ЛАНГЕПАССКОЕ ГОРОДСКОЕ МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ
ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА №3
(ЛГ МАОУ «СОШ №3»)
ул. Мира 21, г. Лангепас, Тюменская обл., 628672
тел.: (34669) 2-68-35, факс: (34669) 2-17-86 e-mail: shkola3L@mail.ru

СОГЛАСОВАНО
Председатель ППО ЛГ МАОУ «СОШ №3»
_____ О.А. Сырцова
29 декабря 2018г.

УТВЕРЖДАЮ
Директор ЛГ МАОУ «СОШ №3»
_____С.Н.Кононова
29 декабря 2018г

ПОЛОЖЕНИЕ ПО ОРГАНИЗАЦИИ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

СОГЛАСОВАНО
Педагогическим советом
ЛГ МАОУ «СОШ №3»
(протокол от 29 .12. 2018 №4)

г.Лангепас – 2018

УТВЕРЖДЕНО
приказом ЛГ МАОУ «СОШ №3»
от 29.12.2018. № 1090-О

ПОЛОЖЕНИЕ ПО ОРГАНИЗАЦИИ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

(предыдущая редакция: приказ от 09.01.17 №06-0)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение разработано на основании Конституции РФ и в соответствии с требованиями Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных», Постановления Правительства РФ от 21.03.2012 N 211"Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами".

1.2. Положение определяет основные мероприятия и порядок проведения работ по обеспечению безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн) ЛГ МАОУ «СОШ № 3» *(далее –Организация)*.

1.3. В Организации обработка ПДн осуществляется в следующих информационных системах (далее - ИС):

- *АВЕРС: АРМ-К СОШ№3;*
- *1С:Зарплата.Кадры;*
- *1С:Бухгалтерия.*

1.4. Все работники Организации, участвующие в обработке ПДн в ИС Организации, должны быть ознакомлены с Положением.

2. ПОРЯДОК ОРГАНИЗАЦИИ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. С целью организации работ по защите ПДн должностное лицо, ответственное за обеспечение безопасности ПДн (*далее администратор ИБ*) назначается *приказом директора ЛГ МАОУ «СОШ №3»*.

2.2. В обязанности ответственного за обеспечение безопасности ПДн входит:

- контроль и организация работ по обеспечению безопасности ПДн;
- утверждение организационно-распорядительных документов по вопросам обеспечения безопасности ПДн;
- утверждение списка лиц, которым необходим доступ к ПДн для выполнения служебных обязанностей;
- утверждение списка лиц, которым разрешены действия по внесению изменений в базовую конфигурацию ИС и системы защиты ПДн (далее – СЗПДн) Организации;
- утверждение базовой конфигурации ИС и СЗПДн Организации;
- проведение разбирательств по фактам возникновения событий, которые могут привести к снижению уровня защищенности ПДн.

2.3. Реализация требований по обеспечению безопасности ПДн осуществляется администраторами, разработчиками и пользователями информационных систем Организации.

3. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Требования по обеспечению безопасности ПДн при их обработке в ИС Организации формируются на основании установленного уровня защищенности ИСПДн и перечня актуальных угроз безопасности ПДн.

3.2. Требования по обеспечению безопасности ПДн при их обработке в ИСПДн реализуются комплексом организационных и технических мер, средств и механизмов защиты информации, определенных в Техническом задании на создание СЗПДн.

3.3. Применение средства защиты информации разрешается после проверки корректности его функционирования и оформления заключения о готовности средства защиты информации к эксплуатации (форма заключения приведена в приложении №1). Применяемые средства защиты информации, эксплуатационная и техническая документация к ним подлежат обязательному учету (форма журнала учета средств защиты информации, эксплуатационной и технической документации приведена в приложении №2).

3.4. Требования по обеспечению безопасности ПДн при их обработке в ИСПДн Организации реализуются в рамках следующих направлений:

- организация системы допуска и учета лиц, допущенных к работе с ПДн;
- организация системы защиты межсетевого взаимодействия;
- организация режима безопасности помещений ИСПДн;
- организация безопасного хранения и уничтожения носителей ПДн;
- организация защиты от вредоносного кода;
- организация парольной защиты;
- организация управления инцидентами информационной безопасности и реагирования на них;
- организация управления конфигурацией ИСПДн и СЗПДн Организации;
- организация системы криптографической защиты информации;
- организация системы резервного копирования и восстановления;
- организация управления СЗПДн Организации;
- организация контроля эффективности мер защиты ПДн;
- организация системы обучения по вопросам обеспечения безопасности ПДн.

4. СИСТЕМА ДОПУСКА И УЧЕТА ЛИЦ

4.1. Ответственным за организацию системы допуска к ПДн является ответственный за обеспечение безопасности ПДн.

4.2. Работники Организации допускаются к обработке ПДн в ИСПДн, использование которых необходимо для выполнения их функциональных обязанностей.

4.3. Приказом директора Организации утверждается Перечень ПДн, обрабатываемых в Организации. Обработка ПДн, не включенных в Перечень, не допускается.

4.4. Перечень определяется и пересматривается в установленном в Организации порядке не реже, чем один раз в три года.

4.5. Доступ работников Организации к ПДн, обрабатываемым в ИСПДн Организации, определяется перечнем подразделений, работники которых имеют доступ к ПДн, утверждаемым приказом по Обществу.

4.6. Права доступа пользователей ИСПДн Организации определяются в соответствии с Матрицами доступа, разрабатываемыми администратором ИБ для каждой ИСПДн Организации.

4.7. Управление учетными записями пользователей и распределение прав доступа к информационным ресурсам ИСПДн Организации, внешним носителям информации и периферийным устройствам осуществляется администратором ИСПДн Организации, назначаемым приказом директора Организации.

4.8. Общий порядок предоставления доступа, изменения и отмены доступа к информационным ресурсам ИСПДн Организации устанавливается организационно-распорядительными документами Организации.

4.9. Администратор ИБ осуществляет оценку необходимости запрашиваемого уровня доступа к ПДн.

4.10. Администратор ИБ осуществляет учет лиц, допущенных к работе с ПДн в ИСПДн Организации.

4.11. Администратор ИБ осуществляет контроль за своевременным блокированием доступа (изменением прав доступа) при увольнении пользователя ИСПДн Организации(изменении должностных обязанностей).

4.12. В пределах контролируемой зоны Организации запрещено подключение к корпоративной информационной сети мобильных технических средств, портативных рабочих станций и внешних носителей информации.

4.13. Подключение к корпоративной информационной сети указанных устройств допускается только при наличии согласования с ответственным по защите информации.

5. СИСТЕМА ЗАЩИТЫ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

5.1. Обеспечение защиты межсетевого взаимодействия реализуется по следующим направлениям:

- выделение сетевых сегментов обработки ПДн в корпоративной информационной сети Организации;
- межсетевое экранирование выделенных сегментов обработки ПДн Организации;
- разграничение доступа пользователей к ресурсам сетей общего пользования.

5.2. В корпоративной информационной сети Организации должны быть выделены:

- сегменты серверов ИСПДн;
- сегменты пользователей ИСПДн;
- сегмент локальной вычислительной сети (далее – ЛВС) Организации;
- сегмент СЗПДн.

5.3. Включение новых серверов и рабочих станций в сегменты ИСПДн должно осуществляться только после выполнения требований по защите ПДн.

5.4. Доступ к сегментам ИСПДн из других сегментов корпоративной информационной сети Организации должен ограничиваться межсетевыми экранами.

5.5. Межсетевое экранирование сегментов ИСПДн Организации должно обеспечивать:

- фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
- регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратного отключения межсетевого экрана);
- восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
- защиту беспроводных соединений, применяемых в ИСПДн.

5.6. Межсетевое экранирование должно обеспечивать отделение ЛВС и сети среды виртуализации от сетей связи общего пользования.

5.7. Серверы, доступные из сетей связи общего пользования, должны быть размещены в выделенном сегменте демилитаризованной зоны. Доступ к таким серверам из сетей связи общего пользования разрешается только по необходимым сетевым портам.

5.8. Используемые межсетевые экраны должны быть сертифицированы в соответствии с требованиями к средствам межсетевого экранирования, установленными Приказом ФСТЭК России № 21 от 18.02.2013.

5.9. Управление сетевым оборудованием Организации осуществляется системными администраторами.

5.10. Внесение изменений в правила межсетевого экранирования осуществляется системными администраторами по согласованию администратором сети.

5.11. Доступ к сетевому оборудованию разрешен только с рабочих станций системных администраторов либо локально.

5.12. В случае производственной необходимости пользователям ИСПДн Организации может предоставляться доступ:

- к сети Интернет;

– к сервисам внешней электронной почты.

5.13. Правила работы пользователей ИСПДн с ресурсами сети Интернет и электронной почты устанавливаются организационно-распорядительными документами Организации.

6. РЕЖИМ БЕЗОПАСНОСТИ ПОМЕЩЕНИЙ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Обеспечение безопасности помещений ИСПДн направлено на исключение возможности несанкционированного доступа к техническим средствам ИСПДн, их хищения и нарушения работоспособности, хищения носителей информации.

6.2. Приказом директора Организации определяются границы контролируемой зоны Организации, на территории которой исключено бесконтрольное пребывание посторонних лиц.

6.3. Режим безопасности помещений ИСПДн реализуется в соответствии с Положением об организации режима безопасности помещений ИСПДн.

6.4. Реализация режима безопасности помещений ИСПДн возлагается на лица, работающие в данных помещениях.

7. БЕЗОПАСНОСТЬ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Безопасность информации, хранящейся на бумажных и отчуждаемых электронных носителях ПДн, обеспечивается путем организации системы учета и безопасного хранения носителей ПДн.

7.2. Ответственным за учет и соблюдение условий хранения электронных носителей ПДн является администратор ИБ.

7.3. Порядок учета, хранения и уничтожения носителей ПДн регламентируется Положением об учете, порядке хранения и уничтожения носителей ПДн.

7.4. При уничтожении носителя ПДн должны обеспечиваться и контролироваться гарантированное уничтожение (стирание) ПДн.

8. ЗАЩИТА ОТ ВРЕДОНОСНОГО КОДА

8.1. Средства защиты от вредоносного кода должны быть установлены на всех рабочих станциях и серверах Организации.

8.2. Средства защиты от вредоносного кода должны обеспечивать:

- автоматическое блокирование или удаление обнаруженного вредоносного программного обеспечения;
- регулярную проверку программных модулей рабочих станций и серверов ИСПДн Организациина предмет наличия в них вредоносного программного обеспеченияпо типовым шаблонам и с помощью эвристического анализа;
- возможность отката операций удаления вредоносного программного обеспечения путем помещения файлов, содержащих вредоносное программного обеспечение, в карантин;
- своевременное обновление антивирусных баз (сигнатур угроз) и программных модулей.

8.3. При выявлении фактов заражения вредоносным программным обеспечением ответственным за обеспечение безопасности ПДн проводится разбирательство с целью установления причин возникновения заражения.

8.4. Обязанности по устранению последствий заражения вредоносным программным обеспечением возлагаются на администратора ИБ.

9. ПАРОЛЬНАЯ ЗАЩИТА

9.1. Парольная защита применяется для исключения возможности получения несанкционированного доступа к элементам ИСПДн Организации (рабочим станциям, серверам, активному сетевому оборудованию) в целях не допущения утечки, а также несанкционированной модификации или уничтожения ПДн.

9.2. Парольная защита применяется:

– при доступе пользователей к операционным системам рабочих станций и серверов, прикладному программному обеспечению ИСПДн Организации, средствам защиты информации;
– при доступе системных администраторов к средствам управления сетевым и серверным оборудованием, операционным системам серверов и рабочих станций, специальному программному обеспечению ИСПДн Организации, средствам защиты информации.

9.3. Требования парольной защиты определяются организационно-распорядительными документами Организации.

9.4. При выявлении фактов нарушения требований парольной защиты ответственным за обеспечение безопасности ПДн проводится разбирательство.

10. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РЕАГИРОВАНИЕ НА НИХ

10.1. Для регистрации и учета событий, которые могут привести к снижению уровня защищенности ПДн (далее – инцидентов), должны использоваться встроенные механизмы регистрации и учета событий безопасности операционных систем, систем управления базами данных, прикладного программного обеспечения и средств защиты информации, а также применяться средства (системы) анализа защищенности.

10.2. Средства (системы) анализа защищенности должны обеспечивать, в том числе:
– выявление и анализ уязвимостей, связанных с ошибками в конфигурации операционных систем и программного обеспечения рабочих станций и серверов ИСПДн Организации;
– контроль установки обновлений программного обеспечения рабочих станций и серверов ИСПДн Организации.

10.3. В Организации должен быть обеспечен контроль заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в ИСПДн Организации.

10.4. Анализ инцидентов осуществляется:
– администратором ИБ при просмотре журналов событий, формируемых средствами защиты информации;
– администратором ИСПДн при просмотре журналов событий, формируемых программным обеспечением ИСПДн и системами управления базами данных;
– системными администраторами при просмотре журналов событий сетевого и серверного оборудования, операционных систем и системного программного обеспечения.

10.5. Журналы аудита должны просматриваться ответственными работниками регулярно (не реже одного раза в месяц).

10.6. О фактах обнаружения инцидентов ответственные работники должны немедленно сообщать администратору ИБ.

10.7. Права доступа на модификацию и удаление журналов событий безопасности должны быть ограничены для всех пользователей ИСПДн Организации.

11. СИСТЕМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

11.1. Система криптографической защиты информации предназначена для криптографической защиты информации, передаваемой по каналам связи, расположенным вне контролируемой зоны Организации.

11.2. Криптографическая защита должна реализовываться алгоритмами, определяемыми ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001 с применением программно-технических средств шифрования и/или специального прикладного программного обеспечения, сертифицированных в установленном порядке ФСБ России.

11.3. Эксплуатация СКЗИ должна осуществляться в полном соответствии с эксплуатационной и технической документации к ним.

11.4. Допуск работников Организации к работе с СКЗИ должен осуществляться в соответствии со списком лиц, допущенных к СКЗИ, утвержденным ответственным за обеспечение безопасности ПДн.

11.5. Допуск работников Организации к работе с СКЗИ должен осуществляться после проведения администратором ИБ обучения и ознакомления с требования по работе с СКЗИ.

11.6. Администратор ИБ должен вести учет используемых СКЗИ, технической и эксплуатационной документации к ним в Журнале учета СКЗИ и Журнале учета приема-выдачи СКЗИ.

11.7. Контроль выполнения требований по эксплуатации СКЗИ осуществляет администратор ИБ. При выявлении фактов нарушения требований по эксплуатации СКЗИ ответственным за обеспечение безопасности ПДн проводится разбирательство.

11.8. Порядок использования СКЗИ в Организации определяется Положением о контроле использования СКЗИ.

12. ОРГАНИЗАЦИЯ СИСТЕМЫ РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ

12.1. Для обеспечения возможности восстановления функционирования и работоспособности ИСПДн Организации и средств защиты информации при возникновении аварийных ситуаций должна быть реализована система резервного копирования и восстановления.

12.2. Резервному копированию подлежит информация следующих основных категорий:

- ПДн, хранящиеся в виде отдельных файлов, каталогов или баз данных ИСПДн;
- системные и конфигурационные файлы операционных систем и специального программного обеспечения серверов;
- конфигурационные файлы сетевого оборудования;
- системные и конфигурационные файлы средств защиты информации.

12.3. Ответственными за осуществление резервного копирования являются системные администраторы соответствующих информационных ресурсов.

12.4. Требования к периодичности и способам осуществления резервного копирования информационного ресурса определяются особенностями функционирования соответствующего информационного ресурса.

12.5. Администратор ИБ должен осуществлять регулярные проверки выполнения требований резервного копирования информационных ресурсов.

13. УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ И СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

13.1. В Организации должно обеспечиваться управление конфигурацией ИСПДн и СЗПДн Организации.

13.2. В Организации допускается использование ограниченного набора программного обеспечения (ПО), формирующего базовую конфигурацию ИСПДн Организации.

13.3. Состав базовой конфигурации ПО на рабочих станциях и серверах ИСПДн Организации утверждается приказом директора Организации (форма состава базовой конфигурации ПО приведена в приложении №3). Установка на рабочих станциях и серверах ИСПДн Организации ПО, не входящего в состав разрешенного ПО, не допускается.

13.4. Состав базовой конфигурации ПО СЗПДн Организации устанавливается эксплуатационной документацией на СЗПДн Организации.

13.5. При первоначальной настройке рабочих станций и серверов системными администраторами производится установка ПО на основании перечня разрешенного ПО.

13.6. Пересмотр базовой конфигурации осуществляется администратором ИБ при возникновении необходимости по согласованию с ответственным за обеспечение безопасности ПДн. Пересмотренная базовая конфигурация доводится до сведения всех работников Организации путем рассылки по электронной почте с обязательным запросом уведомления о прочтении письма.

13.7. Внесение изменений в конфигурацию ИСПДн Организации осуществляется на основании заявки заинтересованного лица, согласованной с руководителем структурного подразделения (форма заявки приведена в приложении №4).

13.8. При согласовании внесения изменений в конфигурацию ИСПДн Организации администратору ИБ необходимо учитывать потенциальное воздействие планируемых изменений на возникновение дополнительных угроз безопасности информации и на работоспособность ИСПДн Организации.

13.9. ПО, используемое в ИСПДн Организации, должно регулярно обновляться. Получение обновлений должно осуществляться из официальных источников производителя ПО. Получение обновлений ПО сертифицированных средств защиты информации должно осуществляться из специализированных источников обновления производителей средств в соответствии с эксплуатационной документацией к ним.

13.10. ПО, используемое на Предприятии, приобретается в соответствии с лицензионной политикой разработчика.

13.11. Установка обновлений ПО не считается внесением изменений в конфигурацию ИСПДн и СЗПДн Организации и не требует заполнения заявки на внесение изменений.

14. УПРАВЛЕНИЕ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

14.1. СЗПДн должна обеспечивать управление:

- заведением и удалением учетных записей пользователей, полномочиями пользователей и поддержанием правил разграничения доступа в ИСПДн Организации;
- резервным копированием и восстановлением работоспособности ИСПДн и СЗПДн Организации;
- обновлением программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации;
- регистрацией и анализом инцидентов ИБ.

14.2. Администрирование СЗПДн осуществляет администратор ИБ.

15. КОНТРОЛЬ ПРИНЯТЫХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

15.1. Ответственным за контроль выполнения принятых мер по обеспечению безопасности ПДн является ответственный за обеспечение безопасности ПДн.

15.2. Администратор ИБ осуществляет постоянный контроль выполнения требований по обеспечению безопасности ПДн в рамках выполнения своих обязанностей.

15.3. Мероприятия по контролю мер выполнения требований по обеспечению безопасности ПДн проводятся в соответствии с Планом внутренних проверок, утвержденным приказом директора Организации.

15.4. Контроль эффективности мер защиты информации должен осуществляться в соответствии с Положением по организации контроля эффективности защиты информации.

16. ОБУЧЕНИЕ ПО ВОПРОСАМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

16.1. Администратор ИБ должен регулярно проходить обучение на курсах повышенияквалификации по вопросам защиты информации (не реже одного раза в три года).

16.2. Ознакомление работников Организации с правилами работы с ПДн осуществляется:

- путем проведения руководителем структурного подразделения Организации, в которое принят работник, первичных инструктажей с вновь принятым работником Организации по соблюдению установленныхправил работы с ПДн;
- путем проведения обучения работников (пользователей средств вычислительной техники) администратором ИБ правилам работы с используемыми средствами защиты информации и СКЗИ;

- путем самостоятельного изучения работником Организации организационно-распорядительных документов, регламентирующих вопросы обеспечения безопасности ПДн.

16.3. Допуск работников Организации к ресурсам ИСПДн осуществляется только после прохождения первичного инструктажа и ознакомления с организационно-распорядительными документами Организациипо вопросам обеспечения безопасности ПДн.

16.4. При проведении первичного инструктажа нового пользователя ИСПДн должны быть разъяснены:

- права и обязанности пользователя ИСПДн;
- действия, которые запрещены при обработке ПДн;
- возможные последствия и ответственность в случае нарушения правил работы с ПДн.

Приложение №1
к Положению по организации работ
по обеспечению безопасности персональных данных
при их обработке в информационных системах персональных данных

Заключение
о готовности средства защиты информации

_____

к эксплуатации в информационной системе персональных данных

«_____»

В соответствии с Приказом руководителя *ЛГ МАОУ «СОШ №3»* от «___» _____20___ г.
Комиссия в составе
Председателя _____
(должность, ФИО)
и членов: _____
(должность, ФИО)
_____
(должность, ФИО)
_____
(должность, ФИО)

провела проверку корректности функционирования средства защиты информации
«_____»
в информационной системе персональных данных «_____
_____»
и установила:
1) Установка и настройка средства защиты информации произведена в соответствии с эксплуатационной документацией.
2) Средство защиты информации выполняет следующие функции:
– _____;
– _____;
– _____.
3) Средство защиты информации не нарушает функционирование информационной системы персональных данных.
По результатам оценки признать средство защиты информации
«_____»
готовым к эксплуатации в информационной системе персональных данных
«_____».
Ввести средство защиты информации
«_____»
в постоянную эксплуатацию с «___» _____ 20___г.
Председатель комиссии _____ /_____/
Члены комиссии _____ /_____/
_____ /_____/
_____ /_____/

«___» _____ 20___г.

Регистрационный №_____

Приложение №2
к Положению по организации работ
по обеспечению безопасности персональных данных
при их обработке в информационных системах персональных данных

ЖУРНАЛ УЧЕТА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ, ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ, ИСПОЛЬЗУЕМЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Начат «___»_____20__ г.

Окончен «___»_____20__ г.

На _____листах

_____ _____ _____
(должность руководителя) (подпись) (Фамилия И.О.)

Журнал учета средств защиты информации, эксплуатационной и технической документации к ним,
используемых в информационной системе персональных данных стр._____

№ п/п	Индекс и наименование средства защиты информации (наименование эксплуатационной/ технической документации)	Серийный (заводской) номер	Номер специального защитного знака	Наименование организации, установившей средство защиты информации	Примечание (данные о сертификате, ФИО и подпись ответственного)
1					
2					
3					
4					
5					
6					
7					
8					
9					

Приложение №3
к Положению по организации работ
по обеспечению безопасности персональных данных
при их обработке в информационных системах персональных данных

ФОРМА
перечня разрешенного к использованию программного обеспечения

Категория ПО	**Необходимость установки**	
	Обязательное	**Дополнительное**
Платное	– MS Windows 7 enterprise sp1(x64); – MS office 2003 (2007, 2010); – …	– «Консультант Плюс»; – Собственный клиент MS SQL 2008; – …
Бесплатное	– 7 zip; – Acrobate reader 10.x; – …	– Punto switcher; – ООО «ДубльГИС» (различные города); – бесплатные программы для работы с фото/ аудио и мобильными устройствами, которые поставляются на носителях с устройствами; – …

Приложение №4
к Положению по организации работ
по обеспечению безопасности персональных данных
при их обработке в информационных системах персональных данных

Администратору информационной безопасности
информационных систем персональных данных

_____
(ФИО)

От _____
(Фамилия)

_____
(Имя, Отчество)

_____
(наименование должности)

_____
(структурное подразделение)

заявление.

Прошу Вас внести изменения в конфигурацию

_____
(наименование и место установки рабочей станции / сервера)

в соответствии с прилагаемой таблицей.

«_____» _____ 201__ г. _____
(подпись)

СОГЛАСОВАНО
Руководитель структурного подразделения:

_____	_____	_____
(ФИО)	(подпись)	(дата)

ОТМЕТКА О ВЫПОЛНЕНИИ
Системный администратор

_____	_____	_____
(ФИО)	(подпись)	(дата)

Таблица 1 – Перечень необходимых изменений конфигурации рабочей станции / сервера

№ п/п	Наименование информационного ресурса/сервиса	Изменение	Обоснование
1.			
2.			
3.			
4.			