УТВЕРЖДАЮ
Руководитель Администрации Рузского
муниципального района

_____ Тарханов М.В.
«15» декабря 2014 года

ПОЛОЖЕНИЕ
О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ И КОНТРАГЕНТОВ ПРИ ИХ АВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ АДМИНИСТРАЦИИ РУЗСКОГО МУНИЦИПАЛЬНОГО РАЙОНА

РАЗРАБОТАЛ

Начальник отдела кадров _____ Б.В. Козлова
(должность, подпись, инициалы, фамилия ответственного за эксплуатацию АС)
«____» _____ 2014 г

Руза
2014

СОДЕРЖАНИЕ

1. СПИСОК СОКРАЩЕНИЙ

АС	-	автоматизированная система
АРМ	-	автоматизированное рабочее место
ВПр	-	вредоносная программа
ИС	-	информационная система
ИСПДн	-	информационная система персональных данных
КЗ	-	контролируемая зона
НСД	-	несанкционированный доступ
ПО	-	программное обеспечение
СВТ	-	средства вычислительной техники
СЗИ	-	средство защиты информации
ТУ	-	технические условия
ФСТЭК России	-	Федеральная служба по техническому и экспортному контролю
Гостехкомиссия России	-	Государственная техническая комиссия при Президенте Российской Федерации

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения.

Аттестация объекта информатизации – комплекс организационно-технических мероприятий, в результате которых специальным документом – Аттестатом соответствия подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России (Гостехкомиссией России).

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

Безопасность информации – состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней, целостность и доступность информации при ее обработке техническими средствами.

Защита информации от несанкционированного доступа и воздействия – деятельность, направленная на предотвращение или существенное затруднение несанкционированного доступа к информации (или воздействия на информацию).

Информационные сети общего пользования – вычислительные (информационно-телекоммуникационные) сети открытые для пользования всем физическим и юридическим лицам, в услугах которых этим лицам не может быть отказано.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Контролируемая зона – это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей, а также транспортных средств.

Конфиденциальная информация (сведения конфиденциального характера) – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность информации – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.

Несанкционированный доступ – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств АС.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование и уничтожение.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Машинные носители информации – встроенные (съёмные) накопители на жёстких магнитных дисках, гибкие магнитные диски, Flash-накопители, DVD(CD)-диски, карты памяти и др. устройства, используемые для записи, накопления и хранения информации в электронном виде.

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

Система защиты информации от несанкционированного доступа – комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации (несанкционированных действий с ней).

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в и/или выходящей из информационной системы, и обеспечивает защиту посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) информационной системы.

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. Настоящее «Положение о порядке организации и проведения работ по обеспечению безопасности персональных данных при их автоматизированной обработке в информационной системе персональных данных Администрации Рузского муниципального района (далее – Положение) определяет порядок и организацию проведения работ по защите персональных данных в Администрации Рузского муниципального района (далее – Администрация), и является основным руководящим документом по защите персональных данных в Администрации.

3.2. Данное Положение разработано на основании Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» (в ред. Федерального закона от 25.07.2011 N 261-ФЗ), Постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказа ФСТЭК России №17 от 18.02.2013 и руководящих документов ФСТЭК России в целях обеспечения безопасности персональных данных (далее – ПДн), «Специальных требований и рекомендаций по технической защите конфиденциальной информации» (СТР-К), приказа Гостехкомиссии России от 30 августа 2002 года № 282.

3.3. Положение определяет организацию и порядок проведения мероприятий, направленных на обеспечение защиты персональных данных от утечки по техническим каналам и несанкционированного доступа к информации (далее – НСД)

3.4. Организацию защиты персональных данных в Администрации Рузского муниципального района осуществляют:

– в технических аспектах – администратор безопасности информации;

– в организационных аспектах и аспектах регламентированных настоящим Положением – ответственный за обеспечение безопасности персональных данных.

3.5. Положение ежегодно доводится до руководителей подразделений в полном объеме, до сотрудников подразделений, обрабатывающих персональные данные, в части, их касающиеся.

3.6. Защита персональных данных считается достаточной, если принятые меры обеспечивают выполнение действующих норм и требований руководящих документов по их защите. Обработка персональных данных в Администрации Рузского муниципального района без принятия мер по ее защите не допускается.

4. ОСНОВНЫЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ АДМИНИСТРАЦИИ

4.1. Основными мероприятиями по обеспечению безопасности персональных данных при обработке в информационных системах Администрации являются:

– проверка готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

– установка и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

– обучение сотрудников Администрации правилам работы со средствами защиты информации, применяемых в информационной системе;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

– использование (применение) сертифицированных средств защиты информации и контроль их эффективности;

– учет лиц, допущенных к работе с персональными данными;

– контроль над соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

– контроль над фактами несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности информации или другим нарушениям, приводящим к снижению уровня ее защищенности, разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

– предупреждение угроз непреднамеренных действий пользователей и нарушений безопасности функционирования системы защиты персональных данных (далее – СЗПДн) в результате сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера;

– обеспечение эффективного функционирования системы защиты персональных данных в Администрации;

– определение перечня сведений конфиденциального характера, подлежащих защите;

– разработка оптимальных организационно-технических мероприятий по защите персональных данных и их практическая реализация;

– организация и проведение контроля эффективности применяемых мер и средств защиты;

– планирование мероприятий по защите персональных данных в Администрации;

– классификация информационных систем с целью установления методов и способов защиты персональных данных;

– осуществление специального учета и маркировки носителей информации, бумажных и других носителей, содержащих персональные данные;

– аттестационные испытания информационных систем Администрации по требованиям безопасности информации.

4.2. Финансирование и материально-техническое обеспечение мероприятий по защите информации осуществляется из средств, получаемых в процессе основной деятельности Администрации.

4.3. Ответственность за выполнение требований по защите персональных данных возлагается на Руководителя Администрации.

5. ПЛАНИРОВАНИЕ РАБОТ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Работа по защите персональных данных Администрации проводится в соответствии с годовым «Планом по защите конфиденциальной информации» (далее – План), утверждаемым Руководителем Администрации.

5.2. Годовой План составляет ответственный за обеспечение безопасности персональных данных в Администрации Рузского муниципального района.

5.3. В годовой план включаются следующие основные мероприятия по:

– выполнению требований ФСТЭК России, других правовых и нормативно-методических документов по защите конфиденциальной информации;

– защите конфиденциальной информации, в том числе персональных данных, в информационных системах Администрации от несанкционированного доступа;

– обследованию, классификации и аттестации информационных систем по требованиям безопасности информации;

– разработке, корректировке и согласованию организационно-распорядительных документов, положений, планов, отчетов по вопросам защиты конфиденциальной информации;

– приобретение систем и средств защиты информации;

– проведению занятий с сотрудниками Администрации по обеспечения информационной безопасности;

– организации периодических проверок эффективности применяемых средств и систем защиты информации;

– участию в работе контролирующих органов;

– организации проведения проверок состояния защиты конфиденциальной информации, в том числе персональных данных, в Администрации.

5.4. Годовой план должен содержать мероприятия по защите конфиденциальной информации, выполняемые:

– ответственным за обеспечение безопасности персональных данных;

– администратором безопасности информации;

– руководителями структурных подразделений, которые в силу своих функциональных обязанностей отвечают за обеспечение информационной.

5.5. Контроль над исполнением годового плана возлагается на Руководителя Администрации.

6. ПОРЯДОК ФОРМИРОВАНИЯ МОДЕЛИ УГРОЗ И МОДЕЛИ НАРУШИТЕЛЯ ПДн

6.1. Модель угроз формируется в результате выявления и учета факторов, которые воздействуют или могут воздействовать на информацию (угроз безопасности информации) в конкретных условиях (для каждого конкретного объекта в частности и в целом – для Администрации).

6.2. Формирование модели угроз проводятся в соответствии с ГОСТ Р 51275-99, «Базовой моделью угроз безопасности ПДн при их обработке в ИСПДн», утвержденной заместителем директора ФСТЭК России от 15.02.2008, «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной заместителем директора ФСТЭК России от 14.02.2008,

«Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утверждёнными руководством 8 Центра ФСБ России 21.02.2008 № 149/54-144 и составляет основу для планирования мероприятий, направленных на защиту персональных данных в Администрации.

6.3. Анализ конкретных условий предполагает:

– определение условий расположения объекта информатизации относительно границ КЗ;

– определения порядка доступа персонала и лиц, представителей сторонних организаций, на территорию Администрации;

– определение конфигурации и топологии ИСПДн и систем связи в целом и их отдельных компонентов, физических, функциональных и технологических связей как внутри этих систем, так и с другими системами различного уровня и назначения;

– определение технических средств и систем, предполагаемых к использованию при обработке персональных данных, условий их расположения;

– определение степени участия персонала Администрации в обработке (обсуждении, передаче, хранении) информации, характер их взаимодействия между собой.

6.4. Сформированные Модель угроз и Модель нарушителя определяют перечень возможных актуальных угроз безопасности персональных данных в Администрации, возможных нарушителей, организационных и технических мероприятий необходимых для обеспечения выполнения действующих норм и требований руководящих документов по защите персональных данных.

6.5. Уровень технической защиты персональных данных, а также перечень необходимых мер защиты определяется дифференцировано по результатам обследования объекта информатизации, с учетом сформированной Модели угроз и Модели нарушителя, а также соотношения затрат на организацию защиты информации и величины ущерба, который может быть нанесен Администрации.

6.6. Обследование с целью формирования Модели угроз и нарушителя проводится комиссией из числа сотрудников Администрации, назначаемых Приказом Руководителя Администрации. Для проведения обследования также могут привлекаться специализированные организации, имеющие соответствующую лицензию.

7. ПОРЯДОК ДОПУСКА К РАБОТЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

7.1. Допуск пользователей для работы на автоматизированной система (далее – АС) ИСПДн осуществляется в соответствии со Списком сотрудников, имеющих доступ к персональным данным, обрабатываемым в информационной системе Администрации Рузского муниципального района, для выполнения служебных (трудовых) обязанностей.

7.2. Основанием для допуска сотрудника к обработке персональных данных является Приказ Руководителя Администрации Рузского муниципального района о приеме на работу, переводе сотрудника на должность, предусматривающую обработку персональных данных или иное распоряжение Руководителя Администрации.

7.3. Утверждать «Список сотрудников…» имеет право только Руководитель Администрации, или лицо, его замещающее.

7.4. Пересмотр «Списка сотрудников…», должен осуществляться каждый раз при изменении состава субъектов доступа к ИСПДн, а также не реже 1 раза в год.

7.5. Перед предоставлением сотруднику Администрации права допуска к работам в ИСПДн он должен ознакомиться со следующими организационно-распорядительными документами Администрации:

– специальными (техническими, технологическими) инструкциями по работе со штатными техническими средствами ИСПДн (из комплекта поставки);

– комплектом пользовательской документации на программные средства ИСПДн;

– нормативными документами и должностными инструкциями по работе со сведениями конфиденциального характера в части качающейся;

– руководством пользователя на использование средств защиты информации в ИСПДн.

7.6. После изучения указанных документов сотрудник проходит инструктаж по допуску к самостоятельной работе с персональными данными у ответственного за обеспечение безопасности персональных данных в Администрации.

7.7. Пользователи, показавшие твердые теоретические знания и практические навыки по изученным организационно – распорядительных и эксплуатационных документов, допускаются к работе в информационных системах, обрабатывающих персональные данные, в соответствии со своими служебными обязанностями.

7.8. Для проведения занятий, семинаров и совещаний могут привлекаться специалисты по программному и техническому обеспечению, а также специалисты органов по аттестации объектов информатизации, организаций-лицензиатов ФСТЭК России и ФСБ России.

7.9. Пользователи, демонстрирующие недостаточные знания и умения для обеспечения безопасности персональных данных в соответствии с требованиями настоящего Положения, к работе в ИСПДн не допускаются.

7.10. Основанием для прекращения допуска сотрудника к обработке персональных данных является Приказ об увольнении сотрудника из Администрации Рузского муниципального района, его переводе на должность, не предусматривающую обработку персональных данных, либо иное распоряжение Руководителя Администрации.

8. ПОРЯДОК РАБОТЫ ПЕРСОНАЛА В ЧАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ

8.1. Настоящий порядок определяет действия персонала Администрации в части обеспечения безопасности персональных данных при их обработке в ИСПДн.

8.2. Руководитель Администрации:

– назначает должностных лиц, ответственных за обеспечение безопасности персональных данных в ИСПДн;

– утверждает руководящие документы по защите персональных данных;

– принимает решения о финансировании мероприятий по защите персональных данных;

– принимает решения о прекращении работ на участке, где выявлены нарушения в обеспечении безопасности персональных данных, а также о возобновлении выполнения работ после их устранения.

5.2. С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации в ИСПДн Приказом Руководителя Администрации назначается администратор безопасности информации. С целью общей организации обеспечения информационной безопасности персональных данных и эффективности менеджмента информационной безопасности в данных аспектах Приказом Руководителя назначается ответственный за обеспечение безопасности персональных данных.

8.3. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для записи и хранения персональных данных разрешается использовать съемные носители, учтенные установленным порядком в Журнале учета машинных носителей, предназначенных для хранения конфиденциальной информации.

8.4. Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (далее – СВТ), входа в систему и всех действий при работе в ИСПДн.

8.5. Вход пользователя в систему осуществляется по выдаваемому ему идентификатору (логину) и персональному паролю.

8.6. При работе со съемными носителями пользователь, каждый раз перед началом работы, обязан проверить их на отсутствие вирусов с использованием штатных антивирусных средств, согласно «Инструкции по организации антивирусной защиты ….».

8.7. Каждый пользователь, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам и программному обеспечению в ИСПДн, несет персональную ответственность за свои действия и ***обязан***:

– строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

– знать и строго выполнять правила работы со средствами защиты информации, установленными в ИСПДн;

– хранить в тайне свой пароль (пароли) и с установленной периодичностью менять свой пароль (пароли) в соответствии с разделом 6 «Инструкции пользователю ИСПДн…»;

– выполнять требования «Инструкции по организации антивирусной защиты…» в полном объеме;

– немедленно известить ответственного за обеспечение безопасности персональных данных и (или) администратора безопасности информации при подозрении компрометации и подбора личных ключей и паролей, а также при обнаружении:

- нарушений целостности печатей (пломб, защитных наклеек) на составляющих узлах и блоках СВТ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее – НСД) к персональным данным;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;

- некорректного функционирования установленных в ИСПДн технических средств защиты;
- непредусмотренных отводов кабелей и подключенных устройств.

8.8. Пользователю категорически ***запрещается***:

– использовать компоненты программного и аппаратного обеспечения ПЭВМ в неслужебных целях;

– самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;

– осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;

– записывать и хранить персональные данные на неучтенных носителях;

– оставлять включенным без присмотра АС не активизировав систему защиты от НСД (временную блокировку экрана и клавиатуры);

– оставлять без личного присмотра на рабочем месте или где бы то ни было свои носители и листы бумаги, содержащие персональные данные;

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении (далее – ПО) или в настройках средств защиты, которые могут привести к возникновению нештатной ситуации;

– размещать средства ИСПДн так, чтобы с них существовала возможность визуального просмотра информации.

8.9. В своей работе пользователь ИСПДн строго руководствуется «Инструкцией пользователю ИСПДн ….».

8.10. Администратор безопасности информации (а при его отсутствии – ответственный за обеспечение безопасности персональных данных) ***обязан***:

– знать состав основных и вспомогательных технических систем и средств (далее - ОТСС и ВТСС) установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения в ИСПДн;

– контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, технических средствах АС и других устройствах информационной сети;

– производить необходимые настройки подсистемы управления доступом установленной в ИСПДн и сопровождать их в процессе эксплуатации, при этом:

- вести учет СЗИ от НСД, средств межсетевого экранирования, эксплуатационной и технической документации к ним в Журнале поэкземплярного учета средств защиты информации, эксплуатационной и технической документации к ним (приложение 1);
- реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);
- вводить описания пользователей ИСПДн в информационную базу СЗИ от НСД;
- своевременно удалять описания пользователей из базы данных СЗИ при изменении «Списка сотрудников…);

– контролировать доступ лиц в помещение в соответствии со списком сотрудников, допущенных к работе в ИСПДн;

– проводить инструктаж сотрудников – пользователей ИСПДн по правилам работы с используемыми техническими средствами и системами защиты информации;

– контролировать своевременное проведение смены паролей для доступа пользователей к ИСПДн и ее ресурсам;

– обеспечивать постоянный контроль выполнения сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн;

– осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных;

– настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе в ИСПДн;

– в случае отказа средств и систем защиты информации принимать меры по их восстановлению;

– вводить в базу данных СЗИ от несанкционированного доступа описания событий, подлежащих регистрации в системном журнале;

– проводить анализ системного журнала для выявления попыток несанкционированного доступа к персональных данных не реже одного раза в 10 дней;

– организовывать печать файлов пользователей на принтере и осуществлять контроль соблюдения установленных правил и параметров регистрации и учета бумажных носителей информации;

– сопровождать подсистемы обеспечения целостности информации в ИСПДн;

– периодически тестировать функции СЗИ от НСД, особенно при изменении программной среды и полномочий исполнителей;

– восстанавливать программную среду, программные средства и настройки СЗИ при сбоях;

– проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;

– контролировать соответствие документально утвержденного состава аппаратной и программной части ИСПДн реальным конфигурациям ИСПДн, вести учет изменений аппаратно-программной конфигурации;

– обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке технических средств в ремонт (контролировать затирание персональных данных на носителях с составлением соответствующего акта);

– присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;

– поддерживать установленный порядок проведения антивирусного контроля;

– периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядка и правил проведения антивирусных проверок;

– докладывать Руководителю Администрации Рузского муниципального района о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;

– вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

8.11. Администратор безопасности информации и ответственный за обеспечение безопасности персональных данных имеет ***право***:

– требовать от работников (пользователей ИСПДн) соблюдения установленной технологии обработки информации и выполнения требований настоящего Положения и инструкций по обеспечению безопасности и защите информации в ИСПДн;

– инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи персональных данных и технических компонентов ИСПДн;

– требовать прекращения обработки персональных данных в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

– участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

9. ПОРЯДОК РЕЗЕРВИРОВАНИЯ И ВОССТАНОВЛЕНИЯ РАБОТОСПОСОБНОСТИ ТЕХНИЧЕСКИХ СРЕДСТВ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, БАЗ ДАННЫХ, КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ.

9.1. Настоящий порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных, конфиденциальной информации и средств защиты информации (далее – Порядок) определяет действия, связанные с функционированием ИСПДн, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

9.2. Задачей данного Порядка является:

– определение мер защиты от потери конфиденциальной информации;

– определение действий восстановления в случае потери конфиденциальной информации.

9.3. Действие настоящего Порядка распространяется на всех пользователей ИСПДн, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

– системы жизнеобеспечения;

– системы обеспечения отказоустойчивости;

– системы резервного копирования и хранения данных;

– системы контроля физического доступа.

9.4. В настоящем Порядке под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же потерей конфиденциальной информации. Происшествие, вызывающее инцидент, может произойти:

– в результате непреднамеренных действий пользователей;

– в результате преднамеренных действий пользователей и третьих лиц;

– в результате нарушения правил эксплуатации технических средств ИСПДн;

– в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

Все действия в процессе реагирования на Инцидент должны документироваться администратором безопасности информации в «Журнале учета инцидентов информационной безопасности…» (приложение 2), выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн.

9.5. Технические меры обеспечения непрерывности работы и восстановления ИСПДн при возникновении инцидентов:

– к техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

- системы жизнеобеспечения (пожарные сигнализации и системы пожаротушения, системы вентиляции и кондиционирования, системы резервного питания);
- системы обеспечения отказоустойчивости (кластеризация, технология RAID);
- системы резервного копирования и хранения данных;
- системы контроля физического доступа;

– все критичные помещения Администрации (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения;

– для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха;

– для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных автоматизированных рабочих мест;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения.

– для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации, для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров;

– для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение конфиденциальной информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках;

– система резервного копирования и хранения данных, должна обеспечивать хранение конфиденциальной информации на носителях.

9.6. Организационные меры обеспечения непрерывности работы и восстановления ИСПДн при возникновении инцидентов:

– резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых персональных данных – не реже 1 раза в день;
- для технологической информации – не реже 1 раза в месяц;

• эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже 1 раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий);

– к использованию, для создания резервной копии в ИСПДн, допускаются только носители, зарегистрированные в соответствии с Инструкцией о порядке учета, хранения, обращения и уничтожения носителей, предназначенных для хранения конфиденциальной информации;

– машинные носители конфиденциальной информации, предназначенные для создания резервной копии пользовательских АРМ и хранения конфиденциальной информации выдаются установленным порядком ответственным за обеспечение безопасности ПДн и (или) администратором информационной безопасности. По окончании процедуры резервного копирования электронные носители конфиденциальной информации сдаются на хранение администратору безопасности информации или ответственному за обеспечение безопасности ПДн;

– хранение отчуждаемого носителя с резервной копией конфиденциальной информации осуществляется в специальном металлическом хранилище (сейфе) совместно с ключевой и аутентифицирующей информацией.

9.7. Сотрудники Администрации под контролем администратора безопасности информации обязаны осуществлять периодическое резервное копирование конфиденциальной информации, содержащейся в базе данных.

9.8. Резервное копирование базы данных осуществляется штатными программными средствами БД в специально отведенное место на сервер (АРМ).

9.9. Перед резервным копированием пользователь или администратор безопасности информации обязан проверить носители на отсутствие вирусов.

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

9.11. Запрещается запись посторонней информации на носители, предназначенные для создания резервных копий.

9.12. Порядок создания резервной копии:

– вставить в системный блок АРМ зарегистрированный в «Журнале учета машинных носителей, предназначенных для хранения конфиденциальной информации …» носитель для резервного копирования;

– выбрать необходимый каталог (файл) для создания резервного архива;

– при использовании систем управления базами данных необходимо создать файл с резервной копией конфиденциальной информации с помощью встроенных средств системы;

– выполнить процедуру создания резервной копии на носитель;

– произвести отключение носителя.

9.13. При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование конфиденциальной информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.

9.14. Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов, хранение которых осуществляется администратором безопасности информации.

9.15. При необходимости ремонта технических средств, с них удаляются опечатывающие пломбы и по согласованию с администратором безопасности информации и ответственным за обеспечение безопасности ПДн, оборудование передается в сервисный центр производителя. Ремонт носителей с конфиденциальной информацией не допускается. Неисправные носители с конфиденциальной информацией подлежат уничтожению в соответствии с порядком уничтожения носителей конфиденциальной информации. Работа с использованием неисправных технических средств запрещается.

9.16. При работе на АРМ ИСПДн рекомендуется использовать источники бесперебойного питания, с целью предотвращения повреждения технических средств и (или) конфиденциальной информации в результате сбоев в сети электропитания.

9.17. Восстановление средств защиты информации производится с использованием эталонных лицензионных сертифицированных дистрибутивов, которые хранятся у администратора безопасности информации. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций на зарегистрированный МНИ.

9.18. Ответственность за проведение резервного копирования в ИСПДн в соответствии с требованиями настоящего Положения возлагается на администратора безопасности информации.

9.19. Ответственность за проведение мероприятий по восстановлению работоспособности технических средств и программного обеспечения баз данных возлагается на администратора безопасности.

9.20. Ответственность за проведение мероприятий по восстановлению средств защиты информации (далее – СЗИ) возлагается на администратора безопасности информации.

10. ПОРЯДОК КОНТРОЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ И ПРИОСТАНОВКА ПРЕДОСТАВЛЕНИЯ В СЛУЧАЕ ОБНАРУЖЕНИЯ НАРУШЕНИЙ ИХ ОБРАБОТКИ. ПОРЯДОК РАЗБИРАТЕЛЬСТВА И СОСТАВЛЕНИЯ ЗАКЛЮЧЕНИЙ ПО ФАКТАМ НЕСОБЛЮДЕНИЯ УСЛОВИЙ ХРАНЕНИЯ НОСИТЕЛЕЙ ПДн, ИСПОЛЬЗОВАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ И ПРИНЯТИЕ МЕР ПО ПРЕДОТВРАЩЕНИЮ ВОЗМОЖНЫХ ОПАСНЫХ ПОСЛЕДСТВИЙ

10.1. Под контролем защиты персональных данных в ИСПДн понимается комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами персональных данных, выявления, исключения или существенного затруднения несанкционированного доступа к ней, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности ИСПДн.

10.2. Основными задачами контроля являются:

– проверка организации выполнения мероприятий по защите персональных данных в подразделениях Администрации, учета требований по защите персональных данных в разрабатываемых плановых и распорядительных документах;

– проверка выполнения требований по защите персональных данных от несанкционированного доступа;

– проверка выполнения требований по антивирусной защите;

– проверка знаний работников по вопросам защиты персональных данных;

– оперативное принятие мер по пресечению нарушений требований защиты информации в ИСПДн.

10.3. В ходе контроля проверяются:

– соответствие принятых мер по обеспечению безопасности персональных данных;

– своевременность и полнота выполнения требований настоящего Положения и других руководящих документов по обеспечению безопасности персональных данных;

– полнота выявления демаскирующих признаков персональных данных, возможность утечки информации за счет несанкционированного доступа и программно-технического воздействия на нее;

– эффективность применения организационных и технических мероприятий по защите информации;

– устранение ранее выявленных недостатков.

10.4. Основными видами технического контроля являются контроль несанкционированного доступа к информации и программно-технических воздействий на информацию.

10.5. Полученные в ходе ведения контроля результаты обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты персональных данных и выявления нарушений. При обнаружении нарушений требований по защите персональных данных администратор безопасности информации докладывает ответственному за обеспечение безопасности ПДн для принятия им решения о прекращении обработки информации и проведения соответствующих организационных и технических мер по устранению нарушения. Результаты контроля защиты информации оформляются актами либо учитываются в соответствующих журналах учета результатов контроля.

10.6. Невыполнение предписанных мероприятий по защите персональных данных, считается предпосылкой к утечке информации (далее - предпосылка).

10.7. По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по указанию Руководителя Администрации или ответственного за обеспечение безопасности персональных данных проводится расследование.

Для проведения расследования назначается комиссия с привлечением администратора безопасности информации. Комиссия обязана установить, имела ли место утечка сведений, и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите персональных данных, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования Руководитель Администрации принимает решение о наказании виновных лиц и проведения необходимых мероприятиях по устранению недостатков.

10.8. Ведение контроля защиты персональных данных осуществляется путем проведения периодических, плановых и внезапных проверок объектов защиты. Периодические, плановые и

внезапные проверки объектов Администрации проводятся, как правило, силами администратора безопасности информации и(или) ответственного за обеспечение безопасности персональных данных, в соответствии с утвержденным Планом или по согласованию с Руководителем Администрации.

10.9. Одной из форм контроля защиты информации является обследование объектов ИСПДн. Оно проводится не реже одного раза в год рабочей группой в составе администратора безопасности информации, ответственного за обеспечение безопасности персональных данных и представителей организации проводившей аттестацию ИСПДн.

10.10. Обследование ИСПДн проводится с целью определения соответствия помещений, технических и программных средств требованиям по защите информации, установленным в Аттестате соответствия требованиям безопасности информации.

10.11. В ходе обследования проверяется:

– соответствие текущим условиям функционирования обследуемой ИСПДн условиям, сложившимся на момент проверки;

– соблюдение организационно-технических требований к помещениям, в которых располагается ИСПДн;

– сохранность целостности печатей (пломб, защитных наклеек) на составляющих узлах и блоках СВТ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее – НСД) к персональным данным;

– соответствие выполняемых на объекте информатизации мероприятий по защите персональных данных, изложенных в настоящем положении;

– выполнение требований по защите ИСПДн от несанкционированного доступа (контроль защищенности);

– выполнение требований по антивирусной защите.

10.12. Государственный контроль состояния защиты информации осуществляется Федеральной службой по техническому и экспортному контролю России, Федеральной службой безопасности России и Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникациях, в рамках их полномочий в соответствии с действующим законодательством Российской Федерации. Доступ представителей указанных федеральных органов исполнительной власти на объекты для проведения проверки, а также к работам и документам в объеме, необходимом для осуществления контроля, обеспечивается в установленном порядке по предъявлении служебного удостоверения сотрудника, а также документа установленной формы на право проведения проверки.

11. ПРАВИЛА ОБНОВЛЕНИЯ ОБЩЕСИСТЕМНОГО И ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ ИСПДн

11.1. Настоящие правила регламентируют обеспечение безопасности информации при проведении обновления, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе ИСПДн.

11.2. Все изменения конфигураций технических и программных средств ИСПДн должны производиться только на основании заявок ответственного за обеспечение безопасности персональных данных.

11.3. Право внесения изменений в конфигурацию аппаратно-программных средств защищенной ИСПДн предоставляется:

– в отношении системных и прикладных программных средств – администратору безопасности информации по согласованию со специалистами организации, проводившей аттестацию ИСПДн;

– в отношении аппаратных средств, а также в отношении программно-аппаратных средств защиты – администратору безопасности информации по письменному согласованию со специалистами организации, проводившей аттестацию ИСПДн.

11.4. Изменение конфигурации аппаратно-программных средств ИСПДн кем-либо, кроме вышеперечисленных уполномоченных сотрудников и подразделений, запрещено.

11.5. В заявке могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств ИСПДн:

– установка (развертывание) АРМ пользователей программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи в данной ИСПДн);

– обновление (замена) АРМ пользователей программных средств, необходимых для решения определенной задачи (обновление версий используемых для решения определенной задачи программ);

– удаление АРМ пользователей программных средств, использовавшихся для решения определенной задачи.

11.6. Также в заявке указывается условное наименование ИСПДн. Наименования задач указываются в соответствии с перечнем задач архива дистрибутивов установленного программного обеспечения, которые можно решать с использованием указанного АРМ.

11.7. Заявку ответственного за обеспечение безопасности персональных данных, в которой требуется произвести изменения конфигурации, рассматривает Руководитель Администрации, визирует ее, утверждая тем самым производственную необходимость проведения указанных в заявке изменений.

11.8. После чего заявка передается администратору безопасности информации для непосредственного исполнения работ по внесению изменений в конфигурацию АРМ указанного в заявке.

11.9. Подготовка обновления, модификации общесистемного и прикладного программного обеспечения ИСПДн, тестирование, стендовые испытания (при необходимости) и передача исходных текстов, документации и дистрибутивных носителей программ в архив дистрибутивов установленного программного обеспечения, внесение необходимых изменений в настройки средств защиты от НСД и средств контроля целостности файлов на АРМ, обновление и удаление системных и прикладных программных средств производится администратором безопасности информации по согласованию с органом по аттестации, проводившим аттестацию данной ИСПДн. Работы проводятся в присутствии ответственного за обеспечение безопасности персональных данных.

11.10. Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

11.11. Установка и обновление ПО (системного, тестового и т.п.) на АРМ производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), полученных установленным порядком, прикладного ПО – с лицензионных копий программных средств.

11.12. Все добавляемые программные и аппаратные компоненты должны быть предварительно установленным порядком проверены на работоспособность, а также отсутствие опасных функций.

11.13. После установки (обновления) ПО, администратор безопасности информации должен произвести требуемые настройки средств управления доступом к компонентам СВТ и проверить работоспособность ПО и правильность их настройки, а также произвести соответствующую запись в «Журнале учета инцидентов информационной безопасности…». После этого администратор безопасности информации делает отметку о выполнении (на обратной стороне заявки) и в «Техническом паспорте на АС…».

11.14. При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, ответственный за обеспечение безопасности персональных данных докладывает об этом Руководителю Администрации и связывается с сотрудниками органа по аттестации и в дальнейшем действует согласно их инструкций. В данном случае администратор безопасности информации обязан предпринять необходимые меры для затирания персональных данных, которая хранилась на дисках, используемых в АРМ.

11.15. Оригиналы заявок (документов), на основании которых производились изменения в составе программных средств с отметками о внесении изменений в состав программных средств, должны храниться вместе с «Техническим паспортом на АС…» и «Журналом учета инцидентов информационной безопасности …» у ответственного за обеспечение безопасности персональных данных.

11.16. Копии заявок могут храниться у администратора безопасности информации:

– для восстановления конфигурации ИСПДн после аварий;

– для контроля правомерности установки на ИСПДн средств для решения соответствующих задач при разборе конфликтных ситуаций;

– для проверки правильности установки и настройки средств защиты ИСПДн.

11.17. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе на АРМ, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться, и работать в ИСПДн.

11.18. Использование несколькими сотрудниками при работе в ИСПДн одного и того же имени пользователя («группового имени») запрещено.

11.19. Процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется заявкой ответственного за обеспечение безопасности персональных данных. Форма заявки приведена ниже.

В заявке указывается:

– содержание запрашиваемых изменений (регистрация нового пользователя ИСПДн, удаление учетной записи пользователя, получение прав доступа к ресурсам ИСПДн ранее зарегистрированного пользователя);

– должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;

– имя пользователя (учетной записи) данного сотрудника;

– полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИСПДн).

11.20. Заявку рассматривает Руководитель Администрации, визируя её, утверждая тем самым производственную необходимость допуска данного сотрудника к необходимым для решения им указанных в заявке задач ресурсам ИСПДн. Затем передает заявку администратору безопасности информации на внесение необходимых изменений в списки пользователей ИСПДн.

11.21. На основании задания, в соответствии с документацией на СЗИ от несанкционированного доступа, администратор безопасности информации производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля (возможно также регистрацию персонального идентификатора), заявленных прав доступа к ресурсам ИСПДн и другие необходимые действия, указанные в задании. Для всех пользователей должен быть установлен режим принудительного запроса смены пароля не реже одного раза в течение 90 дней.

11.22. Администратор безопасности информации должен обеспечить настройки средств защиты соответствующие требованиям безопасности указанной ИСПДн. По окончании настройки средства защиты и внесения учетной записи пользователя в систему в заявке делается отметка о выполнении задания за подписью исполнителя – администратора безопасности информации.

11.23. Сотруднику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается персональный идентификатор и начальное значение пароля.

11.24. Исполненная заявка и задание (за подписью администратора безопасности информации) передается ответственному за обеспечение безопасности персональных данных и может впоследствии использоваться:

– для восстановления полномочий пользователей после аварий ИСПДн;

– для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИСПДн при разборе конфликтных ситуаций;

– для проверки сотрудниками контролирующих органов правильности настройки СЗИ ИСПДн.

12. ПОРЯДОК КОНТРОЛЯ СОБЛЮДЕНИЯ УСЛОВИЙ ИСПОЛЬЗОВАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

12.1. Данный раздел Положения определяет порядок контроля соблюдения условий использования средств защиты информации (далее – СЗИ) – систем защиты информации от НСД.

12.2. СЗИ являются важным компонентом обеспечения безопасности персональных данных.

12.3. Порядок работы с СЗИ определен в соответствующих руководствах по настройке и использованию СЗИ обязательных для исполнения, как сотрудниками обрабатывающими персональные данные, так и администратором безопасности информации ИСПДн.

12.4. Право проверки соблюдения условий использования средств защиты информации имеют:

– Руководитель Администрации;

– ответственный за обеспечение безопасности персональных данных;

– администратор безопасности информации.

12.5. Пользователю ИСПДн категорически запрещается:

– обрабатывать персональные данные с отключенными СЗИ;

– изменять настройки СЗИ.

12.6. В ИСПДн должны быть выполнены все требования приказа № 21 от 18 февраля 2013 года ФСТЭК России и руководящего документа ФСТЭК России (Гостехкомиссии России) «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» применительно к установленному классу защищенности АС и ИСПДн.

12.7. Администратору безопасности информации запрещается изменять настройки СЗИ без согласования со специалистами организаций, проводившей аттестацию конкретной ИСПДн.

13. ПОРЯДОК ОХРАНЫ И ДОПУСКА ПОСТОРОННИХ ЛИЦ В СЛУЖЕБНЫЕ ПОМЕЩЕНИЯ, ГДЕ ОСУЩЕСТВЛЯЕТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

13.1. Настоящее Положение устанавливает порядок охраны (сдачи под охрану) служебных помещений, где осуществляется обработка персональных данных (далее – служебные помещения).

13.2. Вскрытие и закрытие служебных помещений осуществляется сотрудниками, работающими в данных помещениях.

13.3. Список сотрудников, имеющих право вскрывать (сдавать под охрану) служебные помещения утверждается Руководителем Администрации.

13.4. При отсутствии сотрудников, ответственных за вскрытие (сдачу под охрану) помещений, данные помещения могут быть вскрыты другим сотрудником Администрации под роспись в соответствующем Журнале.

13.5. При закрытии служебных помещений и сдачей их под охрану сотрудники, ответственные за данные помещения проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и машинные носители, содержащие персональные данные, убираются для хранения в сейф (металлический шкаф).

13.6. Служебные помещения сдаются под охрану следующим образом:

– служебное помещение закрывается на ключ, ключ от данного помещения убирается в пенал, который сдается на пост охраны;

– после передачи ключей, сотрудник делает соответствующую запись в Журнале.

13.7. Сотрудник, имеющий право на вскрытие помещений:

– получает на посту охраны пенал с ключами от служебного помещения под роспись в Журнале;

– вскрывает служебное помещение.

13.8. При обнаружении нарушений целостности дверей, повреждения запоров или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт, в присутствии охранника. О происшествии немедленно сообщается Руководителю Администрации.

Одновременно принимаются меры по охране места происшествия и до прибытия должностных лиц в помещение никто не допускается.

13.9. Руководитель подразделения, ответственный за обеспечение безопасности персональных данных и администратор безопасности информации организуют проверку ИСПДн на предмет несанкционированного доступа к персональным данным и наличие документов и машинных носителей информации.

13.10. При срабатывании охранной сигнализации в служебных помещениях в нерабочее время охранник сообщает о случившемся ответственному за помещение, руководителю подразделения, ответственному за обеспечение безопасности персональных данных или администратору безопасности информации.

13.11. Помещения вскрываются ответственным за помещение, руководителем подразделения, ответственным за обеспечение безопасности персональных данных и администратором безопасности информации в присутствии сотрудника охраны с соответствующей записью в Журнале.

Если обнаружено вторжение в служебное помещение, далее процедура происходит в соответствии с п. 13.8 настоящего Положения.

14. ПОРЯДОК СТИРАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ И УНИЧТОЖЕНИЯ МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

14.1. В обязательном порядке уничтожению подлежат поврежденные, выводимые из эксплуатации носители, содержащие персональные данные, использование которых не предполагается в дальнейшем. Не допускается передача неисправных носителей в сервисный центр для ремонта. Такие носители должны уничтожаться в соответствии с «Инструкцией о порядке технического обслуживания, модернизации и ремонта технических средств, при обработке персональных данных …».

14.2. Стирание должно производиться по технологии, предусмотренной для данного типа носителя, с применением средств гарантированного уничтожения информации (допускается задействовать механизмы затирания встроенные в средства защиты информации).

14.3. Уничтожение носителей производится путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления информации (перед уничтожением, если носитель исправен, должно быть произведено гарантирование стирание информации на носителе). Непосредственные действия по уничтожению конкретного типа носителя должны быть достаточны для исключения возможности восстановления персональных данных.

14.4. Бумажные и прочие сгораемые носители уничтожают путем сжигания или с помощью бумагорезательных машин.

14.5. Процедуры стирания и уничтожения осуществляются комиссией, в которую входят: исполнитель документа или файла, ответственный за обеспечение безопасности персональных данных и администратором безопасности информации.

15. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

16.1. Требования настоящего Положения обязательны для всех сотрудников обрабатывающих персональные данные.

16.2. Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение 1
Титульный лист

ТИПОВАЯ ФОРМА

Автоматизированная система журнала учета инцидентов информационной безопасности

г. Руза
2014г.

№ п/п	Дата, время и длительность инцидента ИБ	Краткое описание инцидента ИБ. Результаты анализа, причина инцидента ИБ	Версии ОС и IP-адреса атакованной системы. Имя и местоположение атакованной системы/систем. Тип атакованной системы	Контактная информация работника, обнаружившего инцидент	Решение ответственного за эксплуатацию по факту инцидента ИБ, его подпись, дата и время	Контактная информация работника ПЗКИ, ответственного за управление инцидентом	Описание возможных последствий инцидента	Принятые меры
1.								
2.								
3.								
4.								