Содержание

Список сокращений и обозначений

ИС	Информационная система
БД	База данных
НСД	Несанкционированный доступ
ОС	Операционная система
ПО	Программное обеспечение
АРМ	Автоматизированное рабочее место
СЗИ	Средство защиты информации
ТС	Техническое средство

1. Нормативно-методическое обеспечение

Настоящее Положение по организации и проведению работ по обеспечению безопасности информации, не составляющей государственную тайну, содержащейся в государственных информационныхсистемах (далее – Положение) разработано на основании:

[1] - Федерального закона Российской Федерации (далее – РФ) от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

[2] - Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении требований к защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

[3] - «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденные приказом Гостехкомиссией России от 30 августа 2002 г. № 282;

[4] - Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденный решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

2. Общие положения

Настоящее Положение определяет порядок и правила организации и проведения работ по обеспечению безопасности информации, не составляющей государственную тайну, содержащейся в государственных информационных системах(далее – информация).

Положение разработано с целью

– организации и координации работ по защите информации, обрабатываемой в информационных системах, взаимодействующих с федеральными государственными информационными системами и с государственными информационными системами Свердловской области (далее - ИС);

– регламентации порядка проведения работ по обеспечению безопасности информации и ИС;

– контроля состояния защиты информации и ИС.

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

3. Администратор информационной безопасности

3.1. Функции администратора информационной безопасности

Администратор информационной безопасности осуществляет следующие мероприятия, направленные на обеспечение безопасности информации и ИС.

1. Настройка и сопровождение системы защиты ИС:

- реализует полномочия доступа для каждого пользователя ИС на основе утвержденного главой городского округа Богданович, перечня сотрудников, имеющих доступ к информации, обрабатываемой в ИС;
- своевременно удаляет учетные записи пользователей из ИС при увольнении или перемещении сотрудника;
- своевременно блокирует и разблокирует учетные записи пользователей ИС при их уходе на больничный или в отпуск и при выходе с больничного или из отпуска;
- периодически, но не реже одного раза в квартал, контролирует смену паролей пользователями для доступа в ИС;
- регистрирует новых пользователей ИС;
- регистрирует СЗИ;
- периодически, но не реже одного раза в месяц, выполняет мероприятия по периодическому тестированию функционирования СЗИ в соответствии с документацией разработчика данных средств, регистрируя проведение данных мероприятий.

2. Настройка и сопровождение подсистемы регистрации и учета ИС:

- проводит регулярный анализ системного журнала ИС для выявления попыток НСД к защищаемым ресурсам с соответствующей регистрацией проверки;
- своевременно информирует руководство о несанкционированных действиях персонала и участвует в разбирательствах по фактам попыток НСД;
- проводит резервное копирования информационных массивов ИС.

3. Сопровождение подсистемы обеспечения целостности ИС:

- осуществляет учет возникновения нештатных ситуаций;
- осуществляет восстановление ИС при возникновении сбоев.

4. Контроль функционирования подсистемы антивирусной защиты ИС:

- обеспечивает поддержание установленного порядка и соблюдение правил антивирусной защиты;
- периодически, но не реже одного раза в неделю, проводит антивирусные проверки всех жестких дисков автоматизированных рабочих мест (далее – АРМ) пользователей ИС;
- регистрирует результаты антивирусных проверок.

5. Контроль использования машинных носителей информации и ведение их учета.

6. Сопровождение подсистемы межсетевого экранирования ИС.

7. Сопровождение подсистемы обнаружения вторжений ИС.

8. Организация обновлений программного обеспечения (далее – ПО) и средств защиты, выполнение профилактических работ, установки и модификации программных средств на АРМ пользователей ИС.

9. Проведение модернизации аппаратных компонентов.

10. Проведение инструктажа сотрудников, имеющих право доступа к ИС.

11. Осуществление контроля за соблюдением пользователями ИС требований к защите информации.

12. Участие в анализе ситуаций, касающихся функционирования СЗИ и расследования фактов НСД.

13. Оказание методической помощи по вопросам обеспечения безопасности информации, обрабатываемой в ИС, пользователям ИС.

14. Разработка предложений и участие в проводимых работах по совершенствованию системы защиты информации, обрабатываемой в ИС.

3.2. Обязанности администратора информационной безопасности

Администратор информационной безопасности обязан:

– обеспечивать функционирование и поддерживать работоспособность средств защиты АРМ пользователей ИС, в пределах,возложенных на него функций;

– в случае отказа работоспособности ТС и ПО, средств вычислительной техники, в том числе средств защиты ИС, принимать меры по их своевременному восстановлению и выявлению причин, которые вызвали отказ работоспособности;

– информировать руководство о фактах нарушения установленного порядка работ, попытках и фактах НСД к информации, обрабатываемой в ИС.

3.3. Ответственность администратора информационной безопасности

Администратор информационной безопасности несет ответственность за:

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

– совершенные в процессе осуществления своей деятельности правонарушения - в пределах, определенных законодательством РФ;

– невыполнение или ненадлежащее выполнение приказов руководства;

– сохранность информации, обрабатываемой в ИС;

– соблюдение требований нормативных правовых актов и локальных актовадминистрации городского округа Богданович, определяющих порядок организации и проведения работ, направленных на обеспечение безопасности информации, обрабатываемой в ИС;

– сохранность и работоспособное состояние ТС, ПО, средств защиты, входящих в состав ИС;

– выполнение обязанностей, предусмотренных настоящим Положением.

3.4. Права администратора информационной безопасности

Администратор информационной безопасности вправе:

– контролировать работу пользователей ИС;

– требовать прекращение обработки пользователямиИС информации в случае выявления нарушений требований по обработке и обеспечению безопасности информации, обрабатываемой в ИС.

4. Пользователь ИС

4.1. Обязанности пользователя ИС

Пользователем ИС является сотрудник, который в силу своих должностных обязанностей осуществляет обработку информациив ИС и имеет доступ к информационным ресурсам, аппаратным средствам, ПО и средствам защиты ИС.

Пользователь ИС несет персональную ответственность за свои действия.

Пользователь ИС в своей работе руководствуется нормативными правовыми актами в сфере защиты информации и локальными актами администрации городского округа Богданович, определяющих порядок организации и проведения работ, направленных на обеспечение безопасности информации, обрабатываемой в ИС.

Пользователь ИС обязан:

– соблюдать требования нормативных правовых актов в сфере защиты информации и локальных актовадминистрации городского округа Богданович, определяющих порядок организации и проведения работ, направленных на обеспечение безопасности информации, обрабатываемой вИС;

– выполнять на АРМ в отношении информации, обрабатываемой вИС, только те процедуры, которые определены для него в локальных актах администрации городского округа Богданович, определяющих порядок организации и проведения работ, направленных на обеспечение безопасности информации,обрабатываемой вИС;

– в случае временного отсутствия на рабочем месте для предотвращения доступа к информации, находящейся на АРМ, минуя ввод пароля, пользователя 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;

– знать и соблюдать установленные требования по обработке и обеспечению безопасности информации, обрабатываемой вИС;

– соблюдать требования антивирусной защиты в ИС;

– соблюдать требования парольной защиты в ИС;

– соблюдать правила при работе в сетях общего доступа и (или) международного обмена.

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

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

При работе в Сети запрещается:

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

– скачивать из Сети ПО и другие файлы;

– посещение сайтов, непосредственно не связанных с исполнением служебных обязанностей;

– нецелевое использование подключения к Сети.

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

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

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.

Пользователю ИС запрещается:

– разглашать защищаемую информацию третьим лицам;

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

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

– обрабатывать информацию в ИС в условиях, позволяющих осуществлять просмотр такой информации лицами, не имеющими к ним права доступа, а также при несоблюдении требований по обеспечению безопасности информации, обрабатываемой вИС;

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

– самостоятельно вносить изменения в конфигурацию ПО и ТС ИС, изменять установленный алгоритм функционирования технических и программных средств;

– записывать и хранить информацию, обрабатываемую вИС, на неучтенных установленным порядком машинных носителях информации;

– использовать АРМ и другие ресурсы ИС в неслужебных целях;

– подключать к АРМ личные машинные носители информации и мобильные устройства;

– отключать (блокировать) СЗИ;

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

Для получения консультаций по вопросам работы и настройке элементов ИС пользовательИС должен обращаться к администраторуинформационной безопасности.

4.2. Ответственность пользователя ИС

Пользователь ИС несет ответственность за:

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

– совершенные в процессе осуществления своей деятельности правонарушения - в пределах, определенных законодательством РФ;

– невыполнение или ненадлежащее выполнение поручений руководителя;

– сохранность информации, обрабатываемой в ИС;

– соблюдение требований нормативных правовых актов в сфере защиты информации и локальных актовадминистрации городского округа Богданович, определяющих порядок организации и проведения работ, направленных на обеспечение безопасности информации, обрабатываемой в ИС;

– сохранность и работоспособное состояние ТС, ПО, средств защиты, входящих в состав ИС;

– выполнение обязанностей, предусмотренных настоящим Положением.

4.3 Права пользователя ИС

– осуществлять обработкуинформации, обрабатываемой в ИС,в пределах установленных полномочий;

– обращаться к администратору информационнойбезопасности за оказанием технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, ТС ИС, а также с СЗИ.

5. Первичный инструктаж лица, допущенного к работе с ИС

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

Лицо получает непосредственный доступ к ИС только после прохождения первичного инструктажа.

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

Лицо должно быть ознакомлено с локальными актамиадминистрации городского округа Богданович, 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 ИС, должно быть предупреждено:

– об обязанностях выполнения всех правил и требований, предусмотренных локальными актами администрации городского округа Богдановичв области защиты информации;

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

Факт прохождения лицом первичного инструктажа регистрируется администратором информационной безопасности в соответствующем журнале учетапользователей, имеющих право доступа к информационным системам, форма которого приведена в Приложении 1 к настоящему Положению.

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

Помещения, в которых осуществляется обработка информациив ИС, должны располагаться в пределах контролируемой зоны.

Доступ иных лиц в помещенияадминистрации городского округа Богданович, где осуществляется обработка информациив ИС, разрешается только в присутствии лиц, имеющих право доступа в помещение.

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

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

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

Вскрытие и закрытие помещения, в котором ведется обработкаинформациив ИС, производится сотрудникамиадминистрации городского округа Богданович, имеющими право доступа в соответствующее помещение.

Перед закрытием помещений, в которых осуществляется обработкаинформациив ИС, по окончании служебного дня сотрудники, имеющие право доступа к информации, обрабатываемой в ИС и обрабатываемой в соответствующем помещении, обязаны:

– убрать машинные носители, содержащие информациюобрабатываемую в ИС,(диски, флеш-карты) в запираемые шкафы, запереть шкафы на замок;

– отключитьТС (кроме постоянно действующего оборудования) и электроприборы от сети, выключить освещение;

– закрыть окна, двери.

Перед открытием помещений, в которых осуществляется обработкаинформациив ИС, сотрудники обязаны:

– провести внешний осмотр с целью установления целостности двери и замка;

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

При обнаружении неисправности двери и запирающих устройств сотрудники обязаны:

– не вскрывая помещение, в котором осуществляется обработкаинформациив ИС, сообщить об этом руководителю;

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

– составить акт о выявленных нарушениях и передать установленным

порядком руководителю.

При работе с информациейв ИС,двери помещений должны быть всегда закрыты.

Доступ в помещения, где осуществляется обработка информациив ИС, вспомогательного и обслуживающего персонала (уборщиц, электромонтёров, сантехников и других лиц) разрешается только в случае служебной необходимости в сопровождении лица, имеющего право доступа в соответствующее помещение, после принятия мер, исключающих визуальный просмотр документов, содержащих информацию, обрабатываемую в ИС, и экранов мониторов.

Внутренняя планировка и расположение рабочих мест в помещениях, где осуществляется обработкаинформациив ИС, должны исключать визуальный просмотр обрабатываемой в ИС информациидля сотрудников, не осуществляющих обработку таких сведений. Окна помещений, в которых осуществляется обработка информациив ИС, должны быть оборудованы шторами или жалюзи.

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

Ответственность за соблюдение порядка доступа в помещения, в которых осуществляется обработкаинформации в ИС, возлагается на руководителей структурных подразделений, осуществляющих обработку информациив ИС, а также на руководителя администрации городского округа Богданович.

7. Порядок внутреннего контроля за соблюдением требований по обработке и обеспечению безопасности информации

Администрация городского округаБогданович при обработке информациив ИС обязана принимать необходимые правовые, организационные и технические меры для защиты информации, обрабатываемой в ИС,от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.

Внутренний контроль соответствия информации, обрабатываемой в ИС,– это комплекс мероприятий, осуществляемых в целях:

— соблюдения условий и принципов обработки информации, обрабатываемой в ИС;

— соблюдения требований по обработке и обеспечению безопасности обрабатываемой в ИС информации;

— предупреждения и пресечения возможности получения посторонними лицами информации, обрабатываемой в ИС;

— выявления и предотвращения утечки информации, обрабатываемой в ИС,по техническим каналам;

— исключения или затруднения несанкционированного доступа к информации, обрабатываемой в ИС;

— хищения ТС, входящих в состав ИС, и машинных носителей, содержащих информацию;

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

Основными задачами внутреннего контроля являются:

— проверка соответствия локальных актов в области защиты информации действующему законодательству РФ;

—проверка актуальности содержания локальных актов в области обеспечения безопасностиинформации, обрабатываемой в ИС;

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

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

— проверка организации и выполнения мероприятий по защите информации, обрабатываемой в ИС;

— проверка работоспособности применяемых средств защиты информации, обрабатываемой в ИС, в соответствии с их эксплуатационной документацией;

—наличие эксплуатационной документации на технические и программные средства защиты ИС;

— оценка знаний и качества выполнения сотрудникамисвоих функциональных обязанностей в части защиты информации, обрабатываемой в ИС;

— оперативное принятие мер по пресечению нарушений требований по обеспечению безопасности информации, обрабатываемой в ИС.

Внутренний контроль соответствия обработки информации,обрабатываемой в ИС,требованиям к защите информации осуществляется администратороминформационной безопасности ежеквартально. О результатах проверки и мерах, необходимых для устранения выявленных нарушений, администратор информационной безопасности докладывает руководству.

8. Порядок проведения служебнойпроверки по фактам нарушения требований по обеспечению безопасности информации в ИС

8.1. Классификация нарушений требований по обеспечению безопасности информации в ИС

Нарушения требований по обеспечению безопасности информации, обрабатываемой в ИС, и их последствия классифицируются по значимости на:

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

Служебнаяпроверка назначается по нарушениям I и II категорий.

8.2 Перечень нарушений требований по обеспечению безопасности информации

Нарушения I категории, к которым относятся нарушения, повлекшие за собой разглашение (утечку), уничтожение (искажение) информации в ИС и/или утрату машинных носителей информации, выведение из строя технических и программных средств, входящих в состав ИС, а именно:

- успешный подбор административного пароля;
- несанкционированная реконфигурация параметров ИС;
- утрата или кража резервной копии базы, содержащей информацию;
- необоснованная передача информационных массивов ИС;
- организация утечки сведений по техническим каналам;
- умышленное нарушение работоспособности ИС;
- НСД к информации, обрабатываемой в ИС;
- несанкционированное внесение изменений в ИС;
- умышленное заражение АРМ и серверов, входящих в состав ИС, вредоносным ПО;
- проведение работ с ИС, повлекшее за собой необратимую потерю данных;
- другие действия, за совершение которых наступает ответственность в порядке, предусмотренном законодательством РФ.

Нарушения II категории, к которым относятся нарушения, в результате которых возникают предпосылки к разглашению (утечке), уничтожению (искажению) информации,обрабатываемой в ИС, утрате машинных носителей информации, выведению из строя технических и программных средств, входящих в состав ИС, а именно:

- ошибка при входе в ИС (набор не назначенного пароля, более 3 (Трех) раз подряд, периодически);
- оставление АРМ включенным (незаблокированным) во время отсутствия пользователя ИС на рабочем месте;
- перезагрузка АРМ при сбоях в работе, в т.ч. аварийная (неоднократная) перезагрузка путем нажатия кнопки RESET;
- утрата учтенного машинного носителя информации;

– многократная неудачная попытка входа под чужим именем, паролем;
– удачная попытка входа под чужим именем, паролем;
– несанкционированная очистка журналов аудита;
– несанкционированное копирование информации, обрабатываемой в ИС,на внешние носители информации;
– несанкционированная установка (удаление) ПО в ИС;
– несанкционированное изменение конфигурации ПО ИС;
– попытка получения прав администратора на АРМ (увеличения полномочий собственных прав, получение прав на отладку программ) удачная и неудачная;
– попытка получения прав администратора в домене или на удаленной машине, удачная и неудачная;
– неумышленное заражение АРМ компьютерными вирусами;
– несанкционированное использование сканирующего ПО;
– несанкционированное использование анализаторов протоколов (снифферов);
– несанкционированный просмотринформации, обрабатываемой в ИС, вывод на печать и т.п.

Нарушения III категории, к которым относятся нарушения, не несущие признаков нарушений I и II категорий, а именно:
– ошибка при входе в ИС (набор неправильного пароля, сетевого имени более 3 (Трех) раз подряд, не периодическая);
– периодическая попытка неудачного доступа к ИС;
– перевод времени на АРМ;
– однократная перезагрузка АРМ при сбоях в работе АРМ, в т.ч. аварийная перезагрузка, путем нажатия кнопки RESET;
– нецелевое использование корпоративных ресурсов (печать, Internet, электронная почта и т.п.).

8.3. Назначение и проведение служебнойпроверки

Служебнаяпроверка назначается по нарушениям I и II категорий.

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

Служебная проверка проводится комиссией, состав которой утверждает руководитель.

Члены комиссии имеют право:
– требовать документального подтверждения факта нарушений информационной безопасности ИС администрации городского округа Богданович;
– устанавливать причины допущенных нарушений любым из способов, не противоречащих законодательству РФ;
– брать письменные объяснения по поводу выявленных нарушений у любого сотрудника.

За выявление и классификацию нарушения требований по обеспечению безопасности информации,обрабатываемой в ИС, требующего проведения процедуры служебнойпроверки, ответственность несет администратор информационной безопасности.

8.4. Оформление результатов работы комиссии

Результаты работы комиссии должны быть оформлены в виде аналитического экспертного заключения на имя руководителя с предложениями по необходимым организационным выводам, а также по расширению или дополнению перечня нарушений требований по обеспечению безопасности информации,обрабатываемой в ИС.

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 проверкии имеющих значение в определении наличия нарушений, а также иных фактов, которые могут привести к нарушению конфиденциальности информации;

– 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 информации, исключающие в дальнейшем подобные нарушения.

9. Порядок управления доступом субъектов доступа к объектам доступа в ИС

Предоставление доступа пользователю к ИС (или изменение прав доступа) осуществляется на основании Перечня лиц, имеющих право доступа кинформации,обрабатываемой в ИС, утвержденного руководителемадминистрации городского округа Богданович.

С целью организации учета лиц, имеющих право доступа к информации, обрабатываемой в ИС, ведется журнал учета пользователей, имеющих право доступа к информационным системам, форма которого приведена в Приложении 1 к настоящему Положению.

Назначение прав доступа пользователей к информации, обрабатываемой в ИС, осуществляется администратором информационнойбезопасности в соответствии с заявками на предоставление пользователю ИС прав доступа к ИС (ресурсу ИС) отруководителя отдела, оформляемыми по форме, приведенной вПриложении 4 к настоящему Положению. При этом в журнале

учетапользователей, имеющих право доступа к информационным системам, производится соответствующая запись.

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

Контроль за деятельностью пользователей ИС ведется администратором информационнойбезопасности.

Наличие у сотрудника избыточных, неконтролируемых прав доступа является нарушением требований по обеспечению безопасности информации, обрабатываемой в ИС.

Основанием для прекращения права доступапользователякинформации, обрабатываемой в ИС, может служить его исключение из утвержденного руководителем Перечня лиц, имеющих право доступа кинформации, обрабатываемой в ИС, или его увольнение.

10. Организация парольной защиты в ИС

10.1. Общие положения

Целью применения и реализации парольной защиты является исключение утечки информации, обрабатываемой в ИС, 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 администратораинформационнойбезопасности.

10.2. Порядок организации парольной защиты

Защите паролем подлежит доступ к следующей информации:

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

– настройки ОС;

– настройки сетевого оборудования;

– настройки СЗИ;

– ПО, с помощью которого осуществляется обработкаинформации в ИС;

– ресурсы АРМ и информационные ресурсы, содержащие информацию,обрабатываемую в ИС.

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

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

– 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;

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

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

– при смене пароля новое значение должно отличаться от предыдущего;

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

– не допускается использование ранее использованных пароли.

Лица, использующие паролирование, обязаны:

– четко знать и строго выполнять требования по парольной защите;

– своевременно сообщать администраторуинформационнойбезопасности обо всех нештатных ситуациях, возникающих при работе с паролями.

При организации парольной защиты запрещается:

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

– хранить пароли в записанном виде на отдельных листах бумаги;

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

10.3. Порядок применения парольной защиты

Полная плановая смена паролей проводится один раз в 3 (Три) месяца.

Удаление (в т.ч. внеплановая смена) личного пароля любого пользователя должна производиться в следующих случаях:

– при подозрении на компрометацию пароля;

– по завершении срока действия пароля;

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

– по указанию администратораинформационнойбезопасности;

– в случае прекращения полномочий (увольнение, переход на другую работу внутри организации) администратораинформационнойбезопасности.

Смена пароля осуществляется администратороминформационнойбезопасности.

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.

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

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.

Ответственность за организацию парольной защиты возлагается на администратораинформационнойбезопасности.

Ответственность за соблюдение требований парольной защиты возлагается на администратораинформационной безопасности и пользователей ИС.

Нарушения организации и порядка применения парольной защиты классифицируются в соответствии с Перечнем нарушений требований по обеспечению безопасности информации, обрабатываемой в ИС.

При выявлении нарушений I и II категории проводится служебнаяпроверка в соответствии с Порядком проведения служебной проверки по фактам нарушения требований по обеспечению безопасности информации, обрабатываемой в ИС.

11. Организация антивирусной защиты в ИС

11.1. Общие положения

Целью антивирусной защиты ИС является предотвращение и нейтрализация негативных воздействий вредоносного ПО на информационные ресурсы, содержащие информацию, обрабатываемую в ИС,и ПО, предназначенное для обработки такой информации.

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

К использованию в ИС допускаются только лицензионные и сертифицированные ФСТЭК России и ФСБ РФ по требованиям безопасности информации средства антивирусной защиты.

Установка и начальная настройка средств антивирусной защиты в ИС может осуществляться администратороминформационной безопасности, а также представителями организации-лицензиата ФСТЭК России и ФСБ РФ.

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

Пользователи ИС, обязаны руководствоваться в работе Порядком организации антивирусной защиты.

11.2. Порядок организации антивирусной защиты

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация, обрабатываемая в ИС и содержащаяся на машинных носителях (жесткие магнитные диски, оптические носители информации (CD-, DVD-диски), флеш-накопители USB). Антивирусный контроль информации необходимо осуществлять перед архивированием или записью на машинный носитель. Файлы, помещаемые в электронный архив, в обязательном порядке проходят антивирусный контроль. Периодические проверки электронных архивов проводятся администратороминформационнойбезопасности не реже 1 (Одного) раза в месяц.

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

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

В случае обнаружения вредоносного ПО при проведении антивирусной

проверки пользователь ИС обязан:

– приостановить работу АРМ;

– немедленно поставить в известность о факте обнаружения вредоносного ПО администратораинформационнойбезопасности, а также других пользователей ИС, использующих зараженные файлы в работе;

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

– провести «лечение» или удаление зараженных файлов.

Периодически, но не реже 1 (Одного) раза в неделю, администратороминформационнойбезопасности должна проводиться антивирусная проверка всех жестких дисков АРМ пользователей ИС.

Антивирусные проверки подлежат регистрации в журнале учета антивирусных проверокинформационных систем, форма которого приведена в Приложении6 к настоящему Положению.

Ответственность за проведение мероприятий антивирусной защиты и контроля, соблюдения требований антивирусной защиты в ИСвозлагается на администратораинформационнойбезопасности.

12. Организация учета машинных носителей информации

12.1. Порядок учета машинных носителей информации

Все машинные носителиинформации, содержащие информацию, обрабатываемую в ИС, а именно:

– жесткие диски, находящиеся в системных блоках серверов;

– жесткие диски, находящиеся во внешних RAID-массивах серверов;

– жесткие диски, находящиеся в системных блоках АРМИС;

– 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 машинного носителяинформации должен наноситься непосредственно на корпус носителя и быть нестираемым.

На рабочих местах пользователейИС не должны находиться неучтенные машинные носители информации, обрабатываемой в ИС.

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

Сотрудник, получивший носитель для работы с информацией, обязан обеспечить его недоступность для третьих лиц (посторонних лиц и сотрудников, не имеющих право доступа к информации, обрабатываемой в ИС).

Полученные извне машинные носители информации должны:

– проверяться на наличие вредоносных программных продуктов;

– подлежать учету.

Регистрацию и учет машинных носителей информации, содержащихинформацию, обрабатываемую в ИС, осуществляет администраторинформационной безопасности в соответствующем журнале учета машинных носителей информации, форма которого приведена в Приложении 7 к настоящему Положению.

12.2.Порядок хранения машинных носителей информации

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

Машинные носители информациидолжны храниться в недоступном для посторонних лиц месте - в металлических шкафах, оборудованных замками (сейфах).

12.3. Порядок эксплуатации машинных носителей информации

Выдача машинных носителей информациипользователям ИС производится администратором информационнойбезопасности под подпись в соответствующем журнале учета машинных носителей информации.

Передачамашинныхносителейинформациидля ремонта или утилизации запрещена.

Все машинныеносителиинформации,потерявшие актуальность, передаются администратору информационной безопасности.По результатам уничтожения информации с машинного носителя информациииили форматирования такого машинного носителя информации, или уничтожения машинного носителя информации, содержащегоинформацию, составляется акт об уничтожении информации и/или акт об уничтожении машинного носителя, содержащегоинформацию. По факту уничтожения машинного носителяинформации в журнале учета машинных носителей информациипроизводится отметка об уничтожении.

13. Организация резервирования и восстановления информации в ИС

13.1. Общие положения

С целью обеспечения возможности незамедлительного восстановления 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.

13.2. Информация, подлежащая резервному копированию

Резервному копированию подлежат следующие информационные ресурсы:

– файлы, каталоги, БД ИС, содержащие информацию, обрабатываемую в ИС;

– системные и конфигурационные файлы ОС и специального ПО серверов;

– конфигурационные файлы сетевого оборудования;

– системные и конфигурационные файлы СЗИ.

13.3. Порядок резервирования и хранения резервных копий

Резервное копирование информации, обрабатываемой в ИС,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 массивовинформационных систем, форма которого приведена в Приложении 8 к настоящему Положению.

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

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

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

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

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

13.4. Порядок восстановления работоспособности ИС

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 учетанештатных ситуаций в информационных системах, форма которого приведена в Приложении 9 к настоящему Положению.

При восстановлении работоспособности ПО сначала осуществляется резервное копирование информационных ресурсов, содержащихинформациюобрабатываемую в ИС, затем производится полное уничтожение некорректно работающего ПО.

Восстановление ПО производится путем его установки с использованием

эталонных дистрибутивов (установочных дисков).

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

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

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

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

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

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

Проверке подлежат следующие электронные журналы:

– Журнал событий, формируемых СЗИ;

– Журнал событий, формируемых программным обеспечением ИС и СУБД;

– Журналы, формируемые ОС и прикладным ПО.

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

Аудит событий, зафиксированных в электронных журналах, должен анализироваться в плановом порядке на постоянной основе не реже 1 (Одного) раза в неделю администратороминформационной безопасности с обязательной регистрацией в журнале проверки электронных журналовинформационных систем, форма которого приведена в Приложении 10 к настоящему Положению.

15. Порядок обращения со средствами защиты информации

15.1. Учет средств защиты информации

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

Инсталлирующие СЗИ носители, установленные СЗИ, эксплуатационная и техническая документация к СЗИ подлежат поэкземплярному учету в журнале поэкземплярного учета средств защиты информации, эксплуатационной и технической документации к ним,форма которого приведена в Приложении 11к настоящему Положению.

Администратор информационнойбезопасности должен осуществлять периодическое тестирование СЗИс отметкой в журнале учета периодического тестирования средств защиты информации, форма которого приведена в Приложении 12.

15.2. Распространение средств защиты информации

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

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

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

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.

15.3. Получение средств защиты информации

Полученные упаковки вскрываются только лицом, для которого они предназначены.

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

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

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

15.4. Уничтожение средств защиты информации

СЗИ уничтожаются (утилизируются) по решению руководителя.

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

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

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

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

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

15.5. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены средства защиты информации

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

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

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

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

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

15.6. Ответственность за нарушение требований эксплуатации средств защиты

Контроль за организацией и обеспечением функционирования СЗИ возлагается на администратора информационнойбезопасности в пределах его полномочий.

Пользователи ИС несут персональную ответственность за сохранность полученных СЗИ, эксплуатационной и технической документации к СЗИ, за соблюдение положений настоящего Положения.

Администратор информационной безопасности несет ответственность за соответствие проводимых им мероприятий по организации и обеспечению безопасности обработки информациис использованием СЗИ лицензионным требованиям и условиям, эксплуатационной и технической документации к СЗИ.

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

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

- нарушения штатной работы информационных ресурсов и сервисов ИС;
- нарушения штатного функционирования оборудования;
- несанкционированной модификации;
- несанкционированного копирования.

Ответственность за невыполнение требований настоящей главы, проведение в плановом порядке работ по обновлению оборудования, операционной системы, ПО в целях своевременной ликвидации выявленных уязвимостей ПО в информационной инфраструктуре, за отслеживание появления новых уязвимостей в используемых ОС, за установку программных компонентов, устраняющих данные уязвимости, за тестирование ИС при внесении изменений и дополнений в ПО и оборудование на отсутствие негативных воздействий на функционирование ИС, ответственность за мониторинг событий, фиксируемых системами безопасности, несет администратор информационной безопасности.

Установке нового оборудования предшествует тестирование инфраструктурыИС 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 ПО или внесению изменений и дополнений в действующее ПО предшествует тестирование информационной инфраструктуры ИС на отсутствие негативных воздействий устанавливаемого ПО.

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

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

17. Контроль и надзор за эксплуатацией аттестованной ИС

Государственный контроль и надзор за проведением аттестации ИС по требованиям безопасности информации, а также за соблюдением правил эксплуатации аттестованной ИС и эффективностью принятых мер защиты некриптографическими методами, проводится ФСТЭК России и ее территориальными органами.

Объем, содержание и порядок государственного контроля и надзора устанавливаются нормативными и методическими документами по обеспечению безопасности информации при еeобработке в ИС. Контрольные мероприятия проводятся в соответствии с утвержденными планами работ.

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

18.Ответственность за нарушение требований законодательства

Лица, виновные в нарушении норм законодательства в сфере защиты информации, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, предусмотренном законодательством РФ.

Приложение №1
к распоряжению
главы городского округа
Богданович
от 11.01.2016 № 1-р

Форма журнала
учета пользователей, имеющих право доступа к
информационным системам

№ п/п	Дата	Ф.И.О. пользователя информационной системы	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

Приложение № 2
к распоряжению
главы городского округа
Богданович
от 11.01.2016 № 1-р

УТВЕРЖДАЮ

_____
(должность)

_____
(фамилия, имя, отчество)

«___» _____ 20__ г.

М.П.

Акт № _____
об уничтожении информации

Комиссия в составе:

– председатель комиссии _____
(должность) (Фамилия Имя Отчество)

– члены комиссии _____
(должность) (Фамилия Имя Отчество)

_____
(должность) (Фамилия Имя Отчество)

провела отбор машинных носителей информациии 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 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 информации)

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

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

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

Приложение № 3
к распоряжению
главы городского округа
Богданович
от 11.01.2016 № 1-р

УТВЕРЖДАЮ

_____
(должность)

_____
(фамилия, имя, отчество)

«___» _____ 20__ г.

М.П.

Акт № _____
об уничтожении машинных носителей информации

Комиссия в составе:

– председатель комиссии _____
(должность) (Фамилия Имя Отчество)

– члены комиссии _____
(должность) (Фамилия Имя Отчество)

_____
(должность) (Фамилия Имя Отчество)

провела отбор машинных носителей информациии 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 носителейинформации.

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

Всего машинных носителей информации _____
(количество цифрами и прописью)

Указанные машинные носители информации уничтожены путем _____.
(способ уничтожения машинных носителей информации)

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

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

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

Приложение № 4
к распоряжению
главы городского округа
Богданович
от 11.01.2016 № 1-р

Заявка
на предоставление пользователю прав доступа к информационной системе (ресурсу информационной системы)

_____

(наименование информационной системы или ресурсаинформационной системы)

№ п/п	Ф.И.О., № кабинета	Должность	Имя АРМ в домене	Права доступа к информационной системе (ресурсу информационной системы)			Время доступа к информационной системе (ресурсу информационной системы)	
				чтение	редактирование	удаление	дни недели	рабочие часы
1	2	3	4	5	6	7	8	9

Руководитель структурного подразделения_____

(подпись) *(расшифровка подписи)*

«__» _____ 20__ г.

Приложение № 5
к распоряжению
главы городского округа
Богданович
от 11.01.2016 № 1-р

Форма журнала
учета выдачи паролей для доступа к
информационным системам

№ 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 распоряжению
главы городского округа
Богданович
от 11.01.2016 № 1-р

Форма журнала
учета антивирусных проверок
информационных систем

№ п/п	Дата и время проверки	Наименование и инвентарный/серийный номер технического средства, наименование проверяемого информационного ресурса информационной системы	Какими средствами проводилась проверка	Результаты проверки		Наименование инфицированных файлов, источника поступления (носитель, организация)	Примечание (принятые меры)	Ф.И.О. и подпись администратора информационной безопасности
				количество проверенных файлов	количество инфицированных файлов			
1	2	3	4	5	6	7	8	9

Приложение № 7
к распоряжению
главы городского округа
Богданович
от 11.01.2016 № 1-р

Форма журнала
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 сотруднику 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 унич-тожении машинного носителя информации	Примечание
1	2	3	4	5	6	7	8	9	10

Приложение № 8
к распоряжению
главы городского округа
Богданович
от 11.01.2016 № 1-р

Форма журнала
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	Приме-чание
1	2	3	4	5	6	7

Приложение № 9
к распоряжению
главы городского округа
Богданович
от 11.01.2016 № 1-р

Форма журнала
учетанештатных ситуаций винформационных 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	6

Приложение № 10
к распоряжению
главы городского округа
Богданович
от 11.01.2016 № 1-р

Форма журнала
проверки электронных журналов информационных систем

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

Приложение № 11
к распоряжению
главы городского округа
Богданович
от 11.01.2016 № 1-р

Форма журнала
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	6	7	8

Приложение № 12
к распоряжению
главы городского округа
Богданович
от 11.01.2016 № 1-р

Форма журнала
учета периодического тестирования средств защиты информации

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