


УТВЕРЖДАЮ

Глава Валдайского
муниципального района
(руководитель)

 (Ю.В. Стадэ)
«31» января 2019г

**ОПИСАНИЕ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА
ОБРАБОТКИ ИНФОРМАЦИИ СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ В
АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ АДМИНИСТРАЦИИ ВАЛДАЙСКОГО
МУНИЦИПАЛЬНОГО РАЙОНА**

1. Перечень использованных сокращений, единиц и терминов

АИБ	– администратор информационной безопасности.
АС	– автоматизированная система.
АРМ	– автоматизированное рабочее место.
ИСПДн	– информационная система персональных данных.
ЛВС	– локальная вычислительная сеть.
МНИ	– отчуждаемые машинные носители информации.
МЭ	– межсетевой экран.
НСД	– несанкционированный доступ.
ОИ	– объект информатизации.
ОС	– операционная система.
ПДн	– персональные данные
ПО	– программное обеспечение.
ПЭВМ	– персональная электронно-вычислительная машина.
СЗИ	– средство защиты информации.
ЭВМ	– электронно-вычислительная машина.

Описание технологического процесса обработки информации содержащие персональные данные в автоматизированной системе Администрации Валдайского муниципального района (далее Администрация, разработано в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»).

Для целей настоящего Описания используются следующие основные понятия:

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

Администратор сети – сотрудник или группа сотрудников, который выполняет функции администратора информационной безопасности, осуществляющие непосредственную организацию и выполнение работ по созданию (модернизации), техническому обслуживанию и управлению (администрированию) информационной управляющей ЛВС, включая технические аспекты информационной безопасности.

Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. Чаще всего аутентификация выполняется путем набора пользователем своего пароля на клавиатуре компьютера.

Идентификация - присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Администратор информационной безопасности – специалист или группа специалистов, осуществляющие контроль за обеспечением защиты информации в ЛВС, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

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

Информационная безопасность – состояние защищенности информационной среды, обеспечивающее ее формирование, использование и развитие в организации.

Информационная система - совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения различных задач подразделений. В организации используются различные типы информационных систем для решения различных задач.

Информационные ресурсы – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий, используемая в процессах организации.

Локальная вычислительная сеть (ЛВС) - группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

Межсетевой экран (МЭ) - программно-аппаратный комплекс, используемый для контроля доступа между ЛВС, входящими в состав корпоративной сети, а также между корпоративной сетью и внешними сетями (сетью Интернет).

Несанкционированный доступ к информации (НСД) – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Операционная система – системная программа, осуществляющая взаимодействие пользователя и прикладных программ с аппаратной частью ЭВМ.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

Пароль – идентификатор субъекта доступа, который является его (субъекта) секретом.

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

Пользователь ЛВС – сотрудник Комитета (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированный в корпоративной сети в установленном порядке и получивший права на доступ к ресурсам корпоративной сети в соответствии со своими функциональными обязанностями.

Программное обеспечение – совокупность прикладных программ, установленных на сервере или ЭВМ.

Рабочая станция – персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.

Сервер – выделенный компьютер, имеющий разделяемые ресурсы, выполняющий определенный перечень задач и предоставляющий пользователям ЛВС ряд сервисов.

Структурное подразделение – структурное подразделение Администрации с самостоятельными функциями, задачами и ответственностью.

2. Назначение и задачи применения АС

2.1. АС Администрации предназначена для обработки, распечатки, хранения в электронном виде ПДн.

С документами, содержащими сведения о персональных данных, работают сотрудники Администрации, имеющие соответствующий доступ к ресурсам ИСПДн.

Технологический процесс обработки информации в ИСПДн включает в себя:

– внесение ПДн в базы данных, просмотр и редактирование необходимой информации, печать документов на бумажном носителе;

– обеспечение необходимого уровня безопасности обработки, хранения и передачи ПДн.

2.2. Задачами применения ИСПДн являются:

- работа с базами данных ПДн, внесение в них изменений, их хранение и уничтожение;
- распечатка документов, содержащих ПДн;
- размножение необходимого числа экземпляров документов на принтере;
- обеспечение необходимого уровня безопасности обработки, хранения ПДн;
- обеспечение в ИСПДн разграничения доступа к ПДн;
- антивирусная защита программной среды и данных;
- регистрация пользователей СЗИ от НСД перед началом сеанса работы на ПЭВМ, входящей в состав ИСПДн, назначение им прав доступа к защищаемым ресурсам;
- резервное копирование информации осуществляется средствами ОС Windows путем копирования информации на несъемный жесткий диск, в соответствии с «Регламентом резервного копирования и восстановления персональных данных» утвержденного распоряжением Администрации Валдайского муниципального района от 26.04.2012 № 154-рг;
- восстановление информации, поврежденной или стертой при сбоях в работе ПЭВМ с резервных копий.

3. Расположение ОИ. Организация охраны и контроля доступа

ИСПДн, обрабатывающие ПДн, расположены в здании по адресу: г. Валдай, пр-т Комсомольский, д.19/21.

Доступ сотрудников и других лиц в помещения Администрации, в которых осуществляется обработка ПДн, осуществляется в соответствии с «Порядком доступа лиц, замещающих муниципальные должности, муниципальных служащих, служащих Администрации Валдайского муниципального района и других лиц в помещения, в которых ведется обработка персональных данных» утвержденного постановлением Администрации Валдайского муниципального района от 08.02.2017 № 133.

4. Состав АС, обрабатывающей ПДн

В состав ИСПДн Администрации, обрабатывающей ПДн, входят 12 АРМ, которые функционируют в рамках локальной сети, и имеют подключение к сети Интернет.

Питание ПЭВМ и принтера обеспечивается от сети электропитания 220В. Трансформаторная подстанция находится за пределами контролируемой зоны. К трансформаторной подстанции подключены сторонние потребители. Контур заземления оборудован в непосредственной близости от здания.

5. Источники данных АС

5.1. Источниками данных для ИСПДн Администрации являются:

- Данные на бумажных носителях.
- Вводимые пользователями данные - сведения, вводимые с клавиатуры операторами (пользователями).

5.2. Входными данными является информация, поступающая в ИСПДн на различных носителях: данные на бумажных носителях, данные поступающие по средствам межведомственного взаимодействия, данные, вводимые операторами (пользователями) с клавиатуры.

Исходные данные поступают в ИСПДн Администрации от сотрудников, сторонних организаций и клиентов, обращающихся в Администрацию.

ОПИСАНИЕ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ОБРАБОТКИ ИНФОРМАЦИИ

Все носители информации регистрируются, хранятся и передаются в соответствии с требованиями инструкции по обращению с носителями ПДн и Административными регламентами оказания государственных (муниципальных) услуг.

5.2. Выходными данными являются подготовленные и распечатанные в ИСПДн конфиденциальные и не конфиденциальные текстовые документы, файлы, содержащие ПДн, передаваемые по каналам связи.

6. Используемые программные средства

На ПЭВМ Администрации установлены ОС Windows 7 Pro, дистрибутивы версии ОС хранятся у АИБа.

Функции, права и обязанности, ответственных за эксплуатацию объекта информатизации регламентируются инструкцией о порядке технического обслуживания, ремонта, модернизации технических средств, входящих в состав ИСПДн.

Разрешенное к использованию ПО указывается в перечне разрешенного к использованию в ИСПДн ПО (указано в Техническом паспорте на АС Администрации), который разрабатывается АИБом совместно с системным администратором. Пользователям запрещено приносить и устанавливать на рабочие станции ИСПДн ПО без согласования с АИБом.

7. Ресурсы АС

К ресурсам ИСПДн Администрации относятся файлы, каталоги, тома, диски, устройства вывода информации (CD-RW, COM и LPT порты, порты USB).

Информационные ресурсы, предназначенные для хранения и обработки ПДн, перечислены в утвержденном перечне защищаемых информационных ресурсов.

Разграничение доступа пользователей к портам ввода-вывода информации в ИСПДн Администрации реализовано в разрешительной системе доступа.

Если доступ пользователя к конкретному информационному ресурсу не определен, то доступа к нему он не имеет.

Запрещается хранить ПДн на ресурсах, отличных от перечисленных в утвержденном перечне защищаемых ресурсов.

8. Антивирусная защита

Антивирусная защита осуществляется с применением разрешенных программных средств в соответствии с инструкцией по проведению антивирусного контроля в ИСПДн.

Используемые антивирусные средства указываются в Перечне разрешенного к использованию в ИСПДн программного обеспечения.

9. Обеспечение безопасности информации

Оператор должен обеспечивать надлежащие условия защиты ПДн, хранящихся в используемых ИСПДн, от несанкционированного доступа, использования, распространения, искажения и уничтожения. Сотрудники, уполномоченные осуществлять обработку персональных данных, несут ответственность за защиту ПДн в порядке, предусмотренном действующим законодательством Российской Федерации.

Настройку СЗИ от НСД для конкретных пользователей, контроль её работы, обновление антивирусных баз, диагностику и устранение неисправностей или сбоев в работе программного или аппаратного обеспечения осуществляет АИБ.

Функции, права, обязанности АИБа, а также порядок ремонта и модернизации регламентируются специально разработанными инструкцией о порядке технического

ОПИСАНИЕ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ОБРАБОТКИ ИНФОРМАЦИИ

обслуживания, ремонта, модернизации технических средств, входящих в состав ИСПДн и должностной инструкцией АИБа.

Повседневный контроль защищенности ИСПДн от НСД проводится АИБом. Контроль осуществляется с помощью штатных средств СЗИ от НСД. Основным средством контроля является анализ системного журнала.

Доступ пользователей к работе в ИСПДн осуществляется строго в соответствии со списком постоянных пользователей ИСПДн, разрабатываемым АИБом и ответственным лицом за организацию обработки персональных данных в Администрации Валдайского муниципального района.

Допускается наличие только пользователей, указанных в списке постоянных пользователей ИСПДн, имеющих доступ к ПДн.

Порядок работы пользователя определены в «Инструкции по работе пользователей информационной системы персональных данных» утвержденной распоряжением Администрации Валдайского муниципального района от 26.04.2012 № 154-рг

10. Пользователи

Пользователями ИСПДн являются сотрудники Администрации строго в соответствии со списком постоянных пользователей ИСПДн, имеющими соответствующие права допуска. В рамках управления доступом пользователей ИСПДн к ресурсам ИСПДн и в соответствии с решаемыми задачами выделены следующие категории пользователей:

- администратор информационной безопасности – обладает всей полнотой доступа к ресурсам ИСПДн, организует и контролирует работу ИСПДн объектов информатизации, других пользователей;
- ответственный за эксплуатацию ИСПДн;
- пользователи – имеющие доступ к АРМ объектов информатизации на основании распоряжения о допуске к АРМ.

Ответственный за эксплуатацию ИСПДн и /или АИБ осуществляет: настройку систем защиты от НСД, контроль их работы, обновление антивирусных баз, диагностики и устранение неисправностей или сбоев в работе программного или аппаратного обеспечения, также в его обязанности входит выполнение резервного копирования и восстановления информации. Функции, права и обязанности ответственного за эксплуатацию ИСПДн и АИБа регламентируются должностными инструкциями.

Пользователи АС (операторы) непосредственно осуществляют подготовку, ввод, обработку, хранение и удаление информации в ИСПДн. В зависимости от выполняемых задач и для реализации правил разграничения доступа к ресурсам ИСПДн могут выделяться группы пользователей.

11. Задачи технологического процесса обработки информации в ИСПДн

11.1. Технологический процесс обработки информации в ИСПДн Администрации включает в себя задачи:

- получения исходных данных, их подготовка, оформление, регистрация и выдача пользователями ИСПДн Администрации;
- оформления, регистрации и передачи выходных данных;
- ввода, подготовки, обработки, хранения и вывода информации в ИСПДн;
- настройку, управление и техническое сопровождение СЗИ.

11.2. Задача получения исходных данных, их подготовка, оформление, регистрация и выдача пользователями ИСПДн Администрации состоит из следующих этапов:

- получение ПДн на бумажных носителях и в электронном виде от сторонних организаций, клиентов пользователями ИСПДн Администрации;

ОПИСАНИЕ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ОБРАБОТКИ ИНФОРМАЦИИ

– распечатка электронных файлов документов, содержащих ПДн на принтере ИСПДн;

– передача сведений на бумажных носителях и в электронном виде, обработанных пользователями ИСПДн Администрации в сторонние организации по каналам передачи данных.

11.3. Задачи ввода, подготовки, обработки, хранения и вывода информации в ИСПДн выполняются сотрудниками (пользователями ИСПДн) в подразделениях.

Задачи выполняются с помощью, установленного на рабочей станции ИСПДн ПО, указанного в утвержденном перечне разрешенного к использованию в ПО.

11.5. Настройка, управление и техническое сопровождение СЗИ проводится АИБом и включает следующие операции:

– установка и настройка безопасной операционной среды для пользователей ИСПДн. На этом этапе производится: установка и настройка операционной системы рабочих станций, подключение и конфигурирование устройств ввода-вывода информации ИСПДн, установка и настройка СЗИ, регистрация в СЗИ пользовательских учетных записей и настройка прав доступа для каждого пользователя в соответствии с его функциональными обязанностями (в том числе регистрация и выдача пользователям АС и ИСПДн персональных идентификаторов, а также учет и контроль за наличием их у пользователей), создание, предварительное наполнение информацией (не содержащей сведения, составляющие государственную тайну) настройка парольной политики и т.д.

– непрерывный мониторинг безопасности в ИСПДн с целью выявления нарушений правил разграничения доступа пользователями ИСПДн, диагностики и последующего устранения выявленных неисправностей или ошибок в работе программно-аппаратного обеспечения операционной среды ИСПДн. Данная задача выполняется администратором информационной безопасности путем регулярного анализа системных журналов операционной системы и СЗИ от НСД, регулярных проверок соответствия реализованных в ИСПДн правил разграничения доступа к ресурсам, требованиям разрешительной политики доступа, регулярных проверок правильности соблюдения пользователями требований по защите информации.

– регулярное сопровождение подсистемы безопасности с целью обеспечения эффективности работы пользователей ИСПДн и обеспечения защиты информации. Данная задача выполняется администратором информационной безопасности и ответственным за эксплуатацию ПЭВМ (в части касающейся организационных мероприятий по защите информации) регулярно (по расписанию) или при обнаружении внештатных ситуаций и регламентируется инструкцией о порядке технического обслуживания, ремонта, модернизации технических средств, входящих в состав ИСПДн. Задача включает следующие операции: регулярное проведение инструктажа пользователей по безопасной работе в ИСПДн, устранение выявленных неисправностей и ошибок (осуществляется администратором информационной безопасности), регулярные обновления прикладного ПО и обеспечение его целостности.

12. Этапы технологического процесса

12.1. Доступ пользователей к работе в ИСПДн

Доступ пользователей к информационным ресурсам определяется на основании списка постоянных пользователей ИСПДн и перечня защищаемых информационных ресурсов Администрации

Разграничение прав доступа пользователей к информационным ресурсам и установление полномочий этим пользователям реализуется АИБом средствами ОС и дополнительными средствами СЗИ от НСД.

Вход в систему осуществляется по персональному имени (персональному идентификатору) и паролю конкретного пользователя. При успешном входе в систему

ОПИСАНИЕ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ОБРАБОТКИ ИНФОРМАЦИИ

пользователь получает права доступа к устройствам, каталогам, файлам и программам, установленные АИБом.

При увольнении пользователя или переходе в другое подразделение, АИБом или ответственный за эксплуатацию ИСПДн на основании приказа, в последний день работы пользователя (или иной день, указанный в приказе), производится удаление учетной записи пользователя и всех его ресурсов (за исключением необходимых для работы других пользователей).

12.2. Начало сеанса работы.

Перед началом сеанса работы пользователь включает свою рабочую станцию и проходит процедуру аутентификации.

В процессе аутентификации пользователь использует свои личные логин и пароль. Смена личного пароля производится не реже 1 раза в три месяца. Контроль данного процесса осуществляется АИБом.

12.3. Регистрация пользователей и назначение прав доступа.

Регистрация пользователей и назначение прав доступа производится администратором информационной безопасности на основании заявления «На создание (продление) учетной записи пользователя».

Зарегистрированный пользователь устанавливает свой личный пароль.

Права доступа устанавливаются пользователю средствами ОС в соответствии с разрешительной системой доступа.

Удаление пользователя выполняется однократно при необходимости выведения сотрудника из числа пользователей ИСПДн Администрации.

12.4. Работа с файлами документов, внесение изменений, хранение

Файлы документов разрабатываются на рабочем месте пользователем, зарегистрированным в ИСПДн Администрации.

Работа пользователя при подготовке файла документа возможна только после успешного прохождения процедуры аутентификации в ИСПДн.

Пользователи имеют право постоянного хранения файлов (архивов файлов) с ПДн на несъемном жестком магнитном диске АРМ, учтенном в Журнале учета машинных носителей, содержащих персональные данные.

Разработка и подготовка к печати документов производится с применением, установленных на рабочей станции, текстовых и табличных редакторов.

Распечатка документов производится на принтере, размещенном на ОИ и включенном в технический паспорт на этот ОИ.

По окончании сеанса подготовки документа производится его сохранение в виде файла на несъемном жестком магнитном диске АРМ.

В случае отсутствия необходимости дальнейшей работы с документом, впервые набранным с клавиатуры, пользователь может отказаться от сохранения его в виде файла.

Также пользователь может отказаться от сохранения внесенных в файл изменений.

Уничтожение файла может быть произведено без распечатки документа, если в документе отпала необходимость.

Удаление данных (файлов) и временных файлов, содержащие ПДн производится штатными средствами ОС.

12.5. Работа с МНИ

12.5.1 Общие понятия

Для разработки и хранения файлов с ПДн могут использоваться МНИ, учтенные и разрешенные к использованию в ИСПДн в установленном порядке, включенные в технический паспорт на этот ОИ.

В качестве МНИ в ИСПДн Администрации могут использоваться (разрешены к использованию) следующие накопители информации:

-- оптические (лазерные) диски;

ОПИСАНИЕ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ОБРАБОТКИ ИНФОРМАЦИИ

– USB flash накопители (накопители информации, подключаемые к USB порту ввода-вывода ПЭВМ).

МНИ при необходимости выдаются каждому пользователю из числа сотрудников, обрабатывающих персональные данные. Выданный носитель предназначен только для хранения файлов подготовленных документов.

12.5.2. Хранение МНИ пользователя.

Хранение МНИ пользователя должно осуществляться в соответствии с требованиями инструкции по обращению с носителями ПДн.

12.6. Резервное копирование.

Резервное копирование информационных ресурсов производится АИБом или ответственный за эксплуатацию ИСПДн в соответствии с правами доступа на МНИ, учтенные в порядке, установленном инструкцией по резервному копированию.

12.7. Завершение сеанса работы

По завершении работы пользователь выполняет штатную процедуру завершения работы в Windows, выключает рабочую станцию.

13. Заключительные положения

Всем сотрудникам, допущенным к работе с ПДн, разъясняется ответственность за нарушение правил получения, обработки, защиты ПДн.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн субъектов ПДн, несут ответственность в соответствии с действующим законодательством.