ИСПОЛНИТЕЛЬНЫЙ
КОМИТЕТ АГРЫЗСКОГО
МУНИЦИПАЛЬНОГО РАЙОНА
РЕСПУБЛИКИ ТАТАРСТАН

ул. Гагарина, д.13, г. Агрыз, 422230

ТАТАРСТАН РЕСПУБЛИКАСЫ
ӘГЕРЖЕ
МУНИЦИПАЛЬ РАЙОНЫНЫҢ
БАШКАРМА КОМИТЕТЫ

Гагарин ур.,13, Әгерҗе шәһәре, 422230

Тел.: (85551) 2-22-46; Факс: 2-30-61; E-mail: isp.agryz@tatar.ru; www. agryz.tatarstan.ru

**РАСПОРЯЖЕНИЕ** **БОЕРЫК**

«13» октября 20 21 г. № 139-р

Об утверждении организационно - распорядительных документов по защите персональных данных

В соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»:

1. Утвердить:

- перечень персональных данных, обрабатываемых в Исполнительном комитете Агрызского муниципального района Республики Татарстан (приложение №1);
- план внутренних проверок состояния защиты информационных систем персональных данных (приложение №2);
- инструкцию по физической охране и контролю доступа в помещения (приложение №3);
- инструкцию обслуживающего персонала информационных систем персональных данных (приложение №4);
- инструкцию по работе ответственного лица за организацию обработки персональных данных (приложение №5);
- инструкцию по работе ответственного лица за обеспечение безопасности персональных данных (приложение №6);
- инструкцию администратора безопасности информационных систем персональных данных (приложение №7);
- инструкцию по разграничению доступа пользователей к средствам защиты и информационным ресурсам (приложение №8);
- инструкцию по учету машинных носителей и регистрации их выдачи (приложение №9);
- инструкцию пользователя информационных систем персональных данных (приложение №10);
- инструкцию о порядке работы с персональными данными (приложение №11);
- инструкцию по организации антивирусной защиты (приложение №12);
- инструкцию по организации парольной защиты (приложение №13);
- регламент резервного копирования данных (приложение №14).

2. Настоящее распоряжение разместить на официальном сайте Агрызского муниципального района в составе портала муниципальных образований Республики Татарстан (https://agryz.tatarstan.ru) в информационно-телекоммуникационной сети «Интернет».

3. Контроль за исполнением настоящего распоряжения оставляю за собой.

**Руководитель** **А.Э. Акбашев**

Приложение № 1
к распоряжению
Исполнительного комитета
Агрызского муниципального района
Республики Татарстан
от 13.10.2021 № 139-р

**Перечень**
**персональных данных, обрабатываемых в Исполнительном комитете Агрызского муниципального района Республики Татарстан**

| № п/п | Наименование персональных данных | Способ обработки |
|---|---|---|
| **Сведения, составляющие персональные данные работников** | | |
| 1. | Фамилия, имя, отчество | Смешанный |
| 2. | Сведения об идентификационном номере налогоплательщика | Смешанный |
| 3. | Сведения о пенсионном страховом свидетельстве | Смешанный |
| 4. | Табельный номер | Смешанный |
| 5. | Пол | Смешанный |
| 6. | Номер, дата трудового договора | Смешанный |
| 7. | Дата рождения | Смешанный |
| 8. | Место рождения | Смешанный |
| 9. | Гражданство | Смешанный |
| 10. | Образование (среднее (полное) общее, начальное профессиональное, среднее профессиональное, высшее профессиональное, аспирантура, адъюнктура, докторантура) | Смешанный |
| 11. | Наименование образовательного учреждения | Смешанный |
| 12. | Наименование, серия, номер, дата выдачи, направление или специальность, код по ОКСО, ОКИН документа об образовании, о квалификации или наличии специальных знаний | Смешанный |
| 13. | Профессия (в т.ч. код по ОКПДТР) | Смешанный |
| 14. | Стаж работы | Смешанный |
| 15. | Состояние в браке | Смешанный |
| 16. | Состав семьи, с указанием степени родства, фамилии, имени, отчества, года рождения ближайших родственников | Смешанный |
| 17. | Данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ) | Смешанный |
| 18. | Адрес и дата регистрации по месту жительства (месту пребывания) | Смешанный |
| 19. | Контактный телефон | Смешанный |

| № п/п | Наименование персональных данных | Способ обработки |
|---|---|---|
| 20. | Сведения о воинском учете (категория запаса, воинское звание, состав (профиль), полное кодовое обозначение ВУС; категория годности к военной службе, наименование военного комиссариата по месту жительства, состоит на воинском учете, отметка о снятии с учета) | Смешанный |
| 21. | Дата приема на работу | Смешанный |
| 22. | Вид работы (основной, по совместительству) | Смешанный |
| 23. | Структурное подразделение | Смешанный |
| 24. | Занимаемая должность (специальность, профессия), разряд, класс (категория) квалификации | Смешанный |
| 25. | Ранее занимаемая должность | Смешанный |
| 26. | Тарифная ставка (оклад), надбавка, руб. | Смешанный |
| 27. | Основание трудоустройства | Смешанный |
| 28. | Личная подпись работника | Смешанный |
| 29. | Фотография | Смешанный |
| 30. | Сведения об аттестации (дата, решение, номер и дата документа, основание) | Смешанный |
| 31. | Сведения о профессиональной подготовке (дата начала и окончания переподготовки, специальность (направление, профессия, наименование, номер, дата документа, свидетельствующего о переподготовке, основание переподготовки) | Смешанный |
| 32. | Сведения о наградах, поощрениях, почетных званиях (наименование, номер, дата награды) | Смешанный |
| 33. | Сведения об отпусках (вид, период работы, количество дней, дата начала и окончания, основание) | Смешанный |
| 34. | Сведения о социальных льготах, на которые работник имеет право в соответствии с законодательством (наименование льготы, номер, дата выдачи документа, основание) | Смешанный |
| 35. | Сведения об увольнении (основания, дата, номер и дата приказа) | Смешанный |

Приложение №2
к распоряжению
Исполнительного комитета
Агрызского муниципального района
Республики Татарстан
от 13.10.2021 № 139-р

**ПЛАН**
**внутренних проверок состояния защиты информационных систем персональных данных**

| № п/п | Мероприятие | Периодичность | Исполнитель |
|---|---|---|---|
| 1 | Мониторинг результатов регистрации событий безопасности и реагирование на них | Еженедельно | Администратор безопасности |
| 2 | Контроль над выполнением антивирусной защиты | Еженедельно | Администратор безопасности |
| 3 | Контроль над соблюдением режима защиты при подключении к сетям общего пользования | Еженедельно | Администратор безопасности |
| 4 | Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн | Ежегодно | Администратор безопасности |
| 5 | Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн | Ежемесячно | Администратор безопасности |
| 6 | Контроль работоспособности и правильности функционирования программного обеспечения и средств защиты информации | Ежемесячно | Администратор безопасности |
| 7 | Контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации | Ежемесячно | Администратор безопасности |
| 8 | Контроль состава технических средств, программного обеспечения и средств защиты информации | Ежемесячно | Администратор безопасности |
| 9 | Контроль за обеспечением резервного копирования | Ежемесячно | Администратор безопасности |
| 10 | Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз | Ежегодно | Администратор безопасности |
| 11 | Поддержание в актуальном состоянии нормативно-организационных документов | Ежемесячно | Ответственный за организацию обработки |

| № п/п | Мероприятие | Периодичность | Исполнитель |
|---|---|---|---|
| | | | персональных данных |
| 12 | Контроль за разработкой и внесением изменений в программное обеспечение собственной разработки или штатное ПО специально дорабатываемое собственными разработчиками или сторонними организациями. | Ежемесячно | Администратор безопасности |
| 13 | Периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы | Ежемесячно | Администратор безопасности |
| 14 | Проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации | Ежемесячно | Администратор безопасности |
| 15 | Контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков | Ежеквартально | Администратор безопасности |
| 16 | Контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков | Ежеквартально | Ответственный за обеспечение безопасности персональных данных |

Приложение № 3
к распоряжению
Исполнительного комитета
Агрызского муниципального района
Республики Татарстан
от 13.10.2021 № 139-р

# Инструкция
# по физической охране и контролю доступа в помещения

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

**1.1.** Данная Инструкция регламентирует условия и порядок осуществления доступа лиц в помещения со средствами информационных систем персональных данных (далее - ИСПДн) в целях обеспечения предотвращения несанкционированного доступа к сведениям, содержащим персональные данные в Исполнительном комитете Агрызского муниципального района Республики Татарстан (далее – Учреждение). При обеспечении доступа лиц соблюдаются требования законодательства РФ по защите персональных данных.

**1.2.** Обеспечение доступа лиц в помещения предусматривает комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности Учреждения и определяет порядок пропуска в помещения работников Учреждения и посетителей.

**1.3.** В помещениях исключено неконтролируемое пребывание посторонних лиц.

**1.4.** Контроль за порядком обеспечения доступа лиц в помещения возлагается на Руководителя Учреждения.

## 2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**2.1. Информация** - сведения (сообщения, данные) независимо от формы их представления.

**2.2. Носитель информации** - любой материальный объект или среда, используемый для хранения или передачи информации.

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

**2.4. Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**2.5. Доступ к информации** – возможность получения информации и ее использования.

**2.6. Несанкционированный доступ (НСД)** – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путем изменения (повышения, фальсификации) своих прав доступа.

**2.7. Автоматизированное рабочее место (АРМ)** – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

## 3. ПОРЯДОК ДОСТУПА В ПОМЕЩЕНИЯ РАБОТНИКОВ И ПОСЕТИТЕЛЕЙ

**3.1.** Не допускается нахождение работников Учреждения в помещениях в нерабочее для них время.

**3.2.** Нахождение посетителей Учреждения в помещениях допускается только в рабочее время.

**3.3.** В помещения ИСПДн пропускаются:

**3.3.1.** беспрепятственно – Руководитель Учреждения и работники, имеющие допуск к работе с персональными данными и с целью выполнения трудовых обязанностей;

**3.3.2.** при наличии удостоверения, с разрешения Руководителя Учреждения, в сопровождении ответственного за обеспечение безопасности персональных данных или администратора безопасности - сотрудники контролирующих органов, сотрудники пожарных и аварийных служб, сотрудники полиции;

**3.3.3.** ограниченно - работники, не имеющие допуска к работе с персональными данными или не имеющие функциональных обязанностей в помещении, работники сторонних организаций и учреждений для выполнения договорных отношений.

**3.4.** Посетители пропускаются в помещения ИСПДн Учреждения в рабочее время в сопровождении работников, допущенных к обработке персональных данных.

**3.5.** В помещениях, в которых происходит обработка и хранение персональных данных, запрещено использование не предусмотренных трудовыми обязанностями технических устройств, фотографирование, видеозапись, звукозапись, в том числе с использованием мобильных телефонов.

## 4. ОРГАНИЗАЦИЯ И ПОРЯДОК ПРОИЗВОДСТВА РЕМОНТНО-СТРОИТЕЛЬНЫХ РАБОТ В ЗДАНИИ

**4.1.** Рабочие и специалисты ремонтно-строительных организаций пропускаются в помещения для проведения ремонтно-строительных работ на основании заявок, подписанных Руководителем Учреждения.

**4.2.** В целях предотвращения несанкционированного доступа к сведениям, содержащим персональные данные, работы проводятся только под контролем ответственного за обеспечение безопасности персональных данных или администратора безопасности.

## 5. ОРГАНИЗАЦИЯ ОХРАНЫ И ДОСТУПА В ПОМЕЩЕНИЯ

**5.1.** Для исключения возможности бесконтрольного проникновения в помещения и к установленному в них оборудованию посторонних лиц, двери в отсутствие штатных работников запираются на ключ. Помещения должны быть оборудованы специальными инженерными средствами, такими как усиленные двери, охранная сигнализация и т.п.

**5.2.** Работники по окончании рабочего дня обязаны убрать все документы в столы, шкафы и сейфы, закрыть окна и форточки, отключить от сети аппаратуру, радиоточки, электроприборы и освещение.

**5.3.** Оборудование в помещениях должно размещаться таким образом, чтобы исключить возможность бесконтрольного доступа к нему посторонних лиц. Мониторы компьютеров должны быть ориентированы таким образом, чтобы исключить возможность просмотра отображаемой на них информации лицами, не имеющими допуска к обработке персональных данных.

**5.4.** Окна помещений, в которых ведется обработка персональных данных, должны быть оборудованы шторами или жалюзи.

**5.5.** Режим работы охраны устанавливается штатным расписанием и должностными инструкциями.

## 6. УБОРКА ПОМЕЩЕНИЙ

**6.1.** Уборка помещений ИСПДн должна производиться под контролем работника, допущенного к обработке персональных данных в этом помещении.

**6.2.** Во время уборки в помещении должна быть приостановлена работа с персональными данными, должны быть выключены или заблокированы все АРМ, на которых обрабатываются персональные данные. Носители, содержащие персональные данные, должны быть убраны в закрытые шкафы или сейфы.

## 7. ТРЕБОВАНИЯ ПО ТЕХНИЧЕСКОМУ УКРЕПЛЕНИЮ

**7.1.** Руководитель Учреждения обеспечивает обязательное выполнение мероприятий по техническому укреплению и оборудованию специальными техническими средствами охраны, системами пожарной безопасности и должен руководствоваться следующими основными требованиями:

**7.1.1.** двери и окна должны иметь прочные и надежные петли, шпингалеты, крючки или задвижки и быть плотно подогнаны к рамам и дверным коробам. Допускается применение электромеханических, электромагнитных замков и задвижек;

**7.1.2.** оконные проемы первых этажей зданий должны быть укреплены металлическими решетками, запираемыми с внутренней стороны, если это не противоречит требованиям пожарной безопасности.

**7.2.** Конструкция оконных рам должна исключать возможность демонтажа с наружной стороны оконного проема стекол.

**7.3.** Стекла в рамах должны быть надежно закреплены в пазах.

**7.4.** Рамы указанных оконных проемов оборудуются запорными устройствами.

Приложение № 4
к распоряжению
Исполнительного комитета
Агрызского муниципального района
Республики Татарстан
от 13.10.2021 № 139-р

**Инструкция**

**обслуживающего персонала информационных систем персональных данных**

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

**1.1.** Настоящий документ разработан в соответствии с нормативными документами по безопасности информации, и определяет порядок обеспечения информационной безопасности при проведении работ обслуживающим персоналом в информационных системах персональных данных (далее – ИСПДн) Исполнительного комитета Агрызского муниципального района Республики Татарстан (далее – Учреждение).

**1.2.** Субъектами доступа к ресурсам ИСПДн являются пользователи, администратор безопасности и обслуживающий персонал (работники, осуществляющие техническое обслуживание, ремонт) в соответствии с утвержденным перечнем.

**1.3.** Обрабатываемая в ИСПДн информация относится к сведениям, составляющим персональные данные (далее – ПДн).

**1.4.** Машинные носители с защищаемой информацией имеют пометку «ПДн».

**1.5.** Работники, осуществляющие ремонт и обслуживание компонентов ИСПДн (обслуживающий персонал) получают доступ к ресурсам ИСПДн по согласованию с администратором безопасности (далее – АБ).

**1.6.** Обслуживающий персонал осуществляет плановые и внеплановые мероприятия по обеспечению работоспособности основных и вспомогательных технических средств, и систем (далее – ОТСС и ВТСС), входящих в состав ИСПДн.

**1.7.** Методическое руководство по информационной безопасности объектов вычислительной техники (далее – ОВТ) осуществляет АБ.

**1.8.** Обслуживающий персонал имеет право вносить предложения по изменению и дополнению данной Инструкции.

**1.9.** Изменения и дополнения к данной Инструкции утверждаются в установленном порядке.

**1.10.**Право толкования положений настоящей Инструкции возлагается на Руководителя Учреждения.

## 2. ТРЕБОВАНИЯ К ОБСЛУЖИВАЮЩЕМУ ПЕРСОНАЛУ

**2.1.** Обслуживающий персонал, не ознакомленный с данной Инструкцией, а также с изменениями и дополнениями к ней, к работе в ИСПДн не допускается.

**2.2.** Обслуживающий персонал обязан выполнять требования АБ.

**2.3.** Обслуживающий персонал обязан периодически (согласно утвержденному плану) производить проверку работоспособности технических средств.

**2.4.** Обслуживающий персонал обязан немедленно реагировать на сообщения АБ о любых неисправностях в работе ИСПДн.

**2.5.** Обслуживающий персонал обязан отчитаться АБ по факту выполнения работ в ИСПДн.

## 3. ДОСТУП К РЕСУРСАМ ИСПДН

**3.1.** Обязательным условием получения доступа к ресурсам ИСПДн обслуживающего персонала является знание технологии обработки информации в ИСПДн с учетом требований информационной безопасности.

**3.2.** Все работы выполняются в присутствии работника, имеющего право доступа к ресурсам ИСПДн.

**3.3.** Обслуживающий персонал не имеет права требовать у пользователей раскрытия их паролей и/или передачи персональных идентификаторов.

**3.4.** Обслуживающий персонал не имеет право требовать у пользователей распечатывать и/или выводить информацию на экран монитора.

**3.5.** Обслуживающий персонал не имеет права требовать у пользователей предоставления любых машинных носителей (далее – МН) информации, в т.ч. во временное использование.

## 4. ПОРЯДОК РАБОТЫ ОБСЛУЖИВАЮЩЕГО ПЕРСОНАЛА

Ниже приводится перечень работ, производимых обслуживающим персоналом с ресурсами ИСПДн.

### 4.1. Обеспечение работоспособности ИСПДн

В соответствии с утвержденным графиком, а также по требованию АБ обслуживающий персонал проводит проверку работоспособности технических средств, используемых на ОВТ. В случае обнаружения неисправностей необходимо произвести следующие действия:

- для устранения неисправности технических средств, требующего нарушения целостности защитной наклейки, необходимо поставить в известность АБ, а в случае его отсутствия – ответственного за обеспечение безопасности персональных данных Учреждения;
- для замены комплектующих, учтенных в «Техническом паспорте…» (за исключением съемного жесткого диска), необходимо изъять ПЭВМ с рабочего места пользователя (при этом жесткий диск сдается АБ по месту хранения отчуждаемых МН) и произвести его ремонт в установленном в организации порядке;
- при устранении неисправности съемного жесткого диска, все работы производятся в присутствии АБ;
- для замены комплектующих, не учтенных в «Техническом паспорте…» (оперативная память, кабели и др.), допускается проведение ремонтных работ на рабочем месте пользователя (в присутствии АБ или ответственного за обеспечение безопасности персональных данных Учреждения).

### 4.2. Обеспечение работоспособности ВТСС и прочие работы

В соответствии с утвержденным графиком, а также по требованию АБ обслуживающий персонал проводит проверку работоспособности ВТСС (датчики сигнализации, соответствующие кабели и др.) и прочие работы в помещении (ремонт системы электропитания, освещения и пр.). При этом необходимо выполнять следующие требования:

- график проведения работ согласовывается с ответственным за обеспечение безопасности персональных данных Учреждения;
- вне графика производится обязательная проверка в случае обнаружения неисправностей в работе ВТСС;
- при установлении неисправности ВТСС необходимо поставить в известность АБ или ответственного за обеспечение безопасности персональных данных Учреждения;
- при демонтаже неисправных ВТСС присутствие АБ является обязательным;
- если для устранения неисправности демонтаж ВТСС не требуется, присутствие АБ или ответственного за обеспечение безопасности персональных данных Учреждения при проведении работ также является обязательным;
- аналогично производятся прочие работы в помещениях.

## 5. ОТВЕТСТВЕННОСТЬ

Обслуживающий персонал несет персональную ответственность за:

- неразглашение сведений, ставших им известными при выполнении своих обязанностей;
- сохранность ресурсов ИСПДн, изъятых для ремонта;
- качество выполняемых работ;
- соблюдение требований данной Инструкции и правомерное использование ресурсов ИСПДн.

Приложение №5
к распоряжению
Исполнительного комитета
Агрызского муниципального района
Республики Татарстан
от 13.10.2021 № 139-р

**Инструкция**
**по работе ответственного лица за организацию обработки персональных данных**

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

**1.1.** Данная Инструкция определяет основные обязанности, права и ответственность ответственного лица за организацию обработки персональных данных Исполнительного комитета Агрызского муниципального района Республики Татарстан (далее – Учреждение).

**1.2.** Ответственное лицо за организацию обработки персональных данных является штатным работником Учреждения и назначается Приказом Руководителя Учреждения.

**1.3.** Ответственное лицо за организацию обработки персональных данных (далее - Ответственный) - лицо, отвечающее за организацию обработки персональных данных с использованием средств автоматизации и без использования таких средств.

**1.4.** Решение вопросов организации защиты персональных данных в Учреждении входит в прямые трудовые обязанности Ответственного.

**1.5.** Ответственный отвечает за поддержание необходимого уровня безопасности объектов защиты, является уполномоченным на проведение соответствующих работ.

**1.6.** Ответственный в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлениями Правительства, руководящими и нормативными документами ФСТЭК России, а также другими нормативно-правовыми актами, действующими на территории Российской Федерации, настоящей Инструкцией и иными регламентирующими документами Учреждения.

**1.7.** Требования Ответственного, связанные с выполнением им своих трудовых обязанностей, обязательны для исполнения всеми работниками, имеющими санкционированный доступ к персональным данным.

**1.8.** Ответственный обладает правами доступа к любым носителям персональных данных Учреждения.

## 2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**2.1. Блокирование персональных данных** - временное прекращение обработки персональных данных.

**2.2. Доступ к информации** – возможность получения информации и ее использования.

**2.3.Защита информации** — деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной

безопасности.

**2.4.Информация** - сведения (сообщения, данные) независимо от формы их представления.

**2.5.Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**2.6.Несанкционированный доступ (НСД)** – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путем изменения (повышения, фальсификации) своих прав доступа.

**2.7.Носитель информации** - любой материальный объект или среда, используемый для хранения или передачи информации.

**2.8.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.

**2.9.Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

**2.10. Средство защиты информации (СЗИ)** – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

**2.11. Уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

## 3. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО

**3.1.**В области автоматизированной обработки персональных данных Ответственный обязан:

3.1.1. взаимодействовать с администратором безопасности и ответственным за обеспечение безопасности персональных данных по вопросам обеспечения и выполнения требований обработки персональных данных;

3.1.2. контролировать осуществление мероприятий по установке и настройке средств защиты;

3.1.3. осуществлять контроль за порядком учета, создания, хранения и использования резервных копий и машинных носителей, содержащих персональные данные.

**3.2.**В области обработки персональных данных без использования средств автоматизации Ответственный обязан:

3.2.1. контролировать порядок обработки бумажных носителей персональных данных;

3.2.2. осуществлять проверки наличия документов, содержащих

персональные данные.

**3.3.**В области информирования работников Ответственный обязан:

3.3.1. доводить до сведения работников Учреждения положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3.3.2. осуществлять методическое руководство работников, имеющих санкционированный доступ к персональным данным, в вопросах обеспечения безопасности персональных данных;

3.3.3. организовывать повышение квалификации работников в области защиты персональных данных.

**3.4.**В области работы с субъектами персональных данных Ответственный обязан:

3.4.1. разъяснять субъекту персональных данных юридические последствия отказа предоставления его персональных данных;

3.4.2. организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

**3.5.**В области контроля работников Ответственный обязан:

3.5.1. планировать мероприятия по организации обеспечения безопасности персональных данных;

3.5.2. организовывать и осуществлять периодический контроль пользователей по соблюдению ими режима конфиденциальности, правил работы со съемными машинными носителями информации, выполнению организационных мер по защите информации, а также принимать участие в проведении проверок уполномоченными структурами;

3.5.3. организовывать работы по плановому контролю работоспособности технических средств защиты персональных данных, охраны объекта, средств защиты информации от несанкционированного доступа.

**3.6.**В области учета лиц, имеющих доступ к персональным данным, Ответственный обязан:

3.6.1. знать и предоставлять на утверждение Руководителю Учреждения изменения к списку лиц, доступ которых к персональным данным необходим для выполнения ими своих трудовых обязанностей;

3.6.2. участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения трудовых обязанностей.

**3.7.**Иные обязанности Ответственного:

3.7.1. по указанию руководства своевременно и точно отражать изменения в локальных нормативно-правовых актах по правилам обработки персональных данных;

3.7.2. знать перечень и условия обработки персональных данных в Учреждении;

3.7.3. осуществлять организацию учёта документов, содержащих персональные данные, их уничтожение, либо контроль процедуры их уничтожения;

3.7.4. выполнять иные мероприятия, требуемые нормативными

документами по защите персональных данных.

## 4. ПРАВА ОТВЕТСТВЕННОГО

Ответственный имеет право:

**4.1.**Запрашивать и получать необходимые материалы для организации и проведения работ по вопросам организации обработки и обеспечения безопасности персональных данных.

**4.2.**Требовать от всех пользователей ИСПДн выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных.

**4.3.**Инициировать блокирование доступа работников к персональным данным, если это необходимо для предотвращения нарушения режима защиты персональных данных.

**4.4.**Участвовать в разработке мероприятий по совершенствованию системы защиты персональных данных.

**4.5.**Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, несанкционированного доступа, утраты, порчи защищаемых носителей персональных данных и технических средств из состава информационных систем или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

**4.6.**Обращаться к руководителю подразделения с предложением о приостановке процесса обработки персональных данных или отстранению от работы пользователя в случаях нарушения установленной технологии обработки персональных данных или нарушения режима конфиденциальности.

**4.7.**Подавать свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищенности персональных данных.

## 5. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

**5.1.**К попыткам несанкционированного доступа относятся:

5.1.1. сеансы работы с персональными данными незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;

5.1.2. действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учетной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

**5.2.**При выявлении факта несанкционированного доступа Ответственный обязан:

5.2.1. по возможности пресечь дальнейший несанкционированный доступ к персональным данным;

5.2.2. доложить Руководителю Учреждения служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

5.2.3. известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;

5.2.4. известить ответственного за обеспечение безопасности персональных данных и администратора безопасности о факте несанкционированного доступа.

## 6. ОТВЕТСТВЕННОСТЬ

**6.1.** Ответственный несет персональную ответственность за:

6.1.1. соблюдение требований настоящей Инструкции,

6.1.2. правильность и объективность принимаемых решений,

6.1.3. качество и своевременность проводимых им работ по обеспечению безопасности персональных данных,

6.1.4. за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

**6.2.** Ответственный при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение №6
к распоряжению
Исполнительного комитета
Агрызского муниципального района
Республики Татарстан
от 13.10.2021 № 139-р

**Инструкция**
**по работе ответственного лица за обеспечение безопасности персональных данных**

## 1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная Инструкция определяет основные обязанности, права и ответственность ответственного лица за обеспечение безопасности персональных данных Исполнительного комитета Агрызского муниципального района Республики Татарстан (далее – Учреждение).

1.1. Ответственное лицо за обеспечение безопасности персональных данных является штатным работником Учреждения и назначается Приказом Руководителя Учреждения.

1.2. Ответственное лицо за обеспечение безопасности персональных данных (далее - Ответственный) - лицо, отвечающее за организацию и состояние процесса обработки персональных данных в информационных системах персональных данных.

1.3. Решение вопросов организации защиты персональных данных, обрабатываемых в информационных системах Учреждения, входит в прямые трудовые обязанности Ответственного.

1.4. Ответственный отвечает за поддержание необходимого уровня безопасности объектов защиты, является уполномоченным на проведение соответствующих работ.

1.5. Ответственный в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлениями Правительства, руководящими и нормативными документами ФСТЭК России, а также другими нормативными правовыми актами, действующими на территории Российской Федерации, настоящей Инструкцией и иными регламентирующими документами Учреждения.

1.6. Требования Ответственного, связанные с выполнением им своих трудовых обязанностей, обязательны для исполнения всеми работниками, имеющими санкционированный доступ к персональным данным.

1.7. Ответственный обладает правами доступа к любым носителям персональных данных Учреждения.

## 2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Блокирование персональных данных** - временное прекращение обработки персональных данных.

2.2. **Доступ к информации** – возможность получения информации и ее использования.

2.3. **Защита информации** — деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.4. **Информация** - сведения (сообщения, данные) независимо от формы их представления.

2.5. **Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.6. **Несанкционированный доступ (НСД)** – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путем изменения (повышения, фальсификации) своих прав доступа.

2.7. **Носитель информации** - любой материальный объект или среда, используемый для хранения или передачи информации.

2.8. **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.

2.9. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

2.10. **Средство защиты информации (СЗИ)** – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

## 3. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО

Ответственный обязан:

**3.1.**Обеспечивать выполнение режимных и организационных мероприятий на месте эксплуатации ИСПДн, а также следить за выполнением требований по условиям размещения средств вычислительной техники и их сохранностью.

**3.2.**Знать и предоставлять ответственному за организацию обработки персональных данных изменения к списку лиц, доступ которых к персональным данным необходим для выполнения трудовых обязанностей.

**3.3.**Проводить инструктаж и консультации пользователей ПЭВМ по соблюдению режима конфиденциальности.

**3.4.**Участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения трудовых обязанностей.

**3.5.**Организовывать периодический контроль пользователей по соблюдению ими режима конфиденциальности, правил работы со съемными машинными носителями информации, выполнению организационных мер по защите информации, а также принимать участие в проведении проверок

уполномоченными структурами.

**3.6.**Взаимодействовать с администратором безопасности по вопросам обеспечения и выполнения требований обработки персональных данных.

**3.7.**Контролировать осуществление мероприятий по установке и настройке средств защиты.

**3.8.**Организовывать работы по плановому контролю работоспособности технических средств защиты персональных данных, охраны объекта, средств защиты информации от несанкционированного доступа.

**3.9.**Контролировать периодическое резервное копирование баз персональных данных и сопутствующей защищаемой информации.

**3.10.**По указанию руководства своевременно и точно отражать изменения в локальных нормативно-правовых актах по управлению средствами защиты информации в ИСПДн и по правилам обработки персональных данных.

**3.11.**Знать перечень и условия обработки персональных данных в Учреждении.

**3.12.**Знать перечень установленных в подразделениях технических средств, входящих в состав информационных систем, и перечень задач, решаемых с их использованием.

**3.13.**Обеспечивать соблюдение работниками утвержденного порядка проведения работ по установке и модернизации аппаратных и программных средств компьютеров и серверов из состава информационных систем.

**3.14.**Осуществлять контроль за порядком учета, создания, хранения и использования машинных носителей, содержащих персональные данные.

**3.15.**При выявлении возможных каналов неправомерного вмешательства в процесс функционирования информационных систем и осуществления несанкционированного доступа к персональным данным и техническим средствам из состава информационных систем подразделения, сообщать о них Руководителю Учреждения.

**3.16.**Инструктировать работников по вопросам обеспечения информационной безопасности и правилам работы с применяемыми средствами зашиты информации.

**3.17.**Знать законодательство Российской Федерации о персональных данных, следить за его изменениями.

**3.18.**Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

**3.19.**Выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

## 4. **ПРАВА ОТВЕТСТВЕННОГО**

Ответственный имеет право:

**4.1.**Требовать от всех пользователей ИСПДн выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных.

**4.2.**Инициировать блокирование доступа работников к персональным данным, если это необходимо для предотвращения нарушения режима защиты персональных данных.

**4.3.**Участвовать в разработке мероприятий по совершенствованию системы защиты персональных данных.

**4.4.**Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, несанкционированного доступа, утраты, порчи защищаемых носителей персональных данных и технических средств из состава информационных систем или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

**4.5.**Обращаться к руководителю подразделения с предложением о приостановке процесса обработки персональных данных или отстранению от работы пользователя в случаях нарушения установленной технологии обработки персональных данных или нарушения режима конфиденциальности.

**4.6.**Подавать свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищенности персональных данных.

## 5. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

5.1. К попыткам несанкционированного доступа относятся:

5.1.1. сеансы работы с персональными данными незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;

5.1.2. действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учетной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

5.2. При выявлении факта несанкционированного доступа Ответственный обязан:

5.2.1. по возможности пресечь дальнейший несанкционированный доступ к персональным данным;

5.2.2. доложить Руководителю Учреждения служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

5.2.3. известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;

5.2.4. известить ответственного за организацию обработки персональных данных и администратора безопасности о факте несанкционированного

доступа.

## 6. ОТВЕТСТВЕННОСТЬ

6.1. Ответственный несет персональную ответственность за:

6.1.1. соблюдение требований настоящей Инструкции,

6.1.2. правильность и объективность принимаемых решений,

6.1.3. качество и своевременность проводимых им работ по обеспечению безопасности персональных данных,

6.1.4. за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

6.2. Ответственный при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение №7
к распоряжению
Исполнительного комитета
Агрызского муниципального района
Республики Татарстан
от 13.10.2021 № 139-р

**Инструкция**
**администратора безопасности информационных систем персональных данных**

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

**1.1.** Настоящий документ разработан в соответствии с нормативными документами по безопасности информации и определяет порядок обеспечения безопасности информации при проведении работ администратором безопасности (далее – АБ) в информационных системах персональных данных (далее – ИСПДн) Исполнительного комитета Агрызского муниципального района Республики Татарстан (далее – Учреждение).

**1.2.** Субъектами доступа к ресурсам ИСПДн являются пользователи, АБ и обслуживающий персонал (работники, осуществляющие техническое обслуживание, ремонт), в соответствии с утвержденным перечнем.

**1.3.** Обрабатываемая в ИСПДн информация относится к сведениям, составляющим персональные данные (далее – ПДн).

**1.4.** Машинные носители с защищаемой информацией имеют пометку «ПДн».

**1.5.** АБ назначается Приказом Руководителя Учреждения и получает неограниченные права на доступ к ресурсам ИСПДн.

**1.6.** АБ осуществляет общее руководство и контроль за обеспечением безопасности информации при работе пользователей ИСПДн и обслуживающего персонала.

**1.7.** Методическое руководство по информационной безопасности объектов информатизации осуществляет АБ.

**1.8.** АБ имеет право вносить предложения по изменению и дополнению данной Инструкции, а также «Инструкции пользователя…» и «Инструкции обслуживающего персонала…».

**1.9.** Изменения и дополнения к данной Инструкции утверждаются в установленном порядке.

**1.10.** Право толкования положений настоящей Инструкции возлагается на Руководителя Учреждения.

## 2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**2.1. Доступ к информации** – возможность получения информации и ее использования.

**2.2. Защита информации** – деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

**2.3. Информация** – сведения (сообщения, данные) независимо от формы

их представления.

**2.4. Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**2.5. Несанкционированный доступ** – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путем изменения (повышения, фальсификации) своих прав доступа.

**2.6. Носитель информации** – любой материальный объект или среда, используемый для хранения или передачи информации.

**2.7. 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.

**2.8. Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

**2.9. Средство защиты информации** – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

**2.10. Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

## 3. ТРЕБОВАНИЯ К АБ

**3.1.** АБ обязан знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите информации.

**3.2.** АБ, не ознакомленный с данной Инструкцией, а также с изменениями и дополнениями к ней, к работе с ресурсами ИСПДн не допускается.

**3.3.** АБ осуществляет учет съемных машинных носителей информации, их уничтожение, либо контроль процедуры их уничтожения.

**3.4.** АБ обязан немедленно реагировать на сообщения пользователей о любых неисправностях в работе основных и вспомогательных средств и систем (далее – ОТСС и ВТСС), СЗИ, системного и прикладного программного обеспечения (далее – ПО) ИСПДн.

**3.5.** АБ обязан немедленно ставить в известность ответственного за обеспечение безопасности персональных данных Учреждения обо всех неисправностях аппаратно-программных средств ИСПДн.

**3.6.** АБ обязан ставить в известность ответственного за обеспечение безопасности персональных данных Учреждения о необходимости проведения

работ по администрированию СЗИ.

**3.7.** АБ имеет право проводить внеплановые проверки работоспособности СЗИ и соблюдения пользователями технологии обработки персональных данных.

**3.8.** АБ разрабатывает планы мероприятий по администрированию и техническому обслуживанию аппаратных и программных средств ИСПДн Учреждения.

**3.9.** АБ обязан в случае отказа технических средств или программного обеспечения элементов ИСПДн, в том числе СЗИ, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

**3.10.** АБ имеет право требовать прекращения обработки персональных данных, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

**3.11.** АБ присутствует при выполнении технического обслуживания элементов ИСПДн сторонними специалистами на территории Учреждения.

**3.12.** АБ осуществляет разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе с СЗИ, или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

**3.13.** В ходе управления (администрирования) системой защиты ИСПДн АБ обязан осуществлять:

3.13.1. заведение и удаление учетных записей пользователей, управление полномочиями пользователей ИСПДн и поддержание правил разграничения доступа в ИСПДн;

3.13.2. создание, присвоение и уничтожение идентификаторов пользователей и устройств, однозначно их идентифицирующих;

3.13.3. управление СЗИ в ИСПДн, в том числе параметрами настройки программного обеспечения, включая программное обеспечение СЗИ, управление учетными записями пользователей, восстановление работоспособности СЗИ, генерацию, смену и восстановление паролей;

3.13.4. изменение аутентификационной информации (средств аутентификации), заданной их производителями и (или) используемой при внедрении системы защиты информации ИСПДн;

3.13.5. установку обновлений программного обеспечения, включая программное обеспечение СЗИ, выпускаемых разработчиками (производителями) СЗИ или по их поручению;

3.13.6. централизованное управление системой защиты информации ИСПДн (при необходимости);

3.13.7. регистрацию и анализ событий в ИСПДн, связанных с защитой информации;

3.13.8. информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации ИСПДн и отдельных СЗИ, а также их обучение;

3.13.9. сопровождение функционирования системы защиты информации

ИСПДн в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации.

**3.14.** В ходе выявления инцидентов и реагирования на них АБ обязан осуществлять:

3.14.1. обнаружение и идентификацию инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и СЗИ, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

3.14.2. своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИСПДн;

3.14.3. анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

3.14.4. планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИСПДн и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

3.14.5. планирование и принятие мер по предотвращению повторного возникновения инцидентов.

**3.15.** В ходе контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИСПДн, АБ обязан осуществлять:

3.15.1. анализ и оценку функционирования системы защиты информации ИСПДн, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации ИСПДн;

3.15.2. проверку работоспособности и параметров настройки программного обеспечения, аппаратных и программных СЗИ ИСПДн;

3.15.3. проверку состава технических средств, программного обеспечения и СЗИ;

3.15.4. контроль целостности печатей (пломб, наклеек) технических средств, используемых для обработки персональных данных;

3.15.5. еженедельное отслеживание появления новых видов уязвимостей ПО ИСПДн. По необходимости АБ производит устранение уязвимостей согласно рекомендациям разработчика, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств. В качестве источников информации об уязвимостях должны использоваться опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, а также другие базы данных уязвимостей;

3.15.6. периодический анализ изменения угроз безопасности информации в ИСПДн, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;

3.15.7. контроль за событиями безопасности и действиями пользователей в ИСПДн. В частности, АБ обязан осуществлять постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации;

3.15.8. контроль (анализ) защищенности информации, содержащейся в ИСПДн;

3.15.9. документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИСПДн;

3.15.10. принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) системы защиты информации ИСПДн, повторной аттестации ИСПДн или проведении дополнительных аттестационных испытаний.

## 4. ДОСТУП К РЕСУРСАМ ИСПДН

**4.1.** Обязательными условиями получения доступа к ресурсам ИСПДн АБ являются:

- право доступа в помещение;
- наличие допуска к персональным данным;
- право доступа к ИСПДн;
- знание технологии обработки информации в ИСПДн с учетом требований информационной безопасности.

**4.2.** Идентификация АБ в ИСПДн осуществляется по уникальному имени и персональному идентификатору (при его наличии).

**4.3.** Длина пароля АБ и всех пользователей – не менее 6 буквенно-цифровых символов.

**4.4.** Уникальное имя, персональный идентификатор (при его наличии) и пароль АБ получает в установленном порядке. АБ обязан их помнить и не допускать раскрытия, не допускается запись на каких-либо носителях в целях напоминания. Во время ввода пароля на клавиатуре должна быть исключена возможность его просмотра другими лицами. Не допускается оставление без присмотра и передача другим лицам персонального идентификатора (при его наличии).

**4.5.** При утере или подозрении на утечку своего имени, пароля или персонального идентификатора АБ должен немедленно изменить свои идентификационные данные и проконтролировать возможные изменения в настройках СЗИ.

**4.6.** Регистрация пользователя осуществляется АБ в соответствии с «Инструкцией по организации парольной защиты» и состоит в определении имени регистрируемого пользователя, присвоении ему персонального идентификатора (при его наличии) и назначении пароля.

**4.7.** При заведении новой учетной записи, АБ должен проверить личность пользователя и его трудовые обязанности.

**4.8.** Пересмотр и, при необходимости, корректировка учетных записей пользователей производится АБ не реже одного раза в 6 месяцев и по мере необходимости.

**4.9.** Предоставление пользователям прав доступа к объектам доступа ИСПДн должно осуществляться на основании задач, решаемых пользователями.

**4.10.** АБ не имеет права требовать у пользователей раскрытия их паролей, а также передачи ему персональных идентификаторов (при их наличии), кроме случая изменения идентификационных данных.

**4.11.** АБ имеет право требовать у пользователя изменения его пароля, но не имеет права самостоятельно изменять его пароль.

## 5. ПОРЯДОК РАБОТЫ АБ С РЕСУРСАМИ ИСПДН

Ниже приводится перечень работ, производимых АБ с ресурсами ИСПДн.

**5.1. Проверка работоспособности и настройка системы доступа к ресурсам ИСПДн**

АБ присваивает пользователям идентификационные данные к ресурсам ИСПДн. При этом должны выполняться следующие требования:

- АБ определяет политику изменения учетных данных пользователей и периодически контролирует ее соблюдение;
- АБ сообщает пользователю его уникальное имя и предоставляет возможность задать пароль, далее кодирует персональный идентификатор (при его наличии) пользователя;
- изменение учетных данных пользователя производится АБ по требованию ответственного за обеспечение безопасности персональных данных Учреждения, а также периодически по утвержденному плану и в случае увольнения работника;
- АБ имеет право в целях тестирования уязвимости системы доступа (выявление простейших паролей) производить попытки взлома паролей пользователей, если попытка взлома была успешной, АБ обязан потребовать у пользователя изменение пароля.

**5.2. Проверка работоспособности и настройка аппаратных и программных средств защиты информации (СЗИ)**

АБ обязан перед началом работ включить и убедиться в работоспособности аппаратных СЗИ, в случае сбоя – работы прекратить.

В случае сбоя СЗИ, таких, как неправильная идентификация пользователей, АБ обязан приостановить обработку защищаемой информации до устранения неисправности. В случае производственной необходимости – отключить СЗИ и лично контролировать проведение работ пользователями.

**5.3. Антивирусная защита ресурсов ИСПДн**

АБ разрабатывает и контролирует реализацию антивирусной политики, а именно:

- настраивает параметры антивирусной программы;
- контролирует работоспособность антивирусной программы;
- немедленно реагирует на сообщения пользователей о подозрительном поведении ПО, а также о появлении любых сообщений антивирусной программы и принимает соответствующие меры;
- имеет право на проведение внеплановой проверки на наличие вирусов;
- периодически (один раз в неделю) контролирует корректность

процесса обновления антивирусных баз, а также исполняемых модулей антивирусной программы.

**5.4. Хранение дистрибутивов программного обеспечения СЗИ**

АБ должен хранить дистрибутивы программного обеспечения СЗИ и прикладного программного обеспечения, установленного в ИСПДн Учреждения в месте, исключающем доступ посторонних лиц.

**5.5. Проверка целостности системного и прикладного ПО**

Контролю целостности подлежат файлы ПО ИСПДн с расширениями: *.exe, *.com, *.dll, *.sys, *.vxd, *.drv из каталогов: Windows, Program Files.

**5.6. Резервное копирование и восстановление информации**

Резервное копирование производится регулярно с заданной периодичностью, а также в случае производственной необходимости. При этом необходимо выполнять следующие требования:

- обязательное резервное копирование производится в случае обнаружения неисправностей в работе ПЭВМ или отчуждаемых машинных носителей (далее – МН);
- допускается обоснованное внеплановое резервное копирование информации как по инициативе пользователя, так и АБ, если это не нарушает технологию обработки информации;
- резервные копии пользовательской информации и информации операционной системы хранятся на учтенных внешних МН;
- ответственным лицом за хранение резервных копий является АБ.

По мере устранения неисправностей ПЭВМ АБ производит восстановление информации ограниченного доступа с резервных копий.

Восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), производится, в том числе с использованием резервных копий и (или) дистрибутивов.

АБ разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования информационной системы в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

**5.7. Конфигурирование ИСПДн**

Конфигурационной единицей являются услуги, оборудование, программное обеспечение, здания, люди, документы и пр.

Управление изменениями конфигурации осуществляет ответственный за обеспечение безопасности. Планирование реализации и непосредственно реализация необходимых изменений возлагается на АБ.

В ходе управления конфигурацией аттестованной информационной системы и ее системы защиты информации АБ обязан осуществлять:

- поддержание конфигурации ИСПДн и ее системы защиты информации (структуры системы защиты информации ИСПДн, состава, мест установки и параметров настройки СЗИ, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации ИСПДн и ее системы защиты информации);
- управление изменениями базовой конфигурации ИСПДн и ее системы

защиты информации, в том числе определение типов возможных изменений базовой конфигурации ИСПДн и ее системы защиты информации, санкционирование внесения изменений в базовую конфигурацию ИСПДн и ее системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию ИСПДн и ее системы защиты информации, сохранение данных об изменениях базовой конфигурации ИСПДн и ее системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию ИСПДн и ее системы защиты информации;

– анализ потенциального воздействия планируемых изменений в базовой конфигурации ИСПДн и ее системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИСПДн;

– определение параметров настройки программного обеспечения, включая программное обеспечение СЗИ, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИСПДн и ее системы защиты информации;

– внесение информации (данных) об изменениях в базовой конфигурации ИСПДн и ее системы защиты информации в документацию на систему защиты информации ИСПДн;

– принятие решения по результатам управления конфигурацией о повторной аттестации ИСПДн или проведении дополнительных аттестационных испытаний.

Обязанности по управлению изменениями в аппаратном и программном обеспечении и всех элементах документации, которые связаны с работой, поддержкой и сопровождением систем, находящихся в эксплуатации, возлагаются на АБ. При возникновении необходимости изменения конфигурации ИСПДн, аттестованной по требованиям безопасности информации, АБ согласовывает планируемые изменения с предприятием-лицензиатом, проводившим аттестационные испытания.

### 5.8. Вывод ресурсов ИСПДн из эксплуатации

При невозможности ремонта различных ресурсов ИСПДн АБ обязан:

- физически уничтожать любые МН, независимо от содержащейся на них информации; картриджи принтера, иные комплектующие могут быть использованы за пределами ИСПДн;
- факт выхода из строя и замены оборудования должен быть отражен в Техническом паспорте на ИСПДн.

### 5.9. Реагирование на сбои при регистрации событий безопасности

Реагирование на сбои при регистрации событий безопасности осуществляется АБ путем изменения параметров сбора, записи и хранения информации о событиях безопасности в журналах СЗИ от НСД, в том числе отключение записи информации о событиях безопасности от части компонентов ИСПДн, запись поверх устаревших хранимых записей событий безопасности.

В случае выявления признаков инцидентов безопасности, АБ обязан:

- немедленно уведомить Руководителя о данном факте;
- по возможности в максимально сжатые сроки установить причину

возникновения инцидента и исключить возможность его повторения;

- восстановить работоспособность ИСПДн;
- по окончании работ по восстановлению работоспособности ИСПДн произвести запись в соответствующих журналах.

## 6. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

**6.1.** К попыткам несанкционированного доступа относятся:

- сеансы работы с ИСПДн незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;
- действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учетной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

**6.2.** При выявлении факта несанкционированного доступа АБ обязан:

- пресечь дальнейший несанкционированный доступ к ИСПДн;
- доложить ответственному за обеспечение безопасности персональных данных Учреждения служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;
- известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа.

## 7. ОТВЕТСТВЕННОСТЬ

**7.1.** АБ несет персональную ответственность за:

- сохранность носителей информации и содержащейся на них информации в рабочее время;
- несоблюдение требований данной Инструкции и неправомерное использование ресурсов ИСПДн;
- средства защиты информации, применяемые в ИСПДн Учреждения;
- качество проводимых работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени учетной записи АБ в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования учетной записи.

**7.2.** АБ при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение №8
к распоряжению
Исполнительного комитета
Агрызского муниципального района
Республики Татарстан
от 13.10.2021 № 139-р

**Инструкция**
**по разграничению доступа пользователей к средствам защиты и информационным ресурсам**

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Данная Инструкция определяет порядок организации работ по разграничению доступа пользователей к средствам защиты и информационным ресурсам, обрабатываемым в информационных системах персональных данных (далее – ИСПДн) Исполнительного комитета Агрызского муниципального района Республики Татарстан (далее – Учреждение).

2. Основными видами угроз безопасности информационных систем являются:

- противоправные действия посторонних лиц;
- ошибочные действия пользователей ИСПДн;
- отказы и сбои технических средств ИСПДн, приводящие к ее модификации, блокированию, уничтожению или несанкционированному копированию, а также нарушению правил эксплуатации ЭВМ и сетевого оборудования.

3. Целью защиты информации является:

- предотвращение утечки, хищения, утраты, подделки информации, а также неправомерных действий по уничтожению, модификации, искажению, несанкционированному копированию, блокированию информации, предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы обеспечения правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в ИСПДн Учреждения;
- сохранение конфиденциальности информации в соответствии с законодательством Российской Федерации;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

4. Ответственность за соблюдение требований по защите информации ограниченного доступа и надлежащего порядка проводимых работ возлагается на пользователей ИСПДн, администратора безопасности (далее – АБ) и ответственного за обеспечение безопасности персональных данных Учреждения.

5. Субъекты доступа, получающие доступ к базам данных и другим информационным ресурсам, должны изучить «Инструкцию пользователя

информационных систем персональных данных» и оставить письменное подтверждение (подпись) о неразглашении ими информации, к которой они имеют доступ, паролей, а также в том, что за нарушение правил информационной безопасности и данной Инструкции они несут персональную ответственность в соответствии с законодательством Российской Федерации.

## 2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1. **Информация** - сведения (сообщения, данные) независимо от формы их представления.
2. **Носитель информации** - любой материальный объект или среда, используемый для хранения или передачи информации.
3. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.
4. **Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
5. **Доступ к информации** – возможность получения информации и ее использования.
6. **Несанкционированный доступ (НСД)** – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путем изменения (повышения, фальсификации) своих прав доступа.

## 3. РАЗГРАНИЧЕНИЕ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К ИНФОРМАЦИОННЫМ РЕСУРСАМ И СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ

1. Защита от несанкционированного доступа осуществляется:

− идентификацией и проверкой подлинности пользователей ИСПДн при доступе к информационным ресурсам Учреждения;

− разграничением доступа к обрабатываемым базам данных. Пользователь ИСПДн имеет доступ только к тем информационным ресурсам, которые разрешены для него согласно Матрице доступа. Для осуществления доступа к информационным ресурсам, АБ назначает конкретному пользователю ИСПДн идентифицирующее имя пользователя, кодирует персональный идентификатор (при его наличии) и предоставляет возможность задать пароль;

− АБ должен осуществлять мероприятия по обеспечению защиты информационных ресурсов Учреждения от несанкционированного доступа и непреднамеренных изменений, и разрушений, а также иметь в наличии средства восстановления, резервные копии, предусматривающие процедуру восстановления свойств информационных ресурсов после сбоев и отказов оборудования.

## 4. ОБЕСПЕЧЕНИЕ СОХРАННОСТИ ИНФОРМАЦИИ

1. Для обеспечения сохранности электронных информационных

ресурсов Учреждения необходимо соблюдать следующие требования:

- АБ должен иметь не менее двух резервных копий программного обеспечения для работы с информационными ресурсами, хранимых в разных помещениях, а также методику восстановления данных;

- резервное копирование информационных ресурсов Учреждения должно производиться в соответствии с документацией на используемое программное обеспечение;

- в случае сбоя или порчи восстановление информационных ресурсов из резервных копий производится в соответствии с документацией на используемое программное обеспечение с составлением акта;

- для копирования информации должны использоваться только проверенные на наличие компьютерных вирусов и других вредоносных программ носители информации.

2. Субъектам доступа запрещается:

- установка и использование при работе с компьютерами вредоносных программ, ведущих к блокированию работы системы;

- самовольное изменение сетевых адресов;

- самовольное вскрытие блоков компьютеров, модернизация или модификация компьютеров и программного обеспечения;

- несанкционированная передача компьютеров с прописанными сетевыми настройками. Передача компьютеров производится только АБ с предварительно удаленными сетевыми настройками.

3. Сведения, содержащиеся в электронных документах, и базы данных Учреждения должны использоваться только в служебных целях в рамках полномочий работника, работающего с соответствующими материалами.

Приложение № 9

Исполнительного комитета
Агрызского муниципального района
Республики Татарстан
от 13.10.2021 №139-р
к распоряжению

**Инструкция**

**по учету машинных носителей и регистрации их выдачи**

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящая Инструкция регламентирует порядок учета, хранения и регистрации выдачи машинных носителей персональных данных Исполнительного комитета Агрызского муниципального района Республики Татарстан (далее – Учреждение).

2. Под машинными носителями в настоящей Инструкции понимаются следующие носители информации:

- оптические диски (CD, DVD) однократной и многократной записи;
- жесткие диски автоматизированных рабочих мест (далее - АРМ);
- USB-flash носители информации и др.

## 2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1. **Информация** - сведения (сообщения, данные) независимо от формы их представления.
2. **Носитель информации** - любой материальный объект или среда, используемый для хранения или передачи информации.
3. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.
4. **Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
5. **Уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

## 3. ПОРЯДОК ХРАНЕНИЯ И УЧЕТА МАШИННЫХ НОСИТЕЛЕЙ

1. Машинные носители, содержащие персональные данные, подлежат обязательному учету администратором безопасности ИСПДн.

2. Носители, содержащие персональные данные, должны иметь специальную маркировку. Тип маркировки выбирается администратором безопасности ИСПДн.

3. Оптические диски и USB-flash носители информации храниться в сейфе, расположенном в помещении Учреждения, и изыматься только для выполнения трудовых обязанностей.

4. При поступлении нового машинного носителя, который будет использоваться для хранения или передачи персональных данных, администратор безопасности ИСПДн регистрирует его в «Журнале учета машинных носителей».

5. Машинные носители, которые не являются необходимыми для выполнения трудовых обязанностей, хранятся в сейфе не более одного года, после чего их необходимо уничтожить без возможности восстановления с последующей регистрацией в «Журнале учета машинных носителей».

## 4. ПОРЯДОК РЕГИСТРАЦИИ ВЫДАЧИ МАШИННЫХ НОСИТЕЛЕЙ

1. Учет выдачи машинных носителей ведется в «Журнале учета машинных носителей», в котором указывается маркировка носителя, дата, время, фамилия, имя и отчество должностного лица, получившего материальный носитель, его роспись.

2. В случае возврата должностным лицом машинного носителя в «Журнале учета машинных носителей» администратором безопасности ИСПДн проставляется отметка о возврате с указанием даты, времени возврата, личных подписей передающей и принимающей стороны.

## 5. ПОРЯДОК УНИЧТОЖЕНИЯ (СТИРАНИЯ) ИНФОРМАЦИИ НА МАШИННЫХ НОСИТЕЛЯХ

1. Учреждением должно обеспечиваться уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации.

2. Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления информации конфиденциального характера (защищаемая информация) при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации.

3. Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных машинных носителях информации.

4. Перед подключением к информационной системе Учреждением должно быть обеспечено уничтожение (стирание) информации с носителей информации после их приобретения и при первичном подключении к информационной системе, при использовании в иных информационных системах, при передаче для постоянного использования от одного пользователя другому пользователю, после возвращения из ремонта, а также в иных случаях, предусмотренных Учреждением.

5. Машинные носители, не подлежащие очистке (не перезаписываемые машинные носители информации, такие как оптические диски типа CD-R) должны быть уничтожены.

6. В Учреждении для уничтожения (стирания) информации на машинных носителях, исключающего возможность восстановления информации конфиденциального характера, должна производиться перезапись уничтожаемых (стираемых) файлов случайной битовой последовательностью в один цикл, удаление записи о файлах, обнуление журнала файловой системы или полная перезапись всего адресного пространства машинного носителя информации случайной битовой последовательностью в один цикл с последующим форматированием.

## 6. ОТВЕТСТВЕННОСТЬ

1. Персональную ответственность за соблюдение требований настоящей Инструкции несет администратор безопасности ИСПДн Учреждения.

2. За разглашение персональных данных и нарушение порядка обращения с машинными носителями, содержащими персональные данные, администратор безопасности ИСПДн может быть привлечен к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

Приложение № 10
к распоряжению
Исполнительного комитета
Агрызского муниципального района
Республики Татарстан
от 13.10.2021 № 139-р

**Инструкция**
**пользователя информационных систем персональных данных**

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ разработан в соответствии с нормативными документами по безопасности информации и определяет порядок обеспечения информационной безопасности при проведении работ пользователями информационных систем персональных данных (далее – ИСПДн) Исполнительного комитета Агрызского муниципального района Республики Татарстан (далее – Учреждение).

1.2. Субъектами доступа к ресурсам ИСПДн являются администратор безопасности (далее – АБ), пользователи и обслуживающий персонал.

1.3.Обрабатываемая в ИСПДн информация относится к сведениям, составляющим персональные данные (далее – ПДн).

1.4.Машинные носители информации имеют пометку «ПДн».

1.5. Пользователи получают свои права на доступ к ресурсам ИСПДн через АБ.

1.6. Пользователи имеют право письменно вносить предложения по изменению и дополнению данной Инструкции.

1.7. Изменения и дополнения к данной Инструкции утверждаются в установленном порядке.

1.8. Право толкования положений настоящей Инструкции возлагается на Руководителя Учреждения.

## 2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

**2.2. Автоматизированное рабочее место (АРМ)** – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

**2.3. Доступ к информации** – возможность получения информации и ее использования.

2.4. **Защита информации** — деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

**2.5. Информация** - сведения (сообщения, данные) независимо от формы их представления.

**2.6. Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических

средств.

**2.7. Несанкционированный доступ (НСД)** – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путем изменения (повышения, фальсификации) своих прав доступа.

**2.8. 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.

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

**2.10. Средство защиты информации (СЗИ)** – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

## 3. ОБЯЗАННОСТИ

Пользователь обязан:

**3.1.** Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите информации.

**3.2.** Выполнять на автоматизированном рабочем месте (далее – АРМ) только те процедуры, которые определены технологическим процессом обработки ПДн.

**3.3.** Знать и соблюдать установленные требования к обработке ПДн, учету и хранению носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

**3.4.** Соблюдать требования парольной политики в соответствии с «Инструкцией по организации парольной защиты».

**3.5.** Получить уникальное имя и персональный идентификатор (при его наличии) от АБ. Пользователь обязан помнить и соблюдать в тайне свои имена и пароли, не допускается их запись на каких-либо носителях в целях напоминания.

**3.6.** Во время работы располагать экран монитора так, чтобы затруднить посетителям просмотр отображаемой информации. Жалюзи на окнах должны быть закрыты.

**3.7.** При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с АБ ИСПДн провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля - уведомить о результатах АБ ИСПДн для определения им факта наличия или отсутствия

вредоносного программного обеспечения.

3.8. В случае появления информационного окна средства антивирусной защиты, сигнализирующем об обнаружении вредоносного программного обеспечения:

3.8.1. приостановить обработку данных;

3.8.2. немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения АБ ИСПДн, владельца зараженных файлов, а также смежные структурные подразделения, использующие эти файлы в работе;

3.8.3. совместно с владельцем файлов, зараженных вредоносным программным обеспечением, провести анализ необходимости дальнейшего их использования;

3.8.4. произвести лечение или уничтожение зараженных файлов (для выполнения требований данного пункта привлечь АБ ИСПДн).

**3.9.** Немедленно вызывать АБ ИСПДн и поставить в известность руководителя структурного подразделения при обнаружении:

**3.9.1.** нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищаемой АРМ;

**3.9.2.** несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;

**3.9.3.** отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

**3.9.4.** некорректного функционирования установленных на АРМ технических средств защиты;

**3.9.5.** непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств.

**3.10.** При утере или подозрении на утечку своего имени, пароля и персональных идентификаторов пользователь должен немедленно сообщить об этом АБ.

**3.11.** Обо всех выявленных нарушениях, связанных с информационной безопасностью Учреждения, а так же для получения консультаций по вопросам информационной безопасности, необходимо обратиться к АБ.

**3.12.** При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

3.13. В ИСПДн осуществляется блокирование сеанса доступа пользователя после 20 минут его бездействия (неактивности) в информационной системе.

**3.14.** Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий в пределах возложенных на него функций.

**3.15.** Пользователям **запрещается**:

– разглашать **защищаемую информацию** посторонним лицам;

– копировать защищаемую информацию на неучтенные внешние носители;

– самостоятельно устанавливать, тиражировать или модифицировать программное и аппаратное обеспечение, изменять установленный порядок функционирования технических и программных средств;

– подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;

– отключать (блокировать) средства защиты информации;

– выполнять на АРМ работы, не предусмотренные технологическим процессом обработки ПДн;

– сообщать (или передавать) посторонним лицам параметры своей учетной записи (имя, персональный идентификатор (при его наличии) и пароль) в ИСПДн;

– оставлять без присмотра и передавать другим лицам персональный идентификатор;

– привлекать посторонних лиц для ремонта или настройки АРМ без согласования с ответственным за обеспечение безопасности ПДн;

– оставлять без присмотра свое АРМ, не активизировав блокировку доступа, или оставлять свое АРМ включенным по окончании работы;

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению безопасности персональных данных.

## 4. ПОРЯДОК РАБОТЫ ПОЛЬЗОВАТЕЛЯ С РЕСУРСАМИ ИСПДН

### 4.1. Начало работы на ПЭВМ

При включении ПЭВМ необходимо дождаться завершения загрузки и готовности системы защиты информации (далее – СЗИ) и операционной системы (далее – ОС) к идентификации пользователя. Идентификация пользователя осуществляется по уникальному имени и паролю с использованием персонального идентификатора, если таковой предусмотрен комплектацией СЗИ. Для получения доступа к ресурсам ИСПДн пользователь должен приложить к считывателю персональный идентификатор (при его наличии) и ввести с клавиатуры свой пароль. Если после ввода пароля СЗИ выдаст сообщение об ошибке, пользователь должен обратиться к АБ.

### 4.2. Завершение работы на ПЭВМ

По окончании работы пользователь должен либо завершить штатными средствами сеанс своей работы (без выключения ПЭВМ), либо завершить работу ПЭВМ стандартным способом (при этом выключить ПЭВМ).

### 4.3. Требования к распечатыванию информации

Все распечатываемые документы должны быть учтены. Бракованные бумажные носители и черновики документов должны быть уничтожены.

При отсутствии пользователя на рабочем месте либо в присутствии лиц, не

имеющих допуска к ресурсам ИСПДн, все документы, содержащие ПДн, должны быть недоступны для просмотра и иного их использования.

## 5. ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ

**5.1.** Личные пароли доступа к элементам ИСПДн выдаются пользователям АБ или создаются самостоятельно.

**5.2.** Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 12 месяцев.

**5.3.** Правила формирования пароля:

– пароль должен состоять не менее чем из 6 символов;

– в пароле должны присутствовать символы из числа прописных и строчных букв английского алфавита от A до Z; десятичных цифр (от 0 до 9); символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %);

– запрещается использовать в качестве пароля имя учетной записи, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения пользователей ИСПДн и их родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно вычислить, основываясь на информации о пользователе;

– запрещается использовать в качестве пароля один и тот же повторяющийся символ, либо повторяющуюся комбинацию из нескольких символов;

– запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

– запрещается выбирать пароли, которые уже использовались ранее.

**5.4.** Правила ввода пароля:

– ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;

– во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами.

**5.5.** Правила хранения пароля:

– запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

– запрещается сообщать другим пользователям личный пароль и/или регистрировать их в системе под своей учетной записью.

**5.6.** Лица, использующие паролирование, обязаны:

– четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;

– своевременно сообщать АБ об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

## 6. ОТВЕТСТВЕННОСТЬ

**6.1.** Пользователь несет персональную ответственность за:

– сохранность носителей информации и содержащейся на них информации (в рабочее время);

– соблюдение требований данной Инструкции, неправомерное

использование ресурсов ИСПДн и за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

**6.2.** За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн, содержащими персональные данные, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

Приложение №11
к распоряжению
Исполнительного комитета
Агрызского муниципального района
Республики Татарстан
от 13.10.2021 №139-р

**Инструкция**
**о порядке работы с персональными данными**

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

2. Данная Инструкция разработана с целью защиты интересов Исполнительного комитета Агрызского муниципального района Республики Татарстан (далее – Учреждение) и субъектов персональных данных, в целях предотвращения раскрытия (передачи), а также соблюдения надлежащих правил обращения с персональными данными.

3. Данная Инструкция предназначена для использования всеми работниками Учреждения, допущенными к работе с персональными данными.

4. Отнесение информации к сведениям, содержащим персональные данные, осуществляется в соответствии с «Перечнем персональных данных…».

5. Работники Учреждения, доступ которых к персональным данным необходим для выполнения ими своих трудовых обязанностей, должны быть ознакомлены под роспись с настоящей Инструкцией и предупреждены о возможной ответственности за ее нарушение.

## – ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1. **Информация** - сведения (сообщения, данные) независимо от формы их представления.
2. **Доступ к информации** – возможность получения информации и ее использования.
3. **Носитель информации** - любой материальный объект или среда, используемый для хранения или передачи информации.
4. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.
5. **Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
6. **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.
7. **Уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате

которых уничтожаются материальные носители персональных данных.

## – ПОРЯДОК РАБОТЫ СО СВЕДЕНИЯМИ, СОДЕРЖАЩИМИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

1. При обработке персональных данных на бумажных и съемных носителях (дискетах, дисках, USB flash носителях и т.п.), компьютерах и других технических средствах, работники Учреждения обязаны следить как за сохранностью самих бумажных документов, съемных носителей, компьютеров и других технических средств, так и за сохранностью содержащейся в них информации, а именно не допускать неправомерного ознакомления с ней лиц, не имеющих допуска к работе с персональными данными.

2. Запрещается хранение или оставление бумажных документов и съемных носителей, содержащих персональные данные, в виде, позволяющем осуществить визуальный просмотр содержащихся в них персональных данных, их фотографирование или несанкционированное создание копий. Напечатанные документы, содержащие персональные данные, должны изыматься из принтеров немедленно. Хранение бумажных документов и съемных носителей, содержащих персональные данные, допускается только в специальных закрытых шкафах, сейфах и помещениях, к которым исключен доступ лиц, не допущенных к обработке соответствующих персональных данных.

3. Запрещается без прямой служебной необходимости делать выписки персональных данных, распечатывать документы с персональными данными или записывать персональные данные на съемные носители.

4. Запрещается использовать для передачи персональных данных съемные носители, не учтенные в соответствии с «Инструкцией по учету машинных носителей…».

5. Запрещается выносить документы, съемные носители или переносные компьютеры, содержащие персональные данные, за пределы служебных помещений Учреждения, если это не требуется для выполнения трудовых обязанностей и если на это не дано разрешение ответственного за организацию обработки персональных данных Учреждения.

6. Бумажные документы с персональными данными, у которых истек срок хранения, лишние или испорченные копии документов с персональными данными, должны быть уничтожены без возможности их восстановления (например, в шредерах).

7. Бумажные документы с персональными данными, съемные носители с персональными данными, а также встроенные в компьютеры носители с персональными данными должны уничтожаться под контролем ответственного за организацию обработки персональных данных способом, исключающим дальнейшее восстановление информации.

8. Мониторы компьютеров, использующихся для обработки персональных данных, должны быть ориентированы таким образом, чтобы исключить визуальный просмотр информации с них лицами, не имеющими допуска к обработке персональных данных.

9. Категорически запрещается упоминать в разговоре с посторонними лицами сведения, содержащие персональные данные.

10. Запрещается в нерабочее время или за пределами служебных помещений упоминать в разговоре с кем-либо, включая любых работников

Учреждения, сведения, содержащие персональные данные.

11. Запрещается обсуждать порядок доступа, места хранения, средства и методы защиты персональных данных с кем-либо, кроме ответственного за организацию обработки персональных данных, ответственного за обеспечение безопасности персональных данных, администратора безопасности, руководства, или лица, уполномоченного руководством на обсуждение данных вопросов.

## – ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

**1.** Работники Учреждения, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъектов, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с федеральными законами Российской Федерации.

**2.** Руководитель Учреждения за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.

Приложение №12
к распоряжению
Исполнительного комитета
Агрызского муниципального района
Республики Татарстан
от 13.10.2021 № 139-р

# Инструкция
# по организации антивирусной защиты

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ разработан в соответствии с нормативными документами по безопасности информации и определяет требования к организации защиты информационной системы персональных данных (далее – ИСПДн) Исполнительного комитета Агрызского муниципального района Республики Татарстан (далее – Учреждение) от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (далее – вредоносное ПО), устанавливает ответственность администратора безопасности (далее – АБ) за выполнение указанных требований.

1.2. К использованию в Учреждении допускаются только лицензионные средства антивирусной защиты, централизованно закупленные у разработчиков или поставщиков данных средств.

1.3. Установка средств антивирусного контроля на компьютеры и серверы ИСПДн Учреждения осуществляется АБ или под его контролем, настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств и требованиями нормативных документов ФСТЭК РФ в области защиты персональных данных.

## 2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**2.1. Антивирусная защита** – комплекс мер, направленных на предотвращение, обнаружение и обезвреживание действий вредоносного ПО при помощи антивирусных программных продуктов.

**2.2. Автоматизированное рабочее место (АРМ)** – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

**2.3. Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**2.4. Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

## 3. ПРИМЕНЕНИЕ СРЕДСТВ АНТИВИРУСНОГО КОНТРОЛЯ

3.1. Антивирусный контроль должен осуществляться в режиме постоянной антивирусной защиты. Ежедневно в начале работы при загрузке компьютера (для серверов – при перезапуске) в автоматическом режиме должна проводиться проверка

загружаемых модулей операционной системы.

3.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), хранящаяся на АРМ, передающаяся по сети, а также информация на съемных носителях. Контроль входящей информации должен осуществляться автоматически, непосредственно после ее приема.

3.3. Процедура обновления баз данных средства антивирусной защиты должна проводиться не реже одного раза в день на всех АРМ ИСПДн, работающих в сети, не реже одного раза в неделю для всех АРМ ИСПДн, работающих автономно.

3.4. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено АБ на предмет отсутствия вредоносного программного обеспечения. Непосредственно после установки (изменения) программного обеспечения должна быть выполнена антивирусная проверка на всех защищаемых серверах и АРМ ИСПДн.

3.5. При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) пользователь обязан самостоятельно или вместе с АБ провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля - уведомить о результатах АБ для определения им факта наличия или отсутствия вредоносного программного обеспечения.

## 4. ОТВЕТСТВЕННОСТЬ

4.1. Ответственность за проведение мероприятий антивирусного контроля и настройку средств антивирусного контроля в ИСПДн Учреждения в соответствии с требованиями настоящей Инструкции возлагается на АБ.

4.2. Периодический контроль за состоянием антивирусной защиты (обновление антивирусной программы и антивирусных баз, а также проверка работоспособности средств антивирусной защиты) в ИСПДн Учреждения, осуществляется АБ.

Приложение №13
к распоряжению
Исполнительного комитета
Агрызского муниципального района
Республики Татарстан
от 13.10.2021 № 139-р

# Инструкция
# по организации парольной защиты

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ разработан в соответствии нормативными документами по безопасности информации и регламентирует процессы генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных (далее – ИСПДн) Исполнительного комитета Агрызского муниципального района Республики Татарстан (далее – Учреждение), а также контроль над действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.2. Осуществление процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора безопасности ИСПДн.

## 2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

**2.2. Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

**2.3. Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**2.4. Пароль** – секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

**2.5. Компрометация пароля** – раскрытие, обнаружение или утеря пароля.

## 3. ПРАВИЛА ФОРМИРОВАНИЯ ПАРОЛЕЙ

3.1. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями информационной системы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные

слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в шести позициях.

3.2. Работникам допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например, Кожзгсф7!).

3.3. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора безопасности ИСПДн.

3.4. Для обеспечения возможности использования имен и паролей некоторых работников в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), работники обязаны сразу же после установки своих паролей передавать их на хранение вместе с именами своих учетных записей администратору безопасности ИСПДн в запечатанном конверте или опечатанном пенале. Опечатанные конверты (пеналы) с паролями работников должны храниться в сейфе, к которому исключен доступ других работников Учреждения и посторонних лиц. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при их наличии), либо печать администратора безопасности ИСПДн. Все конверты (пеналы) с паролями в обязательном порядке фиксируются в «Журнале учета паролей пользователей…».

## 4. ВВОД ПАРОЛЯ

4.1. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его просмотра посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

4.2. При неверном вводе пароля более 5 раз, учетная запись пользователя должна блокироваться не менее чем на 3 минуты и не более чем на 15 минут.

## 5. ПОРЯДОК СМЕНЫ ЛИЧНЫХ ПАРОЛЕЙ

5.1. Смена паролей должна проводиться регулярно, не реже одного раза в 12 месяцев, самостоятельно каждым пользователем.

5.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учетной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

5.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственного за обеспечение безопасности персональных данных, администратора безопасности и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

5.4. Администратор безопасности ИСПДн ведет «Журнал учета паролей пользователей...», в котором он отмечает причины внеплановой смены паролей пользователей.

5.5. Временный пароль, заданный администратором безопасности ИСПДн при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

## 6. ХРАНЕНИЕ ПАРОЛЯ

6.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других носителях информации.

6.2. Запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей.

6.3. Запрещается регистрировать других пользователей в ИСПДн со своим личным паролем, запрещается входить в ИСПДн под учетной записью и паролем другого пользователя.

## 7. ДЕЙСТВИЯ В СЛУЧАЕ УТЕРИ И КОМПРОМЕТАЦИИ ПАРОЛЯ

7.1. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

## 8. ОТВЕТСТВЕННОСТЬ

**8.1.** Каждый пользователь ИСПДн несет персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения компрометации пароля его учетной записи.

**8.2.** Ответственность за контроль проведения мероприятий по организации парольной защиты в отделах возлагается на ответственного за обеспечение безопасности персональных данных.

**8.3.** За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн, обрабатывающими персональные данные, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.