**АКТУАЛЬНАЯ РЕДАКЦИЯ**

**(с изменениями, внесенными распоряжениями от 18.02.2016 № 84-рг, от 31.01.2019 № 32-рг)**

**Российская Федерация**

# **Новгородская область**

## АДМИНИСТРАЦИЯ ВАЛДАЙСКОГО МУНИЦИПАЛЬНОГО РАЙОНА

### Р А С П О Р Я Ж Е Н И Е

от 26.04.2012 № 154-рг

г. Валдай

Об организации работ по

обеспечению безопасности

персональных данных при

их обработке в информации-

оных системах персональных

данных

С целью организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее ИСПДн) Администрация Валдайского муниципального района:

1.Для защиты конфиденциальной информации, содержащейся на электронных носителях, обеспечить соблюдение требований руководящих и нормативно-методических документов Федеральной службы по техническому и экспортному контролю Российской Федерации и Федеральной службы безопасности Российской Федерации (далее ФСТЕК РФ и ФСБ РФ) всеми сотрудниками Администрации Валдайского муниципального района.

2.Назначить ответственных лиц:

2.1.За эксплуатацию информационных систем персональных данных – Москалькова Л. А.

2.2.Администратор безопасности информации – Москалькова Л. А.

2.3.За соблюдение режима конфиденциальности при обработке персональных данных в информационных системах персональных данных – Москалькова Л. А.

3.Утвердить прилагаемый Перечень персональных данных, подлежащих защите.

4.Утвердить прилагаемый Перечень защищаемых ресурсов Администрации Валдайского муниципального района, подлежащих защите.

5. Ввести в действие и утвердить прилагаемую Технологическую инструкцию по работе администратора безопасности информации информационной системы персональных данных.

6. Ввести в действие и утвердить прилагаемую Инструкцию ответственному за эксплуатацию информационной системы персональных данных.

7. Ввести в действие и утвердить прилагаемую Инструкцию о порядке технического обслуживания, ремонта, модернизации технических средств, входящих в состав информационной системы персональных данных.

8. Ввести в действие и утвердить прилагаемую Инструкцию по проведению антивирусного контроля в информационной системе персональных данных.

10. Ввести в действие и утвердить прилагаемую Инструкцию по применению парольной защиты и личных идентификаторов в информационной системе персональных данных.

11. Ввести в действие и утвердить прилагаемую Инструкцию по работе пользователей информационной системы персональных данных.

12. Ввести в действие и утвердить прилагаемую Инструкцию об организации учета, хранения и выдачи машинных носителей, содержащих персональные данные информационной системы персональных данных.

13. Ввести в действие и утвердить прилагаемую Инструкцию по работе ответственного за соблюдение режима конфиденциальности при обработке персональных данных в информационной системе персональных данных.

14. Ввести в действие и утвердить прилагаемый Регламент резервного копирования и восстановления персональных данных.

15. С настоящим распоряжением и его приложениями ознакомить всех сотрудников (под роспись) в части, их касающейся.

16. Контроль за выполнением распоряжения оставляю за собой.

**Глава муниципального района В.М. Данилов**

УТВЕРЖДЕН

распоряжением Администрации

муниципального района

от 26.04.2012 № 154-рг

ПЕРЕЧЕНЬ

персональных данных, подлежащих защите

Фамилия, имя, отчество.

Год, месяц, дата и место рождения.

Гражданство.

Место жительства/место регистрации.

Семейное положение.

Образование, квалификация, сведения об обучении.

Место работы.

Размер заработной платы, дохода, иных выплат.

Паспортные данные.

При оказании юридических услуг дополнительно члены семьи в части Ф.И.О.; адреса; даты рождения; должности/профессии, места работы, паспортных данных.

Информация о наличии социальных льгот гарантированных государством (документы подтверждающие статусы: мать-одиночка, чернобылец, ветеран войны и т.д.).

Сведения о временной нетрудоспособности.

Сведения об удержаниях из заработной платы, в том числе сведения о размере алиментов и иных долговых обязательствах по исполнительным листам.

Информация о наличии группы инвалидности, сведения о добровольном медицинском страховании.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

УТВЕРЖДЕН

распоряжением Администрации

муниципального района

от 26.04.2012 № 154-рг

**ПЕРЕЧЕНЬ**

защищаемых ресурсов Администрации Валдайского

муниципального района, подлежащих защите

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | Защищаемый ресурс | | |
| Сведения, содержащиеся в защищаемом ресурсе | Наименование ресурса (реализация ресурса) | Степень конфиденциальности информации, содержащейся в защищаемом ресурсе |
| 1. | Сведения, включенные в Перечень персональных данных, подлежащих защите», утвержденный распоряжением Администрации муниципального района  от «\_\_» \_\_\_\_\_2012 №\_\_\_\_ | файлы и архивы файлов, расположенные на несъемном жестком магнитном диске АРМ, учтенном в Журнале учета машинных носителей, содержащих персональные данные | конфиденциально |

УТВЕРЖДЕНА

распоряжением Администрации

муниципального района

от 26.04.2012 № 154-рг

**ТЕХНОЛОГИЧЕСКАЯ ИНСТРУКЦИЯ**

по работе администратора безопасности информации информационной

системы персональных данных

**1. Общие положения**

1.1. Администратор безопасности информации (АБ) - лицо, выполняющее функции по настройке и сопровождению всех программных и технических средств защиты информации информационных систем персональных данных (ИСПДн) Администрации Валдайского муниципального района, предназначенных для обработки информации, содержащей персональные данные.

1.2. АБ в пределах своих функциональных обязанностей обеспечивает безопасность информации, обрабатываемой, передаваемой и хранимой в ИСПДн.

1.3. АБ назначается распоряжением Главы муниципального района.

* 1. АБ в своей работе руководствуется положениями нормативно - правовых актов РФ, руководящими документами по безопасности информации, положениями, приказами и нормативными актами министерств и ведомств Российской Федерации и положениями настоящей Инструкции.

**2. Обязанности**

Основными обязанностями АБ являются:

управление средствами и системами защиты информации (СЗИ) ИСПДн и поддержание их функционирования;

восстановление функций программных и технических СЗИ от несанкционированного доступа (НСД) к информации;

генерация ключей, личных идентификаторов, а так же паролей для пользователей ИСПДн;

формирование и управление списком необходимых реквизитов и значением атрибутов объектов и субъектов доступа;

назначение прав доступа, полномочий и привилегий пользователей к объектам доступа (программам, файлам, каталогам, портам и устройствам ввода-вывода (УВВ);

обеспечение правильной эксплуатации технических и программных СЗИ в ИСПДн;

контроль целостности эксплуатируемого в ИСПДн программного обеспечения, в том числе самих СЗИ, с целью недопущения и выявления несанкционированных модификаций;

текущий, после сбоев и периодический (не реже 1 раза в год) контроль работоспособности средств и систем защиты информации от НСД;

контроль соблюдения пользователями ИСПДн требований инструкций и порядка работы при обработке информации в ИСПДн по вопросам защиты информации от НСД;

контроль выполнения утвержденной технологии обработки информации в ИСПДн;

выявление подозрительных действий пользователей и попыток НСД **к** информации, обрабатываемой в ИСПДн, путем анализа системных журналов информационной безопасности при работе в ИСПДн;

выполнение резервного копирования машинных документов, содержащих персональные данные;

обучение и консультация персонала и пользователей ИСПДн правилам работы **с** СЗИ от НСД;

организация антивирусной защиты информации и программных средств в ИСПДн;

**3. Права**

АБ имеет право:

требовать от пользователей ИСПДн выполнения установленной технологии обработки информации, инструкций по обеспечению информационной безопасности ИСПДн.

останавливать обработку информации в ИСПДн в случаях подтвержденных нарушений установленной технологии обработки данных, приводящих к нарушению функционирования СЗИ.

**4. Ответственность**

4.1. На АБ возлагается персональная ответственность за качество и полноту проводимых им работ по обеспечению защиты информации в соответствии с его функциональными обязанностями.

4.2. АБ несет ответственность по законодательству РФ за нарушение требований нормативно – методических документов по защите информации и настоящей инструкции.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

УТВЕРЖДЕНА

распоряжением Администрации

муниципального района

от 26.04.2012 № 154-рг

**ИНСТРУКЦИЯ**

ответственному за эксплуатацию информационной системы

персональных данных

**1. Общие положения**

1.1. Настоящая инструкция определяет основные обязанности, права и ответственность ответственного за эксплуатацию информационных систем персональных данных (далее - ИСПДн) Администрации Валдайского муниципального района по вопросам защиты информации в ИСПДн.

1.2. Ответственный за эксплуатацию ИСПДн (далее - ответственный объекта) назначается распоряжением Администрации муниципального района и осуществляет контроль за соблюдением правил эксплуатации ИСПДп, на которых проводится обработка персональных данных (далее - информации).

**2.Права и обязанности ответственного за эксплуатацию**

Ответственный за эксплуатацию ИСПДн обязан:

2.1. Знать перечень компьютеров входящих в состав ИСПДп и перечень задач, решаемых с их использованием;

2.2. Обеспечивать постоянный контроль за выполнением пользователями ИСПДн требований руководящих документов по обеспечению безопасной автоматизированной обработки персональных данных;

2.4. Организовать ведение «Журнала учета машинных носителей, содержащих персональные данные»;

2.5. Осуществлять контроль за правильностью использования и хранения машинных носителей информации и документов, содержащих персональные данные;

2.6. Осуществлять контроль за правильностью использования и хранения персональных идентификаторов и личных паролей пользователями:

2.7. Разъяснять сотрудникам администрации муниципального района вопросы обеспечения информационной безопасности и правила работы с используемыми средствами зашиты информации;

2.8. Требовать от сотрудников администрации муниципального района соблюдение организации парольной зашиты (в соответствии с Инструкцией по применению парольной зашиты личных идентификаторов в информационной системе персональных данных);

2.9. Контролировать использование сотрудниками администрации муниципального района средств зашиты информации установленных на объекте информатизации:

2.10. Контролировать прохождение антивирусного контроля (в соответствии с Инструкцией по проведению антивирусного контроля в информационной системе персональных данных) при применении машинных носителей информации;

2.11. Немедленно прекращать работы на рабочих станциях при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности.

Ответственный за эксплуатацию ИСНДн имеет право:

2.12. Требовать от пользователей ИСПДн соблюдения установленных технологий обработки информации и выполнения инструкций по обеспечению безопасности информации в ИСПДн;

2.13. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения зашиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДп;

2.14. Подавать свои предложения по совершенствованию организационных, технологических и технических мер защиты на своем участке работы.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

УТВЕРЖДЕНА

распоряжением Администрации

муниципального района

от 26.04.2012 № 154-рг

**ИНСТРУКЦИЯ**

о порядке технического обслуживания, ремонта, модернизации технических средств, входящих в состав информационной системы

персональных данных

**1. Общие положения**

1.1. Настоящая инструкция определяет правила работ по техническому обслуживанию, ремонту, модернизации технических средств, входящих в состав информационных системах персональных данных (ИСПДн), защищенных от несанкционированного доступа (НСД) и предназначенной для обработки и хранения персональных данных.

1.2. Данные работы проводятся только с разрешения Главы муниципального района или лица, исполняющего его обязанности, после согласования с ответственным за эксплуатацию ИСПДн или администратором безопасности информации ИСПДн.

**2. Порядок проведения работ по техническому обслуживанию, ремонту, модернизации**

2.1. В случае, когда необходимо провести работы по техническому обслуживанию (ремонту, модернизации) технических средств, входящих в состав ИСПДн, ответственный за эксплуатацию ИСПДн представляет служебную записку, в которой:

указывает название и номер ПЭВМ (технического средства, системы), техническое обслуживание (ремонт, модернизацию) которой необходимо провести и с какой целью;

обосновывает необходимость технического обслуживания (модернизации);

указывает планируемые место и сроки работ, режим их проведения;

перечисляет меры безопасности, которые будут реализованы при техническом обслуживании (ремонте, модернизации) с целью недопущения доступа к персональным данным посторонних лиц.

2.2.  В случае если для проведения работ необходимо привлекать лиц, не имеющих постоянного допуска к работе на ПЭВМ или в помещение, составляется список сотрудников, который согласовывается с Главой муниципального района.

Запрещается выносить технические средства и системы (ТСС), входящие в состав ИСПДн, с территории здания без согласования с ответственным за эксплуатацию ИСПДн и разрешения Главы муниципального района.

2.3. Вскрытие печатей на корпусах ПЭВМ или других технических средств (систем) и последующее опечатывание производится комиссионно в присутствии администратора безопасности информации, о чём составляется акт.

В акте указывается:

номер (название) помещения, в котором проводились работы,

дата и время начала и окончания работ,

лица, присутствовавшие при вскрытии и обслуживании (ремонте, модернизации), -наличие, целостность и места размещения печатей (пломб, специальных

защитных знаков) до вскрытия ПЭВМ (технического средства, системы),

установленные неисправности,

виды и результаты проведенных работ,

замененные или отремонтированные узлы (детали), наличие на этих узлах специальных защитных знаков,

какими печатями (пломбами и т.д.) и в каких местах ПЭВМ (устройство) опечатано по окончании работ,

необходимость проведения дополнительной специальной проверки и специальных исследований (сертификации) ПЭВМ (технического средства, системы) или её отдельных узлов,

иная необходимая для дальнейшей работы и обеспечения безопасности информация.

2.4. Если для ремонта (модернизации) ИСПДн (другого технического средства, системы, узла ПЭВМ в составе ИСПДн) необходимо направить в специализированную организацию, то комиссией составляется заключение.

2.5. Перед отправкой ПЭВМ (другого технического средства, системы, узла ПЭВМ) администратор безопасности информации обязан гарантированно удалить персональные данные с жесткого диска и иных устройств памяти ПЭВМ (другого технического средства, системы) сертифицированными средствами, о чем он совместно с ответственным за эксплуатацию ИСПДн составляет акт. По запросу из специализированной организации копия акта передаётся и ей.

2.6. В случае если не имеется возможности гарантировано удалить персональные данные с жесткого диска и иных устройств памяти ПЭВМ (другого технического средства, системы) сертифицированными средствами, эти устройства опечатываются и хранятся у ответственного за эксплуатацию ИСПДн с соблюдением требований, предъявляемым к хранению персональных данных.

2.7. Ремонт и замена жесткого диска производится с соблюдением требований подпунктов 2.4-2.6 настоящей Инструкции в присутствии администратора безопасности информации. При диагностике и ремонте жесткого диска должны быть реализованы меры безопасности, исключающие несанкционированный доступ к хранящимся на нём данным.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

УТВЕРЖДЕНА

распоряжением Администрации

муниципального района

от 26.04.2012 № 154-рг

**ИНСТРУКЦИЯ**

по проведению антивирусного контроля в информационной

системе персональных данных

1. Настоящая Инструкция предназначена для пользователей информационных систем персональных данных (ИСПДн) Администрации Валдайского муниципального района.

2. В целях обеспечения антивирусной защиты в ИСПДн производится антивирусный контроль.

3. Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на администратора безопасности информации.

4. К применению в ИСПДн допускаются лицензионные антивирусные средства.

5. В ИСПДн запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

6. Пользователи ИСПДн при работе со съемными носителями информации (компакт-дисками (CD), USB флеш-накопителями, гибкими магнитными дисками (ГМД)) обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.

7. Ярлык для запуска антивирусной программы должен быть вынесен на «Рабочий стол» операционной системы.

8. Администратор безопасности информации осуществляет периодическое обновление антивирусных пакетов и контроль их работоспособности.

9. Администратор безопасности информации проводит периодическое тестирование всего установленного программного обеспечения на предмет отсутствия компьютерных вирусов.

10. При обнаружении компьютерного вируса пользователь ИСПДн обязан немедленно поставить в известность администратора безопасности информации и прекратить какие-либо действия в ИСПДн.

11. Администратор безопасности информации проводит, в случае необходимости, лечение зараженных файлов путем выбора соответствующего пункта меню антивирусной программы и после этого вновь проводит антивирусный контроль.

12. В случае обнаружения на съемных носителях информации нового вируса, не поддающегося лечению, администратор безопасности информации обязан запретить использование данного съемного носителя информации.

13. В случае обнаружения вируса, не поддающегося лечению, администратор безопасности информации обязан поставить в известность ответственного за эксплуатацию ИСПДн, запретить работу в ИСПДн и в возможно короткие сроки обновить пакет антивирусных программ.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

УТВЕРЖДЕНА

распоряжением Администрации

муниципального района

от 26.04.2012 № 154-рг

**ИНСТРУКЦИЯ**

по применению парольной защиты и личных идентификаторов

в информационной системе персональных данных

1. Настоящая Инструкция определяет порядок использования, генерации, смены и прекращения действия паролей и личных идентификаторов пользователей в информационных системах персональных данных (ИСПДн) Администрации Валдайского муниципального района, а также контроль действий пользователей при работе с паролями.

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей, а также контроль действий пользователей при работе с паролями возлагается на администратора безопасности информации.

3. Пароли для всех учетных записей пользователей ИСПДн должны выбираться с учетом следующих требований:

длина пароля должна быть не менее 6 буквенно-цифровых символов;

пароль не должен включать в себя легко вычисляемые (угадываемые) сочетания символов (имена, фамилии, отчества, наименования организации и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER, ADM, ADMIN и т.п.);

максимальное действие пароля - не более чем 90 дней;

пароль не должен повторяться;

пользователь не может неправильно ввести пароль учетной записи более 5 раз, в этом случае должна происходить блокировка учетной записи пользователя, до момента снятия блокировки.

3.1 При первичной регистрации пользователя в системе пароль ему назначает администратор безопасности информации.

3.2 Пользователи ИСПДн обязаны хранить свой личный пароль втайне от других и не передавать любым способом пароль третьим лицам.

3.3. Пользователь ИСПДн лично должен проводить смену пароля учетной записи регулярно не реже одного раза в три месяца.

4. Привязку идентификатора к пользователю (учетной записи) выполняет администратор безопасности информации.

4.1 Пользователи ИСПДн получают свой идентификатор у администратора безопасности информации.

4.2 Пользователь ИСПДн обязан хранить свой личный идентификатор в недоступных для других сотрудников хранилищах.

4.3 Пользователю ИСПДН запрещается передавать свой личный идентификатор.

4.4 В случае утери личного идентификатора, пользователь ИСПДн должен немедленно доложить об этом администратору безопасности информации.

5. В случае прекращения полномочий учетной записи пользователя ИСПДн (увольнение, переход на другую работу, в другой отдел или помещение, а также другие обстоятельства) учетная запись должна быть удалена, а её идентификатор должен быть сдан администратору безопасности информации после окончания последнего сеанса работы данного пользователя в ИСПДн.

6. В случае компрометации личного пароля или утери личного идентификатора пользователя администратором безопасности информации должны быть немедленно предприняты меры в соответствии с п. 7 настоящей Инструкции.

7.  Администратор безопасности информации должен провести служебное расследование для выяснения причин компрометации пароля с целью выработки новых или совершенствования принятых технических и организационных мер по устранению такой угрозы в будущем, а также выяснению величины ущерба, который может быть нанесен собственнику информационных ресурсов.

8. Пользователи ИСПДн должны быть ознакомлены под роспись с личными паролями и с требованиями настоящей Инструкции.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

УТВЕРЖДЕНА

распоряжением Администрации

муниципального района

от 26.04.2012 № 154-рг

**ИНСТРУКЦИЯ**

по работе пользователей информационной системы

персональных данных

**1.Общие положения**

1.1. Пользователями информационных систем персональных данных (ИСПДн) Администрации Валдайского муниципального района, предназначенных для обработки информации, содержащей персональные данные, являются сотрудники Администрации Валдайского муниципального района, допущенные к работе в ИСПДн.

1.2. Настоящая инструкция определяет задачи, функции, обязанности, права и ответственность пользователей, допущенных к работе в ИСПДн.

**2. Обязанности пользователя**

2.1. При эксплуатации ИСПДн пользователь обязан:

2.1.1. Руководствоваться требованиями следующих документов:

Инструкцией по применению парольной защиты и личных идентификаторов в информационной системе персональных данных», в части их касающейся;

Инструкцией по проведению антивирусного контроля в информационной системе персональных данных», в части их касающейся;

Инструкцией об организации учета, хранения и выдачи машинных носителей, содержащих персональные данные информационной системы персональных данных», в части их касающейся;

настоящей Инструкцией.

2.1.2. Помнить личные пароли и идентификаторы.

2.1.3. Соблюдать установленную технологию обработки информации.

2.1.4. Руководствоваться требованиями инструкций по эксплуатации установленных средств вычислительной техники (СВТ) и средств защиты информации (СЗИ).

2.1.5. Размещать устройства вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы, в помещениях, в которых они установлены, таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные.

2.2. При выходе в течение рабочего дня из помещения, в котором размещается ИСПДн, пользователь обязан:

блокировать ввод-вывод информации на своем рабочем месте ИСПДн в случаях кратковременного отсутствия (перерыв) или выключать СВТ ИСПДн;

блокировать вывод информации на монитор ПЭВМ;

Пользователю **ЗАПРЕЩАЕТСЯ:**

подключать к ПЭВМ нештатные устройства;

самостоятельно вносить изменения в состав, конфигурацию и размещение ИСПДн;

самостоятельно вносить изменения в состав, конфигурацию и настройку программного обеспечения (ПО), установленного в ИСПДн;

самостоятельно вносить изменения в размещение, состав и настройку СЗИ ИСПДн;

сообщать устно, письменно или иным способом (показ и т.п.) другим лицам пароли, передавать личные идентификаторы, ключевые дискеты и другие реквизиты доступа к ресурсам ИСПДн.

**3. Права**

Пользователь ИСПДн имеет право:

обращаться к администратору безопасности информации (АБ) с просьбой об оказании технической и методической помощи по обеспечению безопасности обрабатываемой в ИСПДн информации, по использованию установленных программных и технических средств ИСПДн, а также по вопросам эксплуатации установленных СЗИ;

обращаться к ответственному за эксплуатацию ИСПДн по вопросам эксплуатации ИСПДн (выполнение установленной технологии обработки информации, инструкций и других документов по обеспечению информационной безопасности объекта и защиты информации);

обращаться к ответственному за соблюдение режима конфиденциальности при обработке персональных данных в ИСПДн по вопросам выполнения режимных мер при обработке информации.

**4. Ответственность**

Пользователь несет персональную ответственность:

за соблюдение установленной технологии обработки информации;

за соблюдение режима конфиденциальности при обработке и хранении в ИСПДн информации;

за правильность понимания и полноту выполнения задач, функций, прав и обязанностей, возложенных на него при работе в ИСПДн;

за соблюдение требований нормативных правовых актов, приказов, распоряжений и указаний, определяющих порядок организации работ по информационной безопасности при работе с персональными данными.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

УТВЕРЖДЕНА

распоряжением Администрации

муниципального района

от 26.04.2012 № 154-рг

**ИНСТРУКЦИЯ**

об организации учета, хранения и выдачи машинных носителей, содержащих персональные данные информационной системы

персональных данных

1. Настоящая Инструкция устанавливает организацию учета, хранения и выдачи машинных носителей, содержащих персональные данные информационных систем персональных данных Администрации Валдайского муниципального района (ИСПДн).

2. Учет, хранение и выдачу машинных носителей персональных данных осуществляют ответственные за эксплуатацию ИСПДн. Данные сотрудники несут личную ответственность за сохранность персональных данных. При увольнении сотрудника, ответственного за учет, хранение и выдачу машинных носителей персональных данных, составляется акт приема-сдачи этих документов, который утверждается Главой муниципального района.

3. Организация учета машинных носителей персональных данных.

Все находящиеся на хранении и в обращении машинные носители персональных данных (далее - носители) подлежат учёту. Учет всех видов и типов носителей производится в Журнале учета машинных носителей, содержащих персональные данные.

Каждый носитель должен иметь этикетку, на которой указывается его уникальный учетный номер. На несъемной части упаковки носителя ПДн указывается:

учетный номер;

отметка «Персональные данные»;

дата регистрации (день, месяц, год);

ФИО, должность, подпись сотрудника выполнившего учет.

4. Организация выдачи машинных носителей персональных данных. Пользователи ИСПДн получают учтенный съемный носитель от уполномоченного сотрудника, для выполнения работ на конкретный срок. При получении делаются соответствующие записи в Журнале учета машинных носителей, содержащих персональные данные. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в Журнале учета машинных носителей, содержащих персональные данные.

5.Организация хранения машинных носителей персональных данных.

Хранение носителей осуществляется в условиях, исключающих несанкционированное копирование, изменение или уничтожение секретной информации, а также хищение носителей. Носители должны храниться в служебных помещениях, в металлическом хранилище (сейфе) - установленным порядком. Запрещается хранить машинные носители персональных данных вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам.

6. В случае утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений, немедленно ставится в известность администратор безопасности информации. Соответствующие отметки вносятся в Журнале учета машинных носителей, содержащих персональные данные.

7. Носители, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. По результатам уничтожения носителей составляется Акт уничтожения машинных носителей персональных данных.

8. При передаче средств вычислительной техники ИСПДн сторонним организациям для проведения ремонтно-восстановительных или иных работ, несъемные машинные носители изымаются из состава средств вычислительной техники.

9. Ответственность за выполнение правил эксплуатации машинных носителей персональных данных при выполнении непосредственных работ с носителями несет пользователь ИСПДн.

10. Контроль выполнения пользователями установленных правил эксплуатации машинных носителей персональных данных, осуществляет ответственный за эксплуатацию ИСПДн и администратор безопасности информации в рамках своих должностных обязанностей.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

УТВЕРЖДЕНА

распоряжением Администрации

муниципального района

от 26.04.2012 № 154-рг

**ИНСТРУКЦИЯ**

по работе ответственного за соблюдение режима конфиденциальности при обработке персональных данных в информационной

системе персональных данных

**1. Общие положения**

1.1. Настоящая инструкция определяет задачи, функции, обязанности, права и ответственность лица, назначенного ответственным за соблюдение режима конфиденциальности при обработке персональных данных в информационной системе персональных данных (ИСПДн).

1.2. Ответственный за соблюдение режима конфиденциальности назначается распоряжением Главы муниципального района.

1.3. Ответственный за соблюдение режима конфиденциальности в своей работе руководствуется требованиями руководящих документов по безопасности информации, положениями нормативно-правовых актов РФ, приказами, а также положениями настоящей Инструкции.

**2.** **Обязанности**

Основными действиями ответственного за соблюдение режима конфиденциальности при выполнении своих обязанностей являются:

2.1. Проведение инструктажа и консультации пользователей ПЭВМ по соблюдению установленного режима конфиденциальности при обработке персональных данных в ИСПДн;

2.2. Взаимодействие с ответственными за эксплуатацию ИСПДн и администратором безопасности информации (АБ) по вопросам обеспечения защиты информации и прав доступа пользователей к ней.

2.3. Выполнение, учет и контроль изменений, вносимых:

в списки пользователей ИСПДн;

в перечень защищаемых информационных ресурсов ИСПДн;

2.4. Организация и проведение периодического и внеочередного контроля работы пользователей.

2.5. Контроль выполнения пользователями ИСПДн установленного режима конфиденциальности при обработке персональных данных, в том числе, соблюдения режима конфиденциальности при обращении с персональными идентификаторами, личными ключевыми дискетами и карточками паролей, со съемными машинными носителями информации, в процессе создания машинных документов, при процедурах «лечения» администратором безопасности информации зараженных файлов.

2.6. Участие в процедурах контроля операций по безопасному удалению личных файлов пользователя при прекращении полномочий учетной записи, по уничтожению (в установленном порядке) старых карточек паролей (при замене АБ паролей пользователям) и созданию новых карточек паролей.

2.7. Организация и участие в служебных расследованиях для выяснения причин утечки или воздействия на обрабатываемую в ИСПДн информацию, компрометации паролей с целью выяснения величины нанесенного ущерба безопасности информации и выработки новых или совершенствования принятых технических и организационных мер по защите информации от реализации угрозы в будущем.

2.8. При возникновении необходимости организация и участие в мероприятиях, связанных с событиями вскрытия, опечатывания, модификации состава, ремонта и т.д. технических средств ИСПДн. Опечатывание корпусов технических средств ИСПДн. Составление актов о вскрытии и опечатывании корпусов технических средств.

**3. Права**

Ответственный за соблюдение режима конфиденциальности имеет право:

требовать от пользователей ИСПДн выполнения положений следующих инструкций по обеспечению информационной безопасности ИСПДн:

Инструкции по работе пользователей информационной системы персональных данных;

Инструкции по применению парольной защиты и личных идентификаторов в информационной системе персональных данных, в части их касающейся;

Инструкции по проведению антивирусного контроля в информационной системе персональных данных, в части их касающейся;

Инструкции об организации учета, хранения и выдачи машинных носителей, содержащих персональные данные информационной системы персональных данных, в части их касающейся;

участвовать в разработке мероприятий по совершенствованию системы защиты информации в ИСПДн;

обращаться к Главе муниципального района с мотивированным предложением по приостановке процесса обработки информации в ИСПДн или отстранению от работы пользователя ИСПДн в случаях систематического нарушения режима конфиденциальности, технологии обработки информации в ИСПДн.

**4. Ответственность**

4.1 На ответственного за соблюдение режима конфиденциальности возлагается персональная ответственность за полноту и качество выполнения своих должностных обязанностей, а также за реализацию адекватных реальным угрозам безопасности информации режимных мер по защите информации и за их своевременное применение.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

УТВЕРЖДЕН

распоряжением Администрации

муниципального района

от 26.04.2012 № 154-рг

**РЕГЛАМЕНТ**

резервного копирования и восстановления персональных данных

**1. Общие положения**

Настоящий Регламент проведения резервного копирования (восстановления) программ и данных, хранящихся в информационных системах персональных данных (ИСПДн) Администрации Валдайского муниципального района, разработан с целью:

определения порядка резервирования данных для последующего восстановления работоспособности ИСПДн Администрации Валдайского муниципального района при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);

определения порядка восстановления информации в случае возникновения такой необходимости;

упорядочения работы должностных лиц Администрации Валдайского муниципального района, связанной с резервным копированием и восстановлением информации

В настоящем документе регламентируются действия при выполнении следующих мероприятий:

резервное копирование;

контроль резервного копирования;

хранение резервных копий;

полное или частичное восстановление данных и приложений.

Резервному копированию подлежит информация следующих основных категорий:

персональные профили пользователей сети;

персональные данные в электронном виде, согласно «Перечню персональных данных, подлежащих защите».

Машинным носителям информации, содержащим резервную копию, присваивается гриф конфиденциальности «Для служебного пользования».

**2. Порядок резервного копирования**

Резервное копирование автоматизированных систем производится на основании следующих данных:

состав и объем копируемых данных, периодичность проведения резервного копирования;

максимальный срок хранения резервных копий -1 месяц;

хранение 3-х следующих архивов;

архив на 1-е число текущего месяца;

архив среда-четверг либо пятница-суббота текущей недели;

архив сделанный в текущую ночь.

Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, в установленные сроки и с заданной периодичностью. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности произошедших в процессе резервного копирования, сообщается ответственному за эксплуатацию информационной системы персональных данных.

**3. Методика резервного копирования**

Резервное копирование осуществляется средствами ОС Windows путем копирования информации на несъемный жесткий диск.

**4. Контроль результатов резервного копирования**

Контроль результатов всех процедур резервного копирования осуществляется ответственным за эксплуатацию ИСПДн в срок до 17 часов рабочего дня, следующего за установленной датой выполнения этих процедур.

В случае обнаружения ошибки ответственный за эксплуатацию ИСПДн сообщает об этом факте ответственному за соблюдение режима конфиденциальности при обработке персональных данных до 18 часов текущего рабочего дня.

На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, должно осуществляться ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для её хранения.

**5. Ротация носителей резервной копии.**

Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации автоматизированных систем в случае отказа любого из устройств резервного копирования.

Все процедуры по загрузке, выгрузке носителей из системы резервного копирования осуществляются ответственным за эксплуатацию ИСПДн. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек. Персональные данные с носителей, которые перестают использоваться в системе резервного копирования, должны стираться.

**6. Восстановление информации из резервных копий**

В случае необходимости восстановление данных из резервных копий производится на основании Заявки владельца информации, согласованной с Ответственным за эксплуатацию ИСПДн Администрации Валдайского муниципального района. После поступления заявки восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.

**7. Методика резервного копирования**

Любое восстановление информации, не вызванное необходимостью экстренного восстановления, связанной с потерей работоспособности информационной системы персональных данных или ее компонент, выполняется на основании распоряжения Администрации муниципального района.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_