нецелевое использование подключения к Сети.

3.7. Обо всех выявленных нарушениях требований по обработке и обеспечению безопасности защищаемой информации пользователь ИС должен незамедлительно сообщать администратору информационной безопасности либо руководству.

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

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

3.10. Пользователю ИС запрещается:

1) разглашать защищаемую информацию третьим лицам;

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

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

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

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

6) самостоятельно вносить изменения в конфигурацию программного обеспечения и технические средства информационной системы, изменять установленный алгоритм функционирования технических и программных средств;

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

8) использовать АРМ и другие ресурсы ИС в неслужебных целях;

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

10) отключать (блокировать) средства защиты информации;

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

3.11. Пользователь ИС несет ответственность за:

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

2) совершенные в процессе осуществления своей деятельности правонарушения – в пределах, определенных административным, уголовным и гражданским законодательством Российской Федерации;

3) невыполнение или ненадлежащее выполнение поручений руководителя;

4) эксплуатацию ИС;

5) сохранность защищаемой информации;

6) соблюдение требований нормативных правовых актов в сфере защиты информации и локальных актов Оператора, определяющих порядок организации и проведения работ, направленных на обеспечение безопасности защищаемой информации при ее обработке в ИС;

7) сохранность и работоспособное состояние технических средств, программного обеспечения, средств защиты, входящих в состав ИС;

8) выполнение обязанностей, предусмотренных настоящим положением.

3.12. Пользователь ИС имеет право:

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, техническими средствами информационной системы, а также средствами защиты информации.

Часть 4. Первичный инструктаж лица, допущенного к работе с защищаемой информации

Первичный инструктаж лица, допущенного к работе с защищаемой информации (далее – лицо), проводит администратор информационной безопасности после утверждения руководителем документа о наделении лица правом доступа к защищаемой информации до непосредственного доступа этого лица к защищаемой информации.

Лицо получает непосредственный доступ к защищаемой информации только после прохождения первичного инструктажа.

Лицо должно быть ознакомлено с нормативными правовыми актами Российской Федерации в сфере защиты информации.

Лицо должно быть ознакомлено с локальными актами Оператора, регламентирующими вопросы защиты информации.

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

Администратор информационной безопасности, проводящий инструктаж лица, обязан разъяснить ему, какие действия в ИС лицо имеет право совершать, а какие действия ему запрещены.

Лицо, допущенное к работе с защищаемой информации, должно быть предупреждено:

1) об обязанностях выполнения всех правил и требований, предусмотренных локальными актами Оператора в области защиты информации;

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

Факт прохождения лицом первичного инструктажа регистрируется администратором информационной безопасности в соответствующем журнале учета пользователей, имеющих право доступа к информационным системам, форма которого приведена в приложении № 1 к настоящему Положению.

Часть 5. Обработка персональных данных без использования средств автоматизации

5.1. Порядок обработки персональных данных, осуществляемой без использования средств автоматизации осуществляется в соответствии с Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687.

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях, обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами, а также настоящим порядком.

5.2. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

1) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, полное наименование и адрес Оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых способов обработки персональных данных;

2) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, – при необходимости получения письменного согласия на обработку персональных данных;

3) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел

возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

4) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

5.3. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию Оператора, или в иных аналогичных целях, должны соблюдаться следующие условия:

1) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена локальным актом Оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится Оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

2) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

3) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию Оператора.

5.4. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

1) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

2) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

5.5. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

5.6. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

5.7. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

5.8. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

5.9. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

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

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

Доступ иных лиц в помещения Оператора, где осуществляется обработка защищаемой информации, разрешается только в присутствии лиц, имеющих право доступа к защищаемой информации, обрабатываемой в соответствующем помещении.

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

Защищаемая информация на бумажных носителях и машинные носители защищаемой информации (диски, флеш-карты) должны храниться в недоступном для посторонних лиц месте: в шкафах, оборудованных замками.

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

Вскрытие и закрытие помещений, в которых ведется обработка защищаемой информации, производится работниками Оператора, имеющими

право доступа к защищаемой информации, обрабатываемой в соответствующем помещении.

6.2. Перед закрытием помещений, в которых осуществляется обработка защищаемой информации, по окончании служебного дня работники, имеющие право доступа к защищаемой информации, обрабатываемой в соответствующем помещении, обязаны:

1) убрать бумажные носители защищаемой информации и машинные носители защищаемой информации (диски, флеш-карты) в запираемые шкафы, запереть шкафы на замок;

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

3) закрыть окна, двери.

6.3. Перед открытием помещений, в которых осуществляется обработка защищаемой информации, работники 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.

6.4. 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.

6.5. При работе с защищаемой информации двери помещений должны быть всегда закрыты.

Присутствие лиц, не имеющих права доступа к защищаемой информации, должно быть исключено.

6.6. Доступ в помещения, где осуществляется обработка защищаемой информации, вспомогательного и обслуживающего персонала (уборщиц, электромонтеров, сантехников и других лиц) разрешается только в случае служебной необходимости в сопровождении лица, имеющего право доступа к защищаемой информации, обрабатываемой в соответствующем помещении, после принятия мер, исключающих визуальный просмотр документов, содержащих защищаемую информацию, и экранов мониторов.

6.7. Корпус технического средства, с которым осуществляется штатное функционирование ИС, должен быть оборудован средствами контроля их вскрытия (опечатаны, опломбированы), место опечатывания (опломбирования) должно быть визуально контролируемым.

6.8. Внутренняя планировка и расположение рабочих мест в помещениях, где осуществляется обработка защищаемой информации, должны исключать визуальный просмотр обрабатываемой защищаемой информации для

работников, не осуществляющих обработку такой информации. Окна помещений, в которых осуществляется обработка защищаемой информации, должны быть оборудованы шторами (жалюзи).

В случае, когда помещения, в которых осуществляется обработка защищаемой информации, располагаются на первых и последних этажах здания, их окна должны быть оснащены прочными решетками или жалюзи.

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

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

6.9. Помещения, предназначенные для размещения архивов, должны отвечать следующим требованиям:

1) помещение должно располагаться в контролируемой зоне;

2) двери помещения должны иметь надежные запоры, приспособления для опечатывания, либо должны быть оснащены контроллерами, включенными в систему контроля ограничения доступа;

3) желательно наличие видеокамеры системы видеозаписи, контролирующей вход в помещение;

4) должны быть задействованы все меры, исключающие неконтролируемое пребывание в помещении любых лиц, включая работников, не допущенных к работе с защищаемой информацией;

5) помещение должно быть оборудовано датчиками пожарной и охранной сигнализации, желательно имеющими отдельные (не связанные с другими помещениями) шлейфы сигнализации, включенные в пульты охранно-пожарной сигнализации;

6) помещение должно быть оборудовано средствами пожаротушения, желательно наличие автономной автоматической системы пожаротушения;

7) помещение должно быть оборудовано необходимым количеством стеллажей и/или запираемых металлических шкафов для хранения архивных носителей;

8) микроклимат (температурно-влажностный режим) помещения должен отвечать требованиям по сохранности архивных носителей, а условия хранения должны исключать возможность их повреждения (коробления, пересыхания, изгиба и вредного воздействия пыли, магнитных и электрических полей или ультрафиолета);

9) помещение, предназначенное для хранения резервных копий, не должно совмещаться с помещением, в котором размещается оборудование, создающее и/или использующее указанные резервные копии.

Работник, осуществляющий хранение архивов и/или резервных копий ИС, должен иметь печать для опечатывания дверей и сейфа или металлического хранилища.

Часть 7. Контроль и надзор за соблюдением требований по обработке и обеспечению безопасности защищаемой информации

7.1. Контроль и надзор за соблюдением требований по обработке и обеспечению безопасности защищаемой информации Оператора состоит из следующих направлений:

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

2) внутренний контроль за обеспечением уровня защищенности информации (в том числе внутренний контроль соответствия обработки защищаемой информации требованиям к обеспечению безопасности защищаемой информации) (далее – внутренний контроль за обеспечением уровня защищенности информации).

7.2. Внутренний контроль за обеспечением уровня защищенности информации осуществляется Оператором и состоит из:

1) контроля и надзора за исполнением требований по обработке и обеспечению безопасности защищаемой информации с учетом ее уровня защищенности;

2) оценки соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер.

7.3. Внешний контроль и надзор за выполнением требований законодательства в области защиты информации осуществляется:

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

2) Федеральной службой безопасности Российской Федерации в пределах своих полномочий;

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

7.4. Порядок внутреннего контроля за обеспечением уровня защищенности информации.

Оператор при обработке защищаемой информации обязан принимать необходимые правовые, организационные и технические меры для обеспечения безопасности защищаемой информации от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении защищаемой информации.

7.5. Внутренний контроль за обеспечением уровня защищенности информации – это комплекс мероприятий, осуществляемых в целях:

1) соблюдения условий и принципов обработки защищаемой информации;

2) соблюдения требований по обработке и обеспечению безопасности 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) хищения технических средств, входящих в состав ИС, и машинных носителей защищаемой информации;

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

7.6. Основными задачами внутреннего контроля за обеспечением уровня защищенности информации являются:

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

2) соблюдение прав субъектов персональных данных, чьи персональные данные обрабатываются Оператором;

3) наличие необходимых согласий субъектов персональных данных, чьи персональные данные обрабатываются Оператором;

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

5) проверка соблюдения требований нормативных правовых актов, методических документов в сфере обеспечения безопасности защищаемой информации при подготовке организационно-распорядительной документации;

6) проверка организации и выполнения мероприятий по обеспечению безопасности защищаемой информации при ее обработке как с использованием средств автоматизации, так и без использования средств автоматизации;

7) проверка работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией;

8) наличие эксплуатационной документации на технические и программные средства защиты ИС;

9) оценка знаний и качества выполнения работниками своих функциональных обязанностей в части защиты информации;

10) оперативное принятие мер по пресечению нарушений требований по обеспечению безопасности информации при ее обработке в ИС.

7.7. Внутренний контроль за обеспечением уровня защищенности информации осуществляется ответственным за обеспечение уровня защищенности информации в ИС один раз в полгода. О результатах проверки и мерах, необходимых для устранения выявленных нарушений, администратор информационной безопасности докладывает руководству и производит отметку в журнале учета проведения контроля за обеспечением уровня защищенности информации, форма которого установлена приложением № 13.

7.8. Оценкой вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» является определение юридических последствий в отношении субъекта персональных данных, которые могут возникнуть в случае нарушения Федерального закона «О персональных данных».

К юридическим последствиям относятся случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или иным образом затрагивающее его права, свободы и законные интересы.

При обработке персональных данных должны определяться и документально оформляться все возможные юридические или иным образом затрагивающие права и законные интересы последствия в отношении субъекта персональных данных, которые могут возникнуть в случае нарушения Федерального закона «О персональных данных».

Определение таких юридических последствий необходимо для недопущения нарушения Федерального закона «О персональных данных» и обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», оформляется документально.

7.9. Во время осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных производится оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» и применяемых мер, направленных на выполнение обязанностей, предусмотренных Федеральным законом «О персональных данных».

При оценке соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», для ИС производится экспертное сравнение заявленной Оператором в своих локальных актах оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» и применяемых мер, направленных на выполнение обязанностей, предусмотренных Федеральным законом «О персональных данных», и изложенных в настоящем Положении.

По итогам сравнений принимается решение о достаточности применяемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области персональных данных и возможности или необходимости принятия дополнительных мер или изменения установленного порядка организации и проведения работ по обеспечению безопасности персональных данных при их обработке.

Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований Федерального закона

«О персональных данных» и применяемых мер, направленных на выполнение обязанностей, предусмотренных Федеральным законом «О персональных данных», оформляется в виде отдельного документа, подписывается ответственным лицом.

Часть 8. Порядок проведения служебной проверки по фактам нарушения требований по обеспечению безопасности защищаемой информации

8.1. Нарушения требований по обеспечению безопасности защищаемой информации и их последствия классифицируются по значимости на:

- нарушения I категории;
- нарушения II категории;
- нарушения III категории.

Служебная проверка назначается по нарушениям I и II категорий.

8.2. Нарушения I категории, к которым относятся нарушения, 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 ИС, а именно:

1) успешный подбор административного пароля;

2) несанкционированная реконфигурация параметров ИС;

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

4) необоснованная передача информационных массивов ИС;

5) организация утечки сведений по техническим каналам;

6) умышленное нарушение работоспособности ИС;

7) НСД к защищаемой информации;

8) несанкционированное внесение изменений в ИС;

9) умышленное заражение АРМ и серверов, входящих в состав ИС, вирусами;

10) проведение работ с ИС, повлекшее за собой необратимую потерю данных;

11) другие действия, попадающие под действия статей, приведенных в таблице № 1.

Таблица № 1

№ п/п	Название правового акта	Номер статьи	Название статьи
1.	Федеральный закон «Об информации, информационных технологиях и о защите информации»	17	Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации
2.	Федеральный закон «О персональных данных»	24	Ответственность за нарушение требований настоящего Федерального закона
3.	Кодекс Российской Федерации об административных правонарушениях	5.39	Отказ в предоставлении информации
4.		13.11	Нарушение законодательства Российской Федерации в области персональных данных
5.		13.11.1	Распространение информации о свободных рабочих местах или вакантных должностях, содержащей ограничения дискриминационного характера
6.		13.12	Нарушение правил защиты информации

№ п/п	Название правового акта	Номер статьи	Название статьи
7.		13.14	Разглашение информации с ограниченным доступом
8.		19.7	Непредставление сведений (информации)
9.	Уголовный кодекс Российской Федерации	137	Нарушение неприкосновенности частной жизни
10.		140	Отказ в предоставлении гражданину информации
11.		272	Неправомерный доступ к компьютерной информации
12.		273	Создание, использование и распространение вредоносных компьютерных программ
13.		274	Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей
14.	Трудовой кодекс Российской Федерации	90	Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных сотрудника

8.3. Нарушения II категории, к которым относятся нарушения, 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 ИС, а именно:

1) ошибка при входе в ИС (набор не назначенного пароля, более трех раз подряд, периодически);

2) оставление АРМ включенным (незаблокированным) во время отсутствия на рабочем месте;

3) перезагрузка АРМ при сбоях в работе, в том числе аварийная (неоднократная) перезагрузка путем нажатия кнопки RESET;

4) утрата учтенного машинного носителя защищаемой информации;

5) многократная неудачная попытка входа под чужим именем, паролем;

6) удачная попытка входа под чужим именем, паролем;

7) несанкционированная очистка журналов аудита;

8) несанкционированное копирование защищаемой информации на внешние носители информации;

9) несанкционированная установка (удаление) программного обеспечения в ИС;

10) несанкционированное изменение конфигурации программного обеспечения ИС;

11) попытка получения прав администратора на АРМ (увеличения полномочий собственных прав, получение прав на отладку программ) удачная и неудачная;

12) попытка получения прав администратора в домене или на удаленной машине, удачная и неудачная;

13) неумышленное заражение АРМ компьютерными вирусами;

14) несанкционированное использование сканирующего программного обеспечения;

15) несанкционированное использование анализаторов протоколов (снифферов);

16) несанкционированный просмотр, вывод на печать и т.п. защищаемой информации.

8.4. Нарушения III категории, к каковым относятся нарушения, не несущие признаков нарушений I и II категорий, а именно:

1) ошибка при входе в ИС (набор неправильного пароля, сетевого имени более трех раз подряд, не периодическая);

2) периодическая попытка неудачного доступа к защищаемой информации ИС;

3) перевод времени на АРМ;

4) однократная перезагрузка АРМ при сбоях в работе АРМ, в том числе аварийная перезагрузка, путем нажатия кнопки RESET;

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

8.5. Служебная проверка назначается по нарушениям I и II категорий.

Служебная проверка может быть инициирована на основании устного заявления, докладной или служебной записки любого работника по выявленному отдельному факту нарушения, либо по факту группы нарушений.

Служебная проверка проводится комиссией, состав которой утверждается муниципальным правовым актом Администрации Сысертского городского округа.

В случае необходимости вышеуказанной комиссии может привлекать к работе:

- непосредственного начальника нарушителя;
- экспертов из других подразделений;
- специалистов организаций-лицензиатов ФСТЭК России и ФСБ РФ.

Члены комиссии имеют право:

- требовать документального подтверждения факта нарушений информационной безопасности;
- устанавливать причины допущенных нарушений любым из способов, не противоречащих законодательству Российской Федерации;
- брать письменные объяснения по поводу выявленных нарушений у любого работника Оператора.

За выявление и классификацию нарушения требований по обеспечению безопасности защищаемой информации, требующего проведения процедуры служебной проверки, ответственность несет администратор информационной безопасности.

За назначение процедуры служебной проверки ответственность несет руководитель Оператора.

Результаты работы комиссии должны быть оформлены в виде аналитического экспертного заключения на имя руководителя с предложениями о необходимых организационных выводах, а также о

расширении или дополнении перечня нарушений требований по обеспечению безопасности защищаемой информации.

Результатом работы Комиссии должен стать акт, в котором изложены:

- состав комиссии;
- период времени, в течение которого проводилась служебная проверка;
- основание для проведения служебной проверки;
- документальное подтверждение фактов нарушений, выявленных в ходе служебной проверки и имеющих значение в определении наличия нарушений, а также иных фактов, которые могут привести к нарушению конфиденциальности защищаемой информации или к снижению уровня защищенности персональных данных;
- установленные причины выявленных нарушений;
- вывод о значимости, их причинах и виновных, допустивших данные нарушения;
- сформированные предложения по устранению причин выявленных нарушений;
- рекомендации по совершенствованию обеспечения безопасности защищаемой информации, исключающие в дальнейшем подобные нарушения.

8.6. При обнаружении нарушений I категории обработка персональных данных незамедлительно приостанавливается до выявления причин нарушений и устранения этих причин.

Принятие решения о приостановлении обработки персональных данных принимается руководителем Оператора.

По факту нарушения требований по обеспечению безопасности, повлекшего приостановление обработки персональных данных, проводится служебная проверка.

Часть 9. Обезличивание персональных данных

9.1. В соответствии с Федеральным законом «О персональных данных» обезличивание персональных данных может быть проведено:

1) если обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением таких целей как продвижение товаров, работ и услуг на рынке, политической агитации;

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

Обезличивание персональных данных осуществляется с учетом методических рекомендаций по применению приказа Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных», утвержденными 13.12.2013 руководителем Роскомнадзора.

9.2. Методы обезличивания должны обеспечивать требуемые свойства обезличенных данных, соответствовать предъявляемым требованиям к их характеристикам (свойствам), быть практически реализуемыми в различных программных средах и позволять решать поставленные задачи обработки

персональных данных. К наиболее перспективным и удобным для практического применения относятся следующие методы обезличивания:

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

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

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

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

9.3. Процедура обезличивания обеспечивает практическую реализацию метода обезличивания и задается своим описанием.

Допускается программная реализация процедуры различными способами и средствами.

9.4. При использовании процедуры обезличивания не допускается совместное хранение персональных данных и обезличенных данных.

Обезличивание персональных данных субъектов должно производиться перед внесением их в ИС.

Оператор вправе обрабатывать в ИС обезличенные данные, полученные от третьих лиц.

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

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

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

Хранение и защиту дополнительной (служебной) информации, содержащей параметры методов и процедур обезличивания/деобезличивания, следует обеспечить в соответствии с внутренними процедурами обеспечения конфиденциальности, установленными Оператором. При этом должно обеспечиваться исполнение установленных правил доступа пользователей к хранимым данным, резервного копирования и возможности актуализации и восстановления хранимых данных.

Процедуры обезличивания/деобезличивания должны встраиваться в процессы обработки персональных данных как их неотъемлемый элемент, а

также максимально эффективно использовать имеющуюся у Оператора инфраструктуру, обеспечивающую обработку персональных данных.

9.5. При выборе методов и процедур обезличивания персональных данных следует руководствоваться целями и задачами обработки персональных данных.

Обезличивание персональных данных, 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 персональными данными (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.

При выборе метода и процедуры обезличивания также следует учитывать:

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

2) форму 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 ИС меры по обеспечению безопасности данных.

Ниже представлены типовые классы задач, состоящие из наиболее часто встречающихся задач обработки персональных данных. Проведенная классификация позволяет Оператору применять наиболее эффективные для данного класса методы.

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.	Статистическая обработка и статистические исследования персональных данных	- осуществление выборки по заявленным параметрам; - проведение исследований по заданным параметрам субъектов	- перемешивания; - декомпозиции; - изменения состава или семантики
2.	Сбор и хранение персональных данных	внесение персональных данных субъектов в информационную систему на основе анкет, заявлений и прочих документов	- декомпозиции; - перемешивания; - 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 персональные данные;	-перемешивания; - декомпозиции; - введения идентификаторов

№ п/п	Класс задач	Задачи обработки	Метод обезличивания
		- выдача справок, выписок, уведомлений по запросам субъектов или уполномоченных органов	
4.	Актуализация персональных данных	- 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 Российской Федерации	-перемешивания; - декомпозиции; - введения идентификаторов
5.	Интеграция данных различных операторов	- поиск информации о субъектах; - передача данных смежным органам	- перемешивания; - декомпозиции; - введения идентификаторов
6.	Ведение учета субъектов персональных данных	- прием анкет, заявлений; - ведение учета персональных данных в соответствии с функциями органа	- декомпозиции; - перемешивания; - введения идентификаторов

При наличии в системе нескольких классов задач рекомендуется выбирать общий метод для всех этих классов, либо совместно применять несколько методов.

Часть 10. Уничтожение защищаемой информации

10.1. Уничтожение защищаемой информации должно быть проведено:

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

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

3) в случае выявления фактов неправомерной обработки персональных данных (в том числе при обращении субъекта персональных данных) при невозможности обеспечения правомерности их использования.

10.2. 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 информации подходящим способом, указанным в соответствующем требовании или распорядительном документе;

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

10.3. Уничтожение защищаемой информации возможно осуществить одним из следующих способов:

1) физическое уничтожение носителя защищаемой информации;

2) уничтожение защищаемой информации с машинного носителя

информации.

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

Уничтожение информации на машинных носителях необходимо осуществлять путем стирания информации с использованием программного обеспечения с гарантированным уничтожением. При уничтожении защищаемой информации необходимо учитывать возможность ее наличия в архивных базах данных и производить уничтожение во всех копиях базы данных, если иное не установлено действующим законодательством Российской Федерации.

Если защищаемая информация хранится 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 программного обеспечения 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 составляется акт уничтожения защищаемой информации либо акт уничтожения машинных носителей информации, формы которых приведены в приложениях № 2 и 3 к настоящему положению.

Часть 11. Порядок управления доступом субъектов доступа к объектам доступа в ИС

11.1. Предоставление доступа пользователю к ИС (или изменение прав доступа) осуществляется на основании перечня лиц, имеющих право доступа к защищаемой информации, обрабатываемой в ИС, утвержденного руководителем.

11.2. С целью организации учета лиц, имеющих право доступа к защищаемой информации, обрабатываемой в ИС, ведется журнал учета пользователей, имеющих право доступа к информационным системам, форма которого приведена в приложении № 1 к настоящему положению.

11.3. Назначение прав доступа пользователей к защищаемой информации в ИС осуществляется администратором информационной безопасности в соответствии с заявками на предоставление пользователю ИС прав доступа к ИС (ресурсу ИС) от руководителя структурного подразделения, оформляемыми по форме, приведенной в приложении № 4 к настоящему положению. При этом в журнале учета пользователей, имеющих право доступа к информационным системам, производится соответствующая запись.

11.4. Все факты несанкционированной организации доступа и регистрации в ИС, а также их последствия классифицируются в соответствии с Перечнем нарушений требований по обеспечению безопасности защищаемой информации.

11.5. Контроль за деятельностью пользователей ИС ведется администратором информационной безопасности.

11.6. Наличие у сотрудника избыточных, неконтролируемых прав доступа является нарушением требований по обеспечению безопасности защищаемой информации.

11.7. Основанием для прекращения права доступа пользователя к ИС может служить его исключение из утвержденного руководителем перечня лиц, имеющих право доступа к защищаемой информации, обрабатываемой в ИС, или его увольнение.

Часть 12. Организация парольной защиты в ИС

12.1. Целью применения и реализации парольной защиты является исключение утечки защищаемой информации, а также ее несанкционированной модификации или уничтожения.

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

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

12.2. Защите паролем подлежит доступ к следующей информации:

1) базовая система ввода-вывода АРМ, входящей в состав ИС;

2) настройки операционной системы;

3) настройки сетевого оборудования;

4) настройки средств защиты информации;

5) программное обеспечение, предназначенное для обработки защищаемой информации;

6) ресурсы АРМ и информационные ресурсы, содержащие защищаемую информацию.

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

1) длина пароля должна быть не менее 15 (пятнадцати) 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, наименования АРМ, общепринятые сокращения (например, ЭВМ, ЛВС, USER, ADMINISTRATOR и

т.д.) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе ИС;

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 пароли.

12.4. Лица, использующие паролирование, 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.

12.5. При организации парольной защиты запрещается:

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

2) хранить пароли в записанном виде на отдельных листах бумаги;

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

12.6. 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 прекращения полномочий пользователя (увольнение, переход на другую работу внутри организации) – после завершения последнего сеанса работы данного пользователя с системой;

4) по указанию администратора информационной безопасности;

5) в случае прекращения полномочий (увольнение, переход на другую работу внутри организации) администратора информационной безопасности.

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

12.8. Порядок применения (смены) паролей при работе на АРМ, оборудованных системой защиты от НСД, приведен в эксплуатационной документации на СЗИ.

12.9. Факт выдачи пароля пользователю ИС фиксируется в журнале учета выдачи паролей для доступа к информационным системам, форма которого приведена в приложении № 5 к настоящему положению.

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

12.11. Ответственность за соблюдение требований парольной защиты возлагается на администратора информационной безопасности и пользователей ИС.

12.12. Нарушения организации и порядка применения парольной защиты классифицируются в соответствии с перечнем нарушений требований по обеспечению безопасности защищаемой информации.

При выявлении нарушений I и II категории проводится служебная проверка в соответствии с порядком проведения служебной проверки по фактам нарушения требований по обеспечению защищаемой информации.

Часть 13. Организация идентификации и аутентификации пользователей ИС

13.1. Управление атрибутами доступа пользователей ИС (идентификаторы и пароли) осуществляется администратором информационной безопасности.

Запрещены действия пользователей до прохождения ими процедур идентификации и аутентификации в ИС.

13.2. Процессы формирования, присвоения, смены и прекращения действия идентификаторов выполняются администратором информационной безопасности.

При добавлении нового пользователя ИС (установленным порядком) администратор информационной безопасности должен зарегистрировать для него персональный идентификатор.

13.3. Идентификатор подлежит блокировке в следующих случаях:

1) при неиспользовании идентификатора более трех месяцев;

2) при увольнении владельца идентификатора – с целью предотвращения его повторного использования – немедленно после окончания последнего сеанса работы данного пользователя с системой.

Удалению подлежат идентификаторы, заблокированные более трех лет.

Часть 14. Управление аутентификационной информацией

14.1. Защите паролем (при наличии такой технической возможности) подлежит доступ к следующим ресурсам:

1) базовым системам ввода-вывода компьютеров;

2) настройкам сетевого оборудования;

3) настройкам операционных систем;

4) настройкам средств защиты информации (в том числе средств антивирусной защиты);

5) запуску специализированного программного обеспечения, предназначенного для обработки защищаемой информации (в том числе персональных данных;

6) ресурсам ИС, содержащих защищаемую информацию.

14.2. Объекты парольной защиты необходимо настраивать таким образом, чтобы:

1) исключить возможность просмотра ранее вводимых паролей;

2) блокировать доступ пользователей к ИС после десятикратной ошибки при вводе пароля (правом снятия блокировки обладает только администратор информационной безопасности);

3) автоматически блокировать сеанс доступа пользователя ИС после его бездействия (неактивности) в течение пятнадцати минут;

4) исключить ознакомление посторонних лиц с аутентификационной информацией в процессе ее ввода (защита обратной связи).

14.3. Запрещается пользоваться аутентификационной информацией, заданной производителем технического средства (программного обеспечения).

14.4. Личные пароли доступа пользователей ИС генерируются и выдаются администратором информационной безопасности или создаются пользователем самостоятельно с учетом следующих требований:

1) длина пароля должна быть не менее пятнадцати 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, наименования АРМ, общепринятые сокращения (например, ЭВМ, ЛВС, USER, ADMINISTRATOR и т.д.) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе ИС;

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 не менее чем в двух символах;

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 пароли.

14.5. Разрешается использовать специализированное программное обеспечение для формирования паролей.

14.6. Полная плановая смена паролей проводится один раз в три месяца.

14.7. Внеплановая смена пароля пользователя ИС должна производиться в случае прекращения полномочий пользователя после завершения последнего сеанса работы данного пользователя с системой.

14.8. В случае прекращения полномочий администратора информационной безопасности производится внеплановая полная смена всех паролей, к которым он имел доступ.

14.9. В случае компрометации личного пароля должны быть немедленно предприняты вышеуказанные меры в зависимости от полномочий владельца скомпрометированного пароля.

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

14.11. При организации парольной защиты запрещается:

1) записывать свои пароли в очевидных местах (например, на мониторе АРМ, на обратной стороне клавиатуры);

2) хранить пароли в записанном виде на отдельных листах бумаги;

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

Часть 15. Организация антивирусной защиты в ИС

15.1. Целью антивирусной защиты ИС является предотвращение и нейтрализация негативных воздействий вредоносного программного обеспечения на информационные ресурсы, содержащие защищаемую информацию, и программного обеспечения, предназначенного для обработки защищаемой информации.

Порядок организации антивирусной защиты определяет требования к организации защиты ИС от разрушающего воздействия вредоносного программного обеспечения и устанавливают ответственность за их выполнение.

К использованию в ИС допускаются только лицензионные и сертифицированные ФСТЭК России по требованиям безопасности информации средства защиты от вредоносного программного обеспечения.

Установка и начальная настройка средств защиты от вредоносного программного обеспечения в ИС может осуществляться администратором информационной безопасности, а также представителями организации-лицензиата ФСТЭК России.

Администратор информационной безопасности должен организовывать осуществление периодического обновления сигнатур средств защиты от вредоносного программного обеспечения и контроль их работоспособности не реже одного раза в неделю.

Пользователи ИС обязаны руководствоваться в работе Порядком организации антивирусной защиты, установленным пунктом 15.2 части 15 настоящего положения.

15.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), защищаемая информация, содержащиеся 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 проходят антивирусный контроль. Периодические проверки электронных архивов проводятся администратором информационной безопасности не реже одного раза в месяц.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вредоносного программного обеспечения. После установки (изменения) программного обеспечения АРМ должна быть осуществлена антивирусная проверка ИС.

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

В случае обнаружения вредоносного программного обеспечения при проведении антивирусной проверки пользователь ИС обязан:

- приостановить работу АРМ;
- немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения администратора информационной безопасности, а также других пользователей ИС, использующих зараженные файлы в работе;
- совместно с владельцем зараженных вредоносным программным обеспечением файлов провести анализ возможности их дальнейшего использования;
- провести «лечение» или удаление зараженных файлов.

Периодически, но не реже одного раза в неделю, администратором информационной безопасности должна проводиться антивирусная проверка всех жестких дисков серверов.

Антивирусные проверки подлежат регистрации в журнале учета антивирусных проверок информационных систем, форма которого приведена в приложении № 6 к настоящему положению.

Ответственность за проведение мероприятий антивирусной защиты и контроля, соблюдения требований антивирусной защиты в ИС возлагается на администратора информационной безопасности.

Часть 16. Организация учета машинных носителей защищаемой информации

16.1. Регистрации и учету подлежат все машинные носители информации, содержащие защищаемую информацию, а именно:

- жесткие диски, находящиеся в системных блоках серверов;
- жесткие диски, находящиеся во внешних RAID-массивах серверов;
- жесткие диски, находящиеся в системных блоках АРМ ИС;
- кассеты со стриммерными лентами, находящиеся в стриммерных устройствах;
- USB-носители, находящиеся у пользователей ИС и содержащие резервные копии;
- CD-R, CD-RW, DVD-R и/или DVD-RW-носители,

подлежат регистрации и учету.

Учетный номер носителя, содержащего защищаемую информацию, должен наноситься непосредственно на корпус носителя и быть нестираемым.

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

Запрещено использование в ИС неучтенных машинных носителей информации для обработки защищаемой информации.

Регистрация действий по подключению к ИС машинных носителей информации осуществляется в электронных журналах средств защиты информации от НСД.

Запрещается копирование защищаемой информации пользователями ИС с целью их передачи другим работникам или посторонним лицам.

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

Полученные извне машинные носители информации, содержащие необходимую для деятельности защищаемую информацию, должны:

- проверяться на наличие вредоносных программных продуктов;
- учитываться в соответствии с настоящей политикой;
- передаваться работникам, являющимся пользователями ИС, только с разрешения руководителя структурного подразделения с записью в соответствующих формах учета.

Регистрацию и учет машинных носителей защищаемой информации для каждой ИС осуществляет администратор информационной безопасности в соответствующем журнале учета машинных носителей информации, форма которого приведена в приложении № 7 к настоящему положению.

16.2. Хранение машинных носителей защищаемой 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 защищаемой информации.

Машинные носители защищаемой информации должны храниться в недоступном для посторонних лиц месте: в шкафах, оборудованных замками.

16.3. Выдача машинных носителей защищаемой информации пользователям ИС производится администратором информационной безопасности под подпись в соответствующем журнале учета машинных носителей информации.

Передача машинных носителей защищаемой информации для ремонта или утилизации запрещена.

Все машинные носители защищаемой информации, потерявшие актуальность, передаются администратору информационной безопасности. По результатам уничтожения защищаемой информации с машинного носителя или форматирования машинного носителя, или уничтожения машинного носителя составляется акт об уничтожении защищаемой информации и/или акт об уничтожении машинного носителя защищаемой информации. По факту уничтожения машинного носителя защищаемой информации в журнале учета машинных носителей информации производится отметка об уничтожении.

Часть 17. Организация резервирования и восстановления информации в ИС

17.1. С целью обеспечения возможности незамедлительного восстановления защищаемой информации в ИС, модифицированной или уничтоженной вследствие НСД к ней или возникновении нештатных ситуаций, повлекших за собой потерю данных, организуется резервирование и восстановление информации в ИС, а также работоспособности ИС.

17.2. Резервному копированию подлежат следующие информационные ресурсы:

- файлы, каталоги, базы данных ИС, содержащие защищаемую информацию;
- системные и конфигурационные файлы операционной системы и специального программного обеспечения серверов;
- конфигурационные файлы сетевого оборудования;
- системные и конфигурационные файлы средств защиты информации.

17.3. Резервное копирование защищаемой информации 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 информационных систем, форма которого приведена в приложении № 8 к настоящему положению.

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 программного обеспечения. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

Машинные носители информации с обновлениями программного обеспечения 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.

17.4. В случае возникновения нештатной ситуации, вызвавшей полную или частичную потерю работоспособности ИС, должно быть обеспечено ее восстановление из резервной копии. Факт возникновения нештатной ситуации в ИС подлежит обязательной регистрации в журнале учета нештатных ситуаций в информационных системах, форма которого приведена в приложении № 9 к настоящему положению.

При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование информационных ресурсов,

содержащих защищаемую информацию, затем производится полное уничтожение некорректно работающего программного обеспечения.

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

При работе в ИС рекомендуется использовать источники бесперебойного питания с целью предотвращения повреждения технических средств, входящих в состав ИС, и (или) защищаемой информации, в результате сбоев в сети электропитания.

Восстановление средств защиты информации производится с использованием дистрибутива. Дистрибутив может быть получен как на машинном носителе информации, так и с официального сайта производителя (разработчика). Порядок получения дистрибутива средств защиты информации устанавливается производителем (разработчиком).

При восстановлении работоспособности средств защиты информации необходимо выполнить их настройку в соответствии с требованиями безопасности информации. После настройки средств защиты информации выполняется резервное копирование настроек данных средств зашиты информации с помощью встроенных в них функций на учтенный машинный носитель информации.

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

Часть 18. Порядок работы с электронными журналами протоколирования и анализа (аудита) значимых событий (регистрация событий безопасности)

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

18.2. Источники событий безопасности, подлежащих регистрации в соответствующих электронных журналах:

1) средства защиты информации;

2) программное обеспечение ИС и СУБД;

3) общесистемное и прикладное программное обеспечение.

18.3. Перечень событий безопасности, подлежащих фиксации средствами защиты информации:

1) регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останов. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

- результат попытки входа: успешная или неуспешная - несанкционированная;

- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

- код или пароль, предъявленный при неуспешной попытке;

2) регистрация выдачи печатных (графических) документов на «твердую» копию. В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);

- спецификация устройства выдачи [логическое имя (номер) внешнего устройства];

- краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;

- идентификатор субъекта доступа, запросившего документ;

3) регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

- дата и время запуска;

- имя (идентификатор) программы (процесса, задания);

- идентификатор субъекта доступа, запросившего программу (процесс, задание);

- результат запуска (успешный, неуспешный - несанкционированный);

4) регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;

- идентификатор субъекта доступа;

- спецификация защищаемого файла;

5) регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;

- идентификатор субъекта доступа;

- спецификация защищаемого объекта [логическое имя (номер)].

18.4. Проверка электронного журнала событий средств защиты информации от НСД производится в соответствии с прилагаемой к ним технической и эксплуатационной документацией.

Срок хранения электронного журнала событий средств защиты информации от НСД должен быть не менее одного года.

18.5. Средство защиты информации от НСД должно сигнализировать администратору информационной безопасности о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий

безопасности. В этом случае администратор информационной безопасности должен предпринять меры для устранения возникшего сбоя с учетом требований настоящего положения и технической и эксплуатационной документации на средства защиты информации от НСД.

Для всех АРМ в составе ИС должна быть обеспечена синхронизация системного времени.

18.6. Администратор информационной безопасности должен еженедельно осуществлять анализ электронных журналов:

1) средств защиты информации;

2) программное обеспечение ИС и СУБД;

3) общесистемное и прикладное программное обеспечение с обязательной регистрацией в журнале проверки электронных журналов информационных систем, форма которого приведена в приложении № 10 к настоящему положению.

Часть 19. Порядок обращения со средствами защиты информации

19.1. Под средствами защиты информации в настоящей части понимается средство защиты информации, не являющееся средствами криптографической защиты.

Процедура установки средства защиты информации сопровождается оформлением акта установки средства защиты информации, форма которого приведена в приложении № 14 к настоящему положению. В случае необходимости деинсталляции средства защиты информации оформляется соответствующая заявка, форма которой приведена в приложении № 15 к настоящему положению. Процедура деинсталляции средства защиты информации сопровождается оформлением акта деинсталляции средства защиты информации, форма которого приведена в приложении № 16 к настоящему положению.

Инсталлирующие средства защиты информации носители, установленные средства защиты информации, эксплуатационная и техническая документация к средствам защиты информации подлежат поэкземплярному учету в журнале поэкземплярного учета средств защиты информации информационных систем, эксплуатационной и технической документации к ним, форма которого приведена в приложении № 11 к настоящему положению.

Администратор информационной безопасности должен осуществлять один раз в месяц тестирование средств защиты информации с отметкой в журнале учета периодического тестирования средств защиты информации информационных систем, форма которого приведена в приложении № 12 к настоящему положению.

19.2. Средства защиты информации доставляются фельдъегерской (в том числе ведомственной) связью или со специально выделенными работниками при соблюдении мер, исключающих бесконтрольный доступ к средствам защиты информации во время доставки.

При пересылке средства защиты информации помещаются в прочную упаковку, исключающую возможность их физического повреждения и

внешнего воздействия. Эксплуатационная и техническая документация к средствам защиты информации пересылается заказными, ценными почтовыми отправлениями или доставляется специально выделенными сотрудники.

При пересылке средств защиты информации, 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.

Отправитель контролирует доставку своих отправлений адресатам. Если от адресата своевременно не поступило соответствующего подтверждения, то отправитель направляет ему запрос и принимает меры к уточнению местонахождения отправлений.

19.3. 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 средства защиты информации до получения указаний от отправителя применять не разрешается.

При обнаружении бракованных средств защиты информации 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 средств защиты информации, эксплуатационной и технической документации к ним подтверждается отправителю в соответствии с порядком, указанным в сопроводительном письме.

19.4. Средства защиты информации уничтожаются (утилизируются) по решению руководителя.

Намеченные к уничтожению (утилизации) средства защиты информации изымаются из аппаратных средств, с которыми они функционировали. При этом средства защиты информации считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к средствам защиты информации процедура удаления программного обеспечения средств защиты информации и они полностью отсоединены от аппаратных средств.

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

Уничтожение большого объема инсталлирующих средств защиты информации носителей оформляется актом. Уничтожение по акту производится

комиссией в составе не менее трех человек из числа лиц, допущенных к работе со средствами защиты информации. 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 средств защиты информации 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.

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

Уничтожение большого объема эксплуатационной и технической документации к средствам защиты информации оформляется актом. Уничтожение по акту производится комиссией в составе не менее трех человек из числа лиц, допущенных к работе со средствами защиты информации. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемой эксплуатационной и технической документации к средствам защиты информации. 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.

19.5. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены средства защиты информации, должны обеспечивать сохранность персональных данных, средств защиты информации, исключать возможность неконтролируемого проникновения или пребывания в помещениях, где установлены средства защиты информации, посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

При оборудовании помещений, где установлены средства защиты информации, должны выполняться требования к размещению и монтажу средств защиты информации, а также другого оборудования, функционирующего со средствами защиты информации.

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

Помещения, где установлены средства защиты информации, должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

Для предотвращения просмотра извне помещений, где установлены средства защиты информации, их окна должны быть оборудованы шторами или жалюзи.

19.6. Контроль за организацией и обеспечением функционирования средств защиты информации возлагается на администратора информационной безопасности в пределах его полномочий.

Пользователи ИС несут персональную ответственность за сохранность полученных средств защиты информации, эксплуатационной и технической документации к средствам защиты информации, за соблюдение положений настоящего положения.

Администратор информационной безопасности несет ответственность за соответствие проводимых им мероприятий по организации и обеспечению безопасности обработки персональных данных с использованием средств защиты информации лицензионным требованиям и условиям, эксплуатационной и технической документации к средствам защиты информации.

Часть 20. Порядок обеспечения информационной безопасности ИС при модернизации (обновлении) аппаратных и программных компонентов

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

1) нарушения штатной работы информационных ресурсов и сервисов ИС;

2) нарушения штатного функционирования оборудования;

3) несанкционированной модификации;

4) несанкционированного копирования.

20.2. Ответственность за невыполнение требований настоящей части, проведение в плановом порядке работ по обновлению оборудования, операционной системы, программного обеспечения в целях своевременной ликвидации выявленных уязвимостей программного обеспечения в информационной инфраструктуре, за отслеживание появления новых уязвимостей в используемых операционных систем, за установку патчей, устраняющих данные уязвимости, за тестирование ИС при внесении изменений и дополнений в программное обеспечение и оборудование на отсутствие негативных воздействий на функционирование ИС, ответственность за мониторинг событий, фиксируемых системами безопасности, несет администратор информационной безопасности.

20.3. Установке нового оборудования предшествует тестирование инфраструктуры ИС и критических приложений на отсутствие негативных воздействий вновь устанавливаемого оборудования.

Установке обновлений предшествует тестирование информационной инфраструктуры ИС на отсутствие негативных воздействий от вновь устанавливаемых обновлений.

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

Установке новых версий программного обеспечения или внесению изменений и дополнений в действующее программное обеспечение предшествует тестирование информационной инфраструктуры ИС на отсутствие негативных воздействий устанавливаемого программного обеспечения.

Установка протестированного оборудования и (или) патчей, новых версий программного обеспечения или внесение изменений и дополнений в действующее программное обеспечение, применение организационно-технических и (или) аппаратно-программных решений может быть произведено на основании решения администратора информационной безопасности.

Тестирование нового оборудования и обновлений программного обеспечения не должно осуществляться на ресурсах действующей информационной инфраструктуры ИС.

Часть 21. Управление конфигурацией ИС и ее системы защиты

21.1. Администратор информационной безопасности организует управление конфигурацией ИС и ее системы защиты информации в соответствии с требованиями настоящей части.

21.2. Под конфигурацией ИС и ее системы защиты информации понимается совокупность следующих характеристик:

1) состав программного и аппаратного обеспечения ИС;

2) места размещения технических средств ИС;

3) параметры настройки программного обеспечения и технических средств ИС;

4) структура системы защиты информации;

5) состав, места установки и параметры настройки средств защиты информации.

21.3. Администратор информационной безопасности организует проверку текущей конфигурации ИС и ее системы защиты на соответствие базовой конфигурации. Результат проверки оформляется актом контроля текущей конфигурации (приложение № 17).

21.4. Внесение изменений в конфигурацию ИС и ее системы защиты осуществляется по согласованию с администратором информационной безопасности с обязательной отметкой в журнале регистрации действий по сопровождению информационных систем и изменению их конфигураций, форма которого приведена в приложении № 18.

В случае внесения изменений в конфигурацию аттестованной по требованиям защиты информации ИС и ее системы защиты может возникнуть необходимость согласования изменений с соответствующей организацией-лицензиатом ФСТЭК России.

21.5. Требования настоящей части направлены предотвращение:

1) нарушения штатной работы информационных ресурсов и сервисов ИС;

2) нарушения штатного функционирования оборудования;

3) несанкционированного уничтожения защищаемой информации;

4) несанкционированной модификации защищаемой информации;

5) несанкционированного копирования защищаемой информации.

21.6. Установке нового оборудования предшествует тестирование инфраструктуры ИС и критических приложений на отсутствие негативных воздействий вновь устанавливаемого оборудования.

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

21.7. Установке обновлений программного обеспечения, новых версий программного обеспечения и дополнений в действующее программное обеспечение предшествует тестирование информационной инфраструктуры ИС на отсутствие негативных воздействий от вновь устанавливаемого программного обеспечения (обновлений программного обеспечения).

При обнаружении негативного воздействия устанавливаемого программного обеспечения (обновлений программного обеспечения) на инфраструктуру ИС, функционирующую в штатном режиме, такое программное обеспечение (обновление программного обеспечения) не устанавливается. В этом случае разрабатывается план дополнительных мероприятий, направленных на устранение негативного воздействия устанавливаемого программного обеспечения ПО (обновления программного обеспечения).

Тестирование нового оборудования и обновлений программного обеспечения не должно осуществляться на ресурсах действующей информационной инфраструктуры ИС.

Конфигурация ИС и ее системы защиты фиксируется в эксплуатационной документации ИС. Актуализация эксплуатационной документации осуществляется администратором информационной безопасности по факту принятия решения о внесении соответствующих изменений.

Часть 22. Анализ защищенности информации при ее обработке в ИС

22.1. Администратор информационной безопасности должен ежемесячно осуществлять тестирование работоспособности средств защиты информации штатными средствами с отметкой в журнале учета периодического тестирования средств защиты информации информационных систем, форма которого приведена в приложении № 12.

22.2. Администратор информационной безопасности несет ответственность за анализ защищенности информации при ее обработке в ИС, в том числе:

1) за отслеживание появления новых уязвимостей программного обеспечения и оборудования, используемых в составе ИС;

2) за проведение в плановом порядке работ по обновлению оборудования, общесистемного и прикладного программного обеспечения, программного обеспечения средств защиты информации в целях своевременной ликвидации выявленных уязвимостей;

3) за предварительное тестирование ИС при внесении изменений и дополнений в программное обеспечение и оборудование на отсутствие негативных воздействий на функционирование ИС (в соответствии с требованиями части 21 настоящего положения;

4) за мониторинг событий, фиксируемых средствами защиты информации.

Часть 23. Выявление инцидентов безопасности и реагирование на них

23.1. Инциденты безопасности – непредвиденные или нежелательные события, которые могут нарушить работоспособность ИС или безопасность защищаемой информации:

1) отказ в обслуживании;

2) длительные нарушения в работе технических средств, программного обеспечения и (или) средств защиты информации;

3) нарушение правил разграничения доступа;

4) неправомерные действия по сбору информации;

5) внедрение вредоносных компьютерных программ (вирусов);

6) выявление признаков инцидентов безопасности при анализе журналов событий;

7) иные события, приводящих к реализации угроз информационной безопасности.

23.2. Источниками информации об инцидентах безопасности для ИС являются:

1) факты, выявленные работниками Администрации Сысертского городского округа;

2) результаты работы средств мониторинга информационной безопасности, аудита (внутреннего или внешнего);

3) журналы и оповещения операционных систем серверов/АРМ/ операционных систем/гостевых операционных систем, антивирусной системы, системы резервного копирования и других подсистем безопасности;

4) обращения субъектов персональных данных с указанием инцидента безопасности;

5) сообщения Федеральной службы технического и экспортного контроля Российской Федерации;

6) сообщения Федеральной службы безопасности Российской Федерации;

7) сообщения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций;

8) иные источники информации.

23.3. Основные виды инцидентов безопасности:

1) несанкционированный доступ к информационным ресурсам ИС;

2) разглашение защищаемой информации либо угроза такого разглашения;

3) превышение полномочий – несанкционированный доступ к каким-либо ресурсам и помещениям;

4) компрометация учетных записей или паролей;

5) вирусная атака или вирусное заражение;

6) сетевые атаки (отказ в обслуживании), атаки типа Man-in-the-Middle, сниффер пакетов, переадресация портов, IP-спуфинг, атаки на уровне приложений и другое.

23.4. Выявление инцидентов безопасности и реагирование на них включает в себя следующие мероприятия:

1) регламентация правил и процедур реагирования на инциденты безопасности, в том числе определение лиц, ответственных за выявление инцидентов и реагирование на них;

2) обнаружение, идентификация и регистрация инцидентов безопасности;

3) своевременное информирование лиц, ответственных за выявление инцидентов безопасности и реагирование на них, о возникновении инцидентов безопасности;

4) анализ инцидентов безопасности, в том числе определение источников и причин возникновения инцидентов безопасности, а также оценка их последствий;

5) принятие мер по устранению последствий инцидентов безопасности;

6) планирование и принятие мер по предотвращению повторного возникновения инцидента безопасности;

7) хранение и защита информации об инцидентах безопасности.

23.5. Обнаружение инцидентов безопасности включает в себя мероприятия, направленные на:

1) выявление инцидентов безопасности с помощью технических средств;

2) выявление инцидентов безопасности в ходе контрольных мероприятий.

23.6. При получении информации о несанкционированном воздействии на инфраструктуру ИС администратор информационной безопасности обязан убедиться, что инцидент безопасности не является результатом собственной ошибки или санкционированных действий.

23.7. Лицо, обнаружившее инцидент, должно незамедлительно, любым доступным способом, сообщить об инциденте администратору информационной безопасности, который принимает решение о необходимости информирования пользователей ИС о возникновении инцидента безопасности и дает указания по дальнейшим действиям.

23.8. Администратор информационной безопасности учитывает инциденты безопасности в журнале учета нештатных ситуаций в информационных системах, форма которого приведена в приложении № 9 к настоящему положению, информирует об инциденте специалиста/подразделение по защите информации, ответственного за защиту информации, а также при необходимости другие структурные подразделения.

23.9. Перечень действий при реагировании на инциденты безопасности, реализуемые администратором информационной безопасности совместно со специалистом/подразделением, ответственным за защиту информации:

1) принятие мер по устранению инцидентов безопасности;

2) анализ инцидентов безопасности, в том числе определение источников и причин возникновения инцидентов безопасности, а также оценка их последствий;

3) планирование и принятие мер по предотвращению повторного возникновения инцидентов безопасности.

23.10. Планирование и принятие мер по предотвращению возникновения инцидентов безопасности осуществляется администратором информационной безопасности и основывается на:

1) планомерной деятельности по повышению уровня осознания информационной безопасности руководством и работниками Администрации Сысертского городского округа;

2) проведении мероприятий по обучению работниками Администрации Сысертского городского округа правилам и способам работы со средствами защиты;

3) доведении до работников Администрации Сысертского городского округа норм законодательства, локальных актов по вопросам информационной безопасности и устанавливающих ответственность за нарушение требований информационной безопасности;

4) разъяснительной работе с лицами, принимаемыми на работу, и увольняющимися работниками;

5) своевременной модернизации системы обеспечения информационной безопасности с учетом возникновения новых угроз информационной безопасности и при изменении требований законодательных актов и нормативных документов по защите информации;

6) своевременном обновлении программного обеспечения, в том числе программного обеспечения средств защиты информации и средств криптографической защиты информации.

Часть 24. Правила и процедуры информирования и обучения персонала

24.1. Цель обучения персонала – формирование и поддержание необходимого уровня квалификации работников Администрации Сысертского городского округа с учетом требований в сфере информационной безопасности и обеспечения требуемого уровня защищенности информации в ИС.

24.2. Задачи в области обучения вопросам информационной безопасности:

1) выработка и соблюдение правил по защите информации в ИС;

2) разработка и внедрение системы обучения, включающей выявление потребности в обучении, планирование и бюджетирование, организацию обучения и контроль его результативности;

3) включение передового опыта, знаний, эффективных методов организации труда в процессе обучения сотрудников вопросам информационной безопасности;

4) мотивация работников к повышению безопасности и обеспечению надежности работы;

5) регулярная проверка знаний в сфере информационной безопасности и их применение на практике.

24.3. По формам планирования, организации обучения и проверки знаний подразделяются на плановые и внеплановые:

1) плановые – проводятся по программам обучения:

а) вводный инструктаж: проводится при поступлении лица на работу в Администрации Сысертского городского округа;

б) первичный инструктаж на рабочем месте: проводится при выполнении работ, к которым предъявляются дополнительные (повышенные) требования по информационной безопасности;

в) первичная проверка знаний: проводится не позднее трех месяцев после назначения на должность;

г) повторное обучение: проводится для работников Администрации Сысертского городского округа, выполняющих работы, к которым предъявляются дополнительные (повышенные) требования по информационной безопасности, проводится один раз в три года;

2) внеплановые – проводятся по производственной необходимости, а также по заявкам руководителей структурных подразделений. Форма заявки приведена в приложении № 19 к настоящему положению:

а) внеочередное обучение: проводится при изменении требований по информационной безопасности, изменениях в бизнес-процессах или при нарушениях информационной безопасности;

б) внеплановая проверка знаний: проводится при изменении требований к информационной безопасности, изменениях в бизнес-процессах или при нарушениях информационной безопасности, проводится не реже одного раза в три года;

в) целевое обучение: проводится при выполнении разовых работ, не связанных с прямыми обязанностями работников;

г) специальное обучение: проводится при выполнении работ, к которым предъявляются дополнительные (повышенные) требования по информационной безопасности.

24.4. По формам проведения обучение и проверки знаний подразделяются на индивидуальные и корпоративные (групповые), внутренние и внешние:

1) индивидуальное обучение: проводится с работником Администрации Сысертского городского округа персонально;

2) корпоративное (групповое): организация групп или обучение одновременно нескольких работников одного подразделения;

3) внешнее: проводится с привлечением внешних образовательных организаций.

24.5. В ходе информирования и обучения персонала осуществляется:

1) информирование персонала об угрозах безопасности информации, о правилах безопасной эксплуатации ИС;

2) доведение до персонала требований по обеспечению безопасности ИС, а также положений организационно-распорядительных документов по информационной безопасности в части, их касающейся;

3) обучение персонала правилам эксплуатации отдельных средств защиты информации, включая проведение практических занятий с персоналом;

4) контроль осведомленности персонала об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения безопасности.

24.6. Обучение и проверка знаний в порядке, установленном настоящим положением, распространяется на руководителей и работников структурных подразделений, которые:

1) осуществляют эксплуатацию ИС;

2) обеспечивающие функционирование (сопровождение, обслуживание, ремонт) технических и программных компонентов ИС;

3) временных сотрудников;

4) работников, выполняющих работы, к которым предъявляются дополнительные (повышенные) требования по информационной безопасности.

24.7. Ответственность за организацию своевременного и качественного обучения и проверки знаний по информационной безопасности возлагается на администратора информационной безопасности.

24.8. Обучение и инструктаж по информационной безопасности должен проводиться в рабочее время.

24.9. Внеочередное обучение и проверка знаний по информационной безопасности руководителей и работников проводится независимо от срока проведения предыдущего обучения и проверки в следующих случаях:

1) при введении в действие новых нормативных документов по информационной безопасности или вступления в законную силу изменений в нормативные документы по информационной безопасности;

2) при изменениях технологических процессов и замене оборудования, требующих дополнительных знаний по информационной безопасности обслуживающего персонала;

3) при назначении или переводе на другую работу, если новые обязанности требуют от руководителей и работников дополнительных знаний по информационной безопасности (до начала исполнения своих обязанностей);

4) по требованию руководителей подразделений при установлении недостаточных знаний;

5) после наступления инцидентов безопасности, нештатных ситуаций, при повышении вероятности осуществления потенциальными нарушителями угроз информационной безопасности;

6) при совершенных нарушениях требований нормативных документов по информационной безопасности руководителями и работниками Администрации Сысертского городского округа;

7) при возникновении перерыва в работе в данной должности более одного года.

24.10. Непосредственно перед очередной (внеочередной) проверкой знаний по информационной безопасности руководителей и работников Администрации Сысертского городского округа могут проводиться:

1) специальная подготовка с целью углубления знаний по наиболее важным вопросам информационной безопасности;

2) семинары;

3) консультации.

24.11. О дате и месте проведения проверки знаний работник должен быть предупрежден не позднее чем за 15 рабочих дней.

24.12. Для проведения проверки знаний по информационной безопасности муниципальным правовым актом создаются комиссии по проверке знаний. Состав, порядок и форма работы комиссий по проверке знаний определяется Администрации Сысертского городского округа.

24.13. Факт проведения обучения, проверки знаний фиксируются в журнале проведения обучения и проверки знаний по вопросам информационной безопасности, форма которого приведена в приложении № 20 к настоящему положению.

24.14. Внешнее обучение по вопросам информационной безопасности руководителей и работников проводится по программам, разработанным и утвержденным учебными центрами, организациями, институтами, имеющими лицензии на обучение в данной сфере знаний.

Часть 25. Правила и процедуры планирования мероприятий по обеспечению безопасности

25.1. Основными целями планирования мероприятий по защите информации в ИС являются:

1) организация проведения комплекса мероприятий по обеспечению безопасности защищаемой информации, направленных на исключение возможных каналов утечки информации;

2) установление персональной ответственности должностных лиц за решение вопросов защиты информации в ходе эксплуатации ИС;

3) определение сроков (времени, периода) проведения конкретных мероприятий по защите информации;

4) систематизация (объединение) всех проводимых на плановой основе мероприятий по различным направлениям защиты информации;

5) установление системы контроля за обеспечением защиты информации в ИС, а также системы отчетности о выполнении конкретных мероприятий;

6) уточнение, конкретизация функций и задач, решаемых отдельными должностными лицами и/или структурными подразделениями.

25.2. Подтверждением проведения контрольных мероприятий является:

1) меры, средства и мероприятия, проводимые в целях защиты информации, обеспечивают поддержание уровня защищенности информации в ИС;

2) система защиты информации обеспечивает защиту информации при эксплуатации ИС;

3) средства защиты информации настроены и используются в соответствии с техническими условиями, правилами эксплуатации и требованиями формуляров;

4) рекомендации предшествующих проверок реализованы в полной мере.

25.3. Контрольные мероприятия (проверки) проводятся Администрацией Сысертского городского округа на плановой основе, а также внепланово. Внеплановые проверки проводятся по фактам выявления работниками Администрации Сысертского городского округа нарушений функционирования элементов ИС и инцидентов информационной безопасности, при существенных изменениях в среде обработки защищаемой информации.

25.4. Плановые проверки проводятся на периодичной основе и включают:

1) проверку актуальности нормативных и организационных документов;

2) проверку работоспособности и эффективности технических средств ИС;

3) проверку соответствия предъявляемых мер защиты к предъявляемым характеристикам ИС по требованиям безопасности информации (уровню защищенности информации в ИС);

4) проверку деятельности работников Администрации Сысертского городского округа, эксплуатирующих ИС, на соответствие требованиям к обеспечению безопасности ИС;

5) проверку компетентности персонала, задействованного в обслуживании системы защиты ИС;

6) проверку управления инцидентами в ИС;

7) контроль модернизации системы безопасности ИС;

8) контроль обеспечения бесперебойной эксплуатации ИС.

25.5. Для проведения контрольных мероприятий администратор информационной безопасности разрабатывает ежегодный план мероприятий по обеспечению безопасности ИС и представляет его на утверждение Главе Сысертского городского округа (далее – план мероприятий). План мероприятий может быть включен в сводный план мероприятий по обеспечению безопасности, утверждаемый Администрацией Сысертского городского округа.

25.6. План мероприятий должен содержать:

1) перечень мероприятий по обеспечению безопасности;

2) сроки проведения мероприятий;

3) состав подразделений (работников), ответственных за реализацию каждого мероприятия.

25.7. Контроль за выполнением плана мероприятий осуществляется структурным подразделением, ответственным за защиту информации, которое ежегодно готовит отчет о выполнении плана мероприятий, который представляется Главе Сысертского городского округа.

25.8. Контроль состояния безопасности проводится ежегодно. Различают внешний и внутренний контроль состояния безопасности. Внутренний контроль включает плановые и внеплановые проверки, указанные выше.

Внутренний контроль проводится комиссией, назначаемой Главой Сысертского городского округа. В состав комиссии входят: администратор информационной безопасности; работники подразделения, ответственного за обеспечение безопасности; а также работники иных заинтересованных подразделений. Результат внутреннего контроля оформляется протоколом, который подписывается членами комиссии и утверждается Главой Сысертского городского округа (приложение № 21).

Внешний контроль (аудит) проводится внешней организацией, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

25.9. Факты проведения плановых или внеплановых контрольных мероприятий Администрации Сысертского городского округа фиксируются в журнале учета проведения внутреннего контроля за обеспечением уровня защищенности информации (приложение № 13).

25.10. По итогам проведения контрольных мероприятий администратор информационной безопасности разрабатывает отчет, в котором указывается:

1) описание проведенных мероприятий по каждому из этапов;

2) перечень и описание выявленных нарушений;

3) рекомендации по устранению выявленных нарушений;

4) заключение по итогам проведения контрольного мероприятия.

25.11. Должностные лица, ответственные за организацию работ по защите информации и непосредственное выполнение указанных работ назначаются муниципальными правовыми актами Оператора.

Лица, виновные в нарушении норм законодательства в сфере обеспечения защиты информации, требований настоящего положения, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, предусмотренном законодательством Российской Федерации.

Приложение № 1
к Положению об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Форма

Журнал учета пользователей, имеющих право доступа к информационным системам

№ п/п	Дата	Ф.И.О. пользователя	Подпись пользователя информационной системы о прохождении первичного инструктажа, об ознакомлении с положениями о порядке защиты информации	Ф.И.О. и подпись администратора информационной безопасности	Примечание
1.					
2.					
3.					
4.					
5.					
6.					
7.					

Приложение № 2
к Положению об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Форма

УТВЕРЖДАЮ

_____
(должность) (подпись) (инициалы и фамилия)

«_____» _____ года
М.П.

Акт об уничтожении защищаемой информации

№ _____ «___» _____ _____ года

Комиссия в составе:
- председатель комиссии - _____
(должность, фамилия, имя, отчество)
- секретарь комиссии - _____
(должность, фамилия, имя, отчество)
- члены комиссии: _____
(должность, фамилия, имя, отчество)
_____
(должность, фамилия, имя, отчество)
_____
(должность, фамилия, имя, отчество)

провела отбор машинных носителей информации и установила, что в соответствии с требованиями с действующего законодательством Российской Федерации информация, записанная на них в процессе эксплуатации, подлежит гарантированному уничтожению, и составила настоящий акт о том, что произведено уничтожение персональных данных:

№ п/п	Дата	Тип носителя	Учетный номер машинного носителя информации	Категория информации	Примечание

Всего машинных носителей информации _____.
(количество цифрами и прописью)

На указанных носителях информация уничтожена путем _____
_____.
(способ уничтожения персональных данных)

Председатель комиссии _____ _____
(подпись) (инициалы и фамилия)

Секретарь комиссии _____ _____
(подпись) (инициалы и фамилия)

Члены комиссии: _____ _____
(подпись) (инициалы и фамилия)

_____ _____
(подпись) (инициалы и фамилия)

_____ _____
(подпись) (инициалы и фамилия)

Приложение № 3
к Положению об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Форма

УТВЕРЖДАЮ

_____
(должность) (подпись) (инициалы и фамилия)

«_____» _____ года
М.П.

Акт об уничтожении машинных носителей информации

№ _____ «___» _____ _____ года

Комиссия в составе:
- председатель комиссии - _____
(должность, фамилия, имя, отчество)
- секретарь комиссии - _____
(должность, фамилия, имя, отчество)
- члены комиссии: _____
(должность, фамилия, имя, отчество)
_____
(должность, фамилия, имя, отчество)
_____
(должность, фамилия, имя, отчество)

провела отбор машинных носителей информации и установила, что в соответствии с требованиями с действующего законодательством Российской Федерации информация, записанная на них в процессе эксплуатации, подлежит гарантированному уничтожению, и составила настоящий акт о том, что произведено уничтожение машинных носителей информации:

№ п/п	Дата	Тип носителя	Учетный номер машинного носителя информации	Категория информации	Примечание

Всего машинных носителей информации _____.
(количество цифрами и прописью)

На указанных носителях информация уничтожена путем _____
_____.
(способ уничтожения машинных носителей информации)

Председатель комиссии _____ _____
(подпись) (инициалы и фамилия)

Секретарь комиссии _____ _____
(подпись) (инициалы и фамилия)

Члены комиссии: _____ _____
(подпись) (инициалы и фамилия)

_____ _____
(подпись) (инициалы и фамилия)

_____ _____
(подпись) (инициалы и фамилия)

Приложение № 4
к Положению об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Форма

Заявка на предоставление пользователю прав доступа к информационной системе (ИС) / информационной системе персональных данных (ИСПДн) (ресурсу ИС/ИСПДн)

_____

(наименованиеИС/ ИСПДн или ресурса ИС/ ИСПДн)

№ п/п	Ф.И.О., № кабинета	Должность	Имя АРМ в домене	Права доступа к ИС/ИСПДн (ресурсу ИС/ИСПДн)			Время доступа к ИС/ИСПДн (ресурсу ИС/ИСПДн)	
				чтение	редактирование	удаление	дни недели	рабочие часы

Руководитель структурного подразделения _____ _____

(подпись) (инициалы и фамилия)

« ____ » _____ 20__ года

Приложение № 5
к Положению об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Форма

Журнал учета антивирусных проверок информационных систем

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

Приложение № 6
к Положению об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Форма

Журнал учета антивирусных проверок информационных систем

№ п/п	Дата и время проверки	Имя технического средства	Наименование события	Примечание (принятые меры)
1.				
2.				
3.				
4.				
5.				

Приложение № 7
к Положению об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Форма

Журнал учета машинных носителей информации

№ п/п	Регистрационный (учетный, серийный) номер машинного носителя информации	Тип, емкость машинного носителя информации	Дата поступления машинного носителя информации	Расписка в получении машинного носителя информации администратором информационной безопасности (Ф.И.О., подпись, дата)	Дата и место установки/ передачи работнику машинного носителя информации	Ф.И.О., подпись лица, установившего/ получившего машинный носитель информации	Расписка в обратном приеме машинного носителя информации (Ф.И.О., подпись, дата)	Дата, номер акта об уничтожении машинного носителя информации	Примечание
1.									
2.									
3.									
4.									
5.									

Приложение № 8
к Положению об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Форма

Журнал резервного копирования информационных массивов информационных систем

№ п/п	Дата проведения резервного копирования	Наименование информационного массива информационной системы	Регистрационный (учетный, серийный) номер машинного носителя информации	Тип носителя	Ф.И.О. и подпись администратора информационной безопасности	Примечание
1.						
2.						
3.						
4.						
5.						

Приложение № 9
к Положению об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Форма

Журнал учета нештатных ситуаций в информационных системах

№ п/п	Дата	Наименование и серийный номер технического средства	Краткое описание нештатной ситуации	Ф.И.О. и подпись администратора информационной безопасности	Примечание
1.					
2.					
3.					
4.					
5.					

Приложение № 10
к Положению об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Форма

Журнал проверки электронных журналов информационных систем

№ 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.						

Приложение № 11
к Положению об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Форма

Журнал поэкземплярного учета средств защиты информации информационных систем, 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.							

Приложение № 12
к Положению об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Форма

Журнал учета периодического тестирования средств защиты информации информационных систем

№ 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.							

Приложение № 13
к Положению об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Форма

Журнал учета проведения внутреннего контроля за обеспечением уровня защищенности информации

№ 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.					

Приложение № 14
к Положению об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Форма

Акт установки средства защиты информации

№ _____ «___» _____ _____ года

Рабочая группа в составе:

- _____
(должность) (фамилия, имя, отчество)
- _____
(должность) (фамилия, имя, отчество)
- _____
(должность) (фамилия, имя, отчество)

составила настоящий акт о том, что на основании заявки/служебной записки от _____ № _____ 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

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

№ п/п	Вид оборудования	Тип	Учетный (заводской) номер
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.	*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*

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 _____ _____
(подпись) (инициалы и фамилия)

Пользователь СЗИ _____ _____
(подпись) (инициалы и фамилия)

Приложение № 15
к Положению об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Форма

Заявка на деинсталляцию средства защиты информации

Прошу деинсталлировать средство защиты информации _____
_____
(наименование средства защиты информации)
_____
с технических средств и систем, приведенных в таблице, и находящихся в пользовании
_____
(должность, фамилия, имя, отчество пользователя СЗИ)
в связи с _____.
(причина деинсталляции средства защиты информации)

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

№ п/п	Вид оборудования	Тип	Учетный (заводской) номер
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*		

(должность) _____ (подпись) _____ (инициалы и фамилия)

Приложение № 16
к Положению об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Форма

Акт деинсталляции средства защиты информации

№ _____ «___» _____ _____ года

Рабочая группа в составе:

- _____
(должность) _____ (фамилия, имя, отчество)

- _____
(должность) (фамилия, имя, отчество)

- _____
(должность) (фамилия, имя, отчество)

составила настоящий акт о том, что на основании заявки/служебной записки от _____ № _____ с технических средств и систем, приведенных в таблице, и находящихся в пользовании _____

_____
(должность, фамилия, имя, отчество пользователя СЗИ)

произведена деинсталляция средства защиты информации (далее – СЗИ) _____

_____
(наименование, версия СЗИ)

следующим способом[1]: _____.

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

№ п/п	Вид оборудования	Тип	Учетный (заводской) номер
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 _____ _____
(подпись) (инициалы и фамилия)

Пользователь СЗИ _____ _____
(подпись) (инициалы и фамилия)

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

Приложение № 17
к Положению об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Форма

Акт контроля текущей конфигурации ИС _____ и ее средств защиты информации

№ _____ «___» _____ _____ года

1. Отклонения в составе ИС: _____
_____
_____
_____

2. Отклонения в составе системы защиты информации: _____
_____
_____
_____

3. Отклонения в подключениях технических средств ИС и системы защиты информации: _____
_____
_____
_____

4. Отклонения в составе программного обеспечения: _____
_____
_____
_____

5. Отклонения в технологии обработки информации: _____
_____
_____
_____

6. Выводы: _____
_____
_____
_____
_____

_____	_____	_____
(должность)	(подпись)	(инициалы и фамилия)

Приложение № 18
к Положению об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Форма

Журнал учета регистрации действий по сопровождению информационных систем и изменению их конфигураций

№ п/п	Дата и номер заявки на внесение изменений	Дата сопровождения/ внесения изменений	Описание выполненных действий	Ф.И.О. и подпись ответственного лица	Дата и номер акта контроля текущей конфигурации и ее средств защиты информации
1.					
2.					
3.					
4.					
5.					

Приложение № 19
к Положению об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Форма

Заявка на проведение обучения по вопросам информационной безопасности

Подразделение	
Должность	
Фамилия, имя, отчество	
Номер служебного телефона	
Номер кабинета	

Провести обучение по следующим темам:

Тема	Дата

Привлечь специалистов для обучения по следующим темам:

Тема	Дата

Провести обучение во внешних организациях по следующим темам:

Тема	Дата

(должность) _____ (подпись) _____ (инициалы и фамилия)

Приложение № 20
к Положению об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Форма

Журнал проведения обучения и проверки знаний по вопросам информационной безопасности

№ п/п	Дата	Вид - обучение/ проверка знаний	Причина проведения обучения/проверки знаний	Ф И.О., подпись обученного/проверенного	Ф.И.О., подпись обучающего/проверяющего/название образовательной организации
1.					
2.					
3.					
4.					
5.					

Приложение № 21
к Положению об организации и проведении работ по обеспечению безопасности защищаемой информации при ее обработке в Администрации Сысертского городского округа

Форма

УТВЕРЖДАЮ

_____
(должность) (подпись) (инициалы и фамилия)
«_____» _____ года
М.П.

Протокол проведения внутреннего контроля за обеспечением уровня защищенности информации

№ _____ «___» _____ _____ года

Комиссия в составе:
- председатель комиссии - _____
(должность, фамилия, имя, отчество)
- члены комиссии: _____
(должность, фамилия, имя, отчество)
_____
(должность, фамилия, имя, отчество)

проведена проверка _____
(тема проверки)
_____.

Проверка осуществлялась в соответствии с требованиями _____
_____.
(название документа)

В ходе проверки установлено: _____
_____.

Выявленные нарушения: _____
_____.

Меры по устранению нарушений: _____
_____.

Срок устранения нарушений: _____.

Председатель комиссии _____ _____
(подпись) (инициалы и фамилия)

Члены комиссии: _____ _____
(подпись) (инициалы и фамилия)
_____ _____
(подпись) (инициалы и фамилия)