КОЗЛОВСКИЙ ВЕСТНИК

ГАЗЕТА ОСНОВАНА В НОЯБРЕ 2007 ГОДА

2024 год
23 декабря
№ 40
часть 4

СЕГОДНЯ В НОМЕРЕ:

РАСПОРЯЖЕНИЯ, ПОСТАНОВЛЕНИЯ, ИЗВЕЩЕНИЯ И ДРУГИЕ НОРМАТИВНО-ПРАВОВЫЕ АКТЫ

ПЕРИОДИЧЕСКОЕ ПЕЧАТНОЕ ИЗДАНИЕ «КОЗЛОВСКИЙ ВЕСТНИК»
АДРЕС РЕДАКЦИОННОГО СОВЕТА И ИЗДАТЕЛЯ: 429430, Г. КОЗЛОВКА, УЛ.ЛЕНИНА, 55 E-MAIL: KOZLOV@CAP.RU
УЧРЕДИТЕЛЬ: АДМИНИСТРАЦИЯ КОЗЛОВСКОГО РАЙОНА ЧУВАШСКОЙ РЕСПУБЛИКИ
ПРЕДСЕДАТЕЛЬ РЕДАКЦИОННОГО СОВЕТА: ДМИТРИЕВ Е.Ю.
ВЫПУСК ОТ
ОБЪЕМ ____ П.Л. ФОРМАТ А-4

АДМИНИСТРАЦИЯ КОЗЛОВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА
РАСПОРЯЖЕНИЕ
18.12.2024 №454 **г. Козловка**

О введении режима защиты персональных данных

Во исполнение требований Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»:

1. Ввести в Администрации Козловского муниципального округа Чувашской Республики режим защиты персональных данных в соответствии с законодательством РФ о персональных данных.
2. Осуществить режим защиты персональных данных в отношении данных, перечисленных в Положении об обработке персональных данных Администрации Козловского муниципального округа Чувашской Республики.
3. Назначить администратором безопасности информационных систем персональных данных (ИСПДн) и ответственным за обеспечение безопасности персональных данных в информационных системах - ведущего специалиста-эксперта сектора цифрового развития и информационных технологий администрации Козловского муниципального округа Чувашской Республики.
4. Назначить администратором ИСПДн «Опека и попечительство» - заведующего сектором опеки и попечительства администрации Козловского муниципального округа Чувашской Республики.
5. Назначить администратором ИСПДн «Администрация» - управляющего делами МО - начальника отдела организационно-контрольной и кадровой работы администрации Козловского муниципального округа Чувашской Республики.
6. Назначить администратором ИСПДн «ЗАГС» - начальника отдела ЗАГС администрации Козловского муниципального округа Чувашской Республики.
7. Назначить администратором ИСПДн «Имущественные и земельные отношения» - заместителя главы администрации МО по экономике и сельскому хозяйству - начальника отдела экономики, инвестиционной деятельности, земельных и имущественных отношений администрации Козловского муниципального округа Чувашской Республики.
8. Назначить ответственным за организацию обработки персональных данных начальника отдела правового обеспечения и цифрового развития администрации Козловского муниципального округа Чувашской Республики.

В должностной инструкции ответственного лица дополнить следующие обязанности:

- осуществлять внутренний контроль за соблюдением Администрации Козловского муниципального округа Чувашской Республики и его работниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников Администрации Козловского муниципального округа Чувашской Республики положения законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- 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.

9. Утвердить следующие документы:

9.1.Положение об обработке персональных данных (Приложение № 1);
9.2. Политику информационной безопасности информационных систем персональных данных (Приложение № 2);
9.3 Положение о разграничении прав доступа к персональным данным Администрации Козловского муниципального округа Чувашской Республики (Приложение № 3);
9.4.Инструкцию по учету обращений сотрудников (Приложение № 4);
9.5.Техническое задание на создание системы защиты для ИСПДн «Администрация», «Опека и попечительство», «Имущественные и земельные отношения» (Приложение № 5);
9.6.Инструкцию администратора безопасности информационных систем персональных данных (Приложение № 6);
9.7.Инструкцию администратора ИСПДн «Администрация» (Приложение № 7);
9.8. Инструкцию администратора ИСПДн «Опека и попечительство» (Приложение № 8);
9.9.Инструкцию пользователя информационных систем персональных данных (Приложение № 9);
9.10. Положение о постоянно действующей экспертной комиссии (Приложение №10);
9.11. Порядок доступа работников Администрации Козловского муниципального округа Чувашской Республики в помещения, в которых ведется обработка персональных данных (Приложение № 11);
9.12. Правила рассмотрения запросов субъектов персональных данных или их представителей в Администрации Козловского муниципального округа Чувашской Республики (далее – Администрации) (Приложение №12);
9.13. Правила работы с обезличенными персональными данными в Администрации Козловского муниципального округа Чувашской Республики (Приложение № 13);
9.14. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», в информационных системах персональных данных Администрации Козловского муниципального округа Чувашской Республики (Приложение № 14);
9.15. Инструкцию ответственного за организацию обработки персональных данных в Администрации Козловского муниципального округа Чувашской Республики (Приложение №15);
9.16. Инструкцию по организации резервного копирования данных в информационных системах персональных данных и другой конфиденциальной информации в Администрации Козловского муниципального округа Чувашской Республики (Приложение № 16);
9.17. Акт «Результаты опроса о частоте (вероятности) реализации угрозы и опасности угрозы по видам угроз безопасности персональных данных при их обработке в ИСПДн (Приложение № 17);
9.18. Частную модель актуальных угроз и вероятного нарушителя ИСПДн «Администрация» (Приложение № 18);
9.19. Частную модель актуальных угроз и вероятного нарушителя ИСПДн «Опека и попечительство» (Приложение № 19);
9.20. Акт определения уровня защищенности персональных данных в ИСПДн «Администрация» (Приложение 20);
9.21. Акт определения уровня защищенности персональных данных ИСПДн «Опека и попечительство» (Приложение № 21);
9.22. Инструкцию администратора ИСПДн «Имущественные и земельные отношения» (Приложение № 22);

9.23. Частную модель актуальных угроз и вероятного нарушителя ИСПДн «Имущественные и земельные отношения» (Приложение № 23);
9.24. Акт определения уровня защищенности персональных данных ИСПДн «Имущественные и земельные отношения» (Приложение № 24);
9.25. Правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных (Приложение № 25);
9.26. Акт определения уровня защищенности персональных данных ИСПДн «ЗАГС» (Приложение № 26);
9.27. Техническое задание на создание системы защиты для ИСПДн «ЗАГС» (Приложение № 27);
9.28. Частную модель актуальных угроз и вероятного нарушителя ИСПДн «ЗАГС» (Приложение № 28);
9.29. Инструкцию администратора ИСПДн «ЗАГС» (Приложение № 29).
9.30. Порядок уничтожения ПДн, обработка которых осуществляется без использования средств автоматизации (Приложение № 30).
9.31. Регламент реагирования на инциденты информационной безопасности в информационных системах персональных данных (Приложение № 31).
9.32. Инструкция по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных (Приложение № 32).
10. Назначить заместителя начальника отдела организационно-контрольной работы администрации Козловского муниципального округа Чувашской Республики ответственным за ведение и сохранность Журнала учета обращений сотрудников для получения доступа к своим персональным данным, форма которого предусмотрена Положением об обработке персональных данных Администрации Козловского муниципального округа Чувашской Республики.
11. Сведения, содержащиеся в Положении об обработке персональных данных Администрации Козловского муниципального округа Чувашской Республики и Инструкции по учету обращений сотрудников для доступа к своим персональным данным, заместителю начальника отдела организационно-контрольной и кадровой работы администрации Козловского муниципального округа Чувашской Республики довести до всех работников Администрации Козловского муниципального округа Чувашской Республики.
12. Заместителю начальника отдела организационно-контрольной и кадровой работы администрации Козловского муниципального округа Чувашской Республики настоящее распоряжение объявить должностным лицам под роспись.
13. Контроль за исполнением настоящего распоряжения оставляю за собой.

Глава
Козловского муниципального округа
Чувашской Республики А.Н. Людков

Приложение № 1
Утверждено
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

АДМИНИСТРАЦИИ КОЗЛОВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА ЧУВАШСКОЙ РЕСПУБЛИКИ

г. Козловка
2024г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым Кодексом Российской Федерации от 30.12.2001 № 197-ФЗ, Гражданским Кодексом Российской Федерации, Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21.03.2012 №211 (ред. от 06.09.2014) «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», нормативно-методическими документами ФСТЭК России в сфере обработки персональных данных.

1.2. Положение определяет порядок и условия обработки персональных данных в Администрации Козловского муниципального округа Чувашской Республики (далее–Администрации) с использованием средств автоматизации и без использования таковых средств.

1.3. Цель разработки настоящего Положения является обеспечение защиты прав и свобод субъектов персональных данных при обработке их персональных данных Администрацией, а также определение порядка сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения персональных данных субъектов персональных данных, обеспечение защиты прав и свобод при обработке их персональных данных, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.4. Обработка персональных данных в Администрации осуществляется в следующих целях:

1.4.1. Для категории работников, а также родственников работников, бывших работников, муниципальных служащих, физических лиц, с которыми заключен договор гражданско-правового характера; граждан, включенных в кадровый резерв; граждан, претендующих на включение в кадровый резерв; граждан, не допущенных к участию в конкурсах; граждан, участвовавших в конкурсах, но не прошедших конкурсный отбор; граждан, претендующих на замещение вакантной должности муниципальной службы; уволенных муниципальных служащих Администрации:

- ведения кадровой работы (ведение и хранение личных дел, трудовых книжек) и выполнения всех требований трудового законодательства; заключения трудовых и иных договоров; начисления и выплаты заработной платы работникам; обработки сведений по сотрудникам об их профессиональной служебной деятельности; обработки персональных данных в информационных системах (ИСПДн); оформления доверенностей; оформления документов по воинскому учету в военкоматах в установленном порядке, составления списков призывников для военкоматов; использования персональных данных для реализации права сотрудника на участие в деятельности первичной профсоюзной организации Администрации Козловского муниципального округа Чувашской Республики, в том числе при отчислении профсоюзных взносов; подготовки документов для прохождения обучения, аттестации, переквалификации; подготовки документов для прохождения медицинского осмотра; размещения сведений по сотрудникам (ФИО, должность, рабочий телефон, фотографию) на официальном сайте Администрации Козловского муниципального округа Чувашской Республики и информационных стендах; Передача данных в: ОСФР по Чувашской Республике - Чувашии, Управление Федеральной налоговой службы по Чувашской Республике, Военный комиссариат Чувашской Республики, кредитные учреждения (банки), медицинские учреждения, органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации; МКУ «ЦБО и ФХО» Козловского Муниципального округа (429430, Чувашская Республика, Козловский р-н, г Козловка, ул. Ленина, д. 55); ПАО Акционерный коммерческий Сберегательный банк Российской Федерации (адрес: Вавилова ул., д. 19, г. Москва, 117997); АО "Россельхозбанк" (119034, город Москва, Гагаринский пер, д. 3) в рамках договора; обработка вышеуказанных персональных данных будет осуществляться путем: смешанной обработки; с передачей по внутренней сети юридического лица; с передачей по сети интернет; перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение; объем обрабатываемых персональных данных менее 100000 субъектов персональных данных; исполнитель руководствуется в своих действиях ч.2.ст. 18.1, 19 Федерального закона №152-ФЗ от 27.07.2006 «О персональных данных»).
- ведения табеля посещаемости
- оформления журналов.

1.4.2. Для категории граждан, обращающихся в Администрацию за предоставлением государственных и муниципальных услуг, посетителей сайта: регистрации и рассмотрения обращений.

1.4.3. Для категории граждан, обращающихся за получением государственных и муниципальных услуг в сфере опеки и попечительства, недееспособных совершеннолетних граждан; ограниченно дееспособных совершеннолетних граждан; опекунов/попечителей; близких родственников недееспособных/ограниченно дееспособных совершеннолетних граждан, родителей (законных представителей) несовершеннолетних:
Исполнения законодательства об опеке и попечительстве.
1.4.4. **Для категории граждан, обращающихся за получением государственных и муниципальных услуг в органах ЗАГС**: регистрация актов гражданского состояния.
1.4.5. **Для категории граждан, обращающихся за получением муниципальных услуг в сфере земельных и имущественных правоотношений**:
осуществление и выполнение возложенных законодательством Российской Федерации функций, полномочий и обязанностей и предоставление муниципальных услуг в сфере имущественных и земельных отношений;
1.5. **Срок или условие прекращения обработки персональных данных**: Реорганизация или ликвидация юридического лица
1.6. **Правовое основание обработки персональных данных:**
1.6.1. Для целей, указанных в пункте 1.4.1., 1.4.2. настоящего Положения:
Трудовой кодекс Российской Федерации (ст. ст. 86-90), Налоговый кодекс Российской Федерации, Гражданский кодекс Российской Федерации, Федеральный закон от 06.10.2003 №131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», Федеральный закон от 02.03.2007 №25-ФЗ "О муниципальной службе в Российской Федерации", Закон Чувашской Республики от 05.10.2007 №62 «О муниципальной службе в Чувашской Республике», Федеральный закон от 02.05.2006 №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Федеральный закон от 28.03.98 №53-ФЗ «О воинской обязанности и военной службе», Федеральный закон от 26.02.97 №31-ФЗ «О мобилизационной подготовке и мобилизации в Российской Федерации», Устав Администрации Козловского муниципального округа Чувашской Республики от 08.11.2022, согласие на обработку персональных данных, Положение об обработке персональных данных от 18.12.2024.
1.6.2. Для целей, указанных в пункте 1.4.3. Федеральный закон от 06.10.2003 №131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», Федеральный закон от 02.03.2007 №25-ФЗ «О муниципальной службе в Российской Федерации», Закон Чувашской Республики от 05.10.2007 №62 «О муниципальной службе в Чувашской Республике», Федеральный закон от 24.04.2008 №48-ФЗ «Об опеке и попечительстве», Федеральный закон от 02.05.2006 №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Федеральный закон от 27.07.2010 №210-ФЗ «Об организации предоставления государственных и муниципальных услуг», Федеральный закон от 15.11.97 № 143-ФЗ «Об актах гражданского состояния», Семейный кодекс Российской Федерации, Гражданский кодекс Российской Федерации, Закон Чувашской Республики от 06.02.2009 № 5 «Об опеке и попечительстве», Устав Администрации Козловского муниципального округа Чувашской Республики от 08.11.2022, согласие на обработку персональных данных, Положение об обработке персональных данных от 18.12.2024.
1.6.3.Для целей, указанных в пункте 1.4.4.Федеральный закон от 06.10.2003 №131-ФЗ "Об общих принципах организации местного самоуправления в Российской Федерации", Федеральный закон от 02.03.2007 №25-ФЗ "О муниципальной службе в Российской Федерации", Закон Чувашской Республики от 05.10.2007 №62 «О муниципальной службе в Чувашской Республике», Федеральный закон от 24.04.2008 №48-ФЗ «Об опеке и попечительстве», Федеральный закон от 02.05.2006 № 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации", Федеральный закон от 27.07.2010 №210-ФЗ «Об организации предоставления государственных и муниципальных услуг», Закон Чувашской Республики от 06.02.2009 №5 «Об опеке и попечительстве», Гражданский кодекс Российской Федерации, Семейный кодекс Российской Федерации, Постановление Правительства РФ от 29 декабря 2018 г. № 1746 "Об утверждении Правил предоставления сведений о государственной регистрации актов гражданского состояния, содержащихся в Едином государственном реестре записей актов гражданского состояния, и признании утратившими силу некоторых актов Правительства Российской Федерации", Приказ Министерства юстиции РФ от 1 октября 2018 г. № 202 “Об утверждении форм записей актов гражданского состояния и Правил заполнения форм записей актов гражданского состояния”, Приказ Минюста России от 01.10.2018 № 201 "Об утверждении форм заявлений о государственной регистрации актов гражданского состояния и Правил заполнения форм заявлений о государственной регистрации актов гражданского состояния",Устав Администрации Козловского муниципального округа Чувашской Республики от 08.11.2022 г, согласие на обработку персональных данных, Положение об обработке персональных данных от 18.12.2024 г.
1.6.4. Для целей, указанных в пункте 1.4.5.Федеральный закон от 06.10.2003 № 131-ФЗ "Об общих принципах организации местного самоуправления в Российской Федерации", Федеральный закон от 02.03.2007 № 25-ФЗ "О муниципальной службе в Российской Федерации", Закон Чувашской Республики от 05.10.2007 №62 "О муниципальной службе в Чувашской Республике",Федеральный закон от 02.05.2006 №59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации", Федеральный закон от 27.07. 2010 г. №210-ФЗ «Об организации предоставления государственных и муниципальных услуг», Земельный кодекс РФ, Жилищный кодекс РФ, Градостроительный кодекс РФ, Семейный кодекс Российской Федерации, Гражданский кодекс Российской Федерации, Закон Чувашской Республики от 06.02.2009 № 5 "Об опеке и попечительстве", Постановление Кабинета Министров Чувашской Республики от 12.01.2006 №2 «О Порядке ведения органами местного самоуправления в Чувашской Республике учета граждан в качестве нуждающихся в жилых помещениях и имеющих право на государственную поддержку на строительство (приобретение) жилых помещений», Постановление Кабинета Министров Чувашской Республики №53 от 26.02.2014 «Порядок формирования и утверждения списков участников мероприятий по улучшению жилищных условий граждан, проживающих в сельской местности, в том числе молодых семей и молодых специалистов, и выдачи свидетельств о предоставлении социальных выплат на строительство (приобретение) жилья в сельской местности», Устав Администрации Козловского муниципального округа Чувашской Республики от 08.11.2022, согласие на обработку персональных данных, Положение об обработке персональных данных от 18.12.2024.
1.7. В настоящем Положении используются следующие понятия, термины и сокращения:
Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных.
Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
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.
Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.
Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
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.
Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.
Конфиденциальность персональных данных - обязанность оператора и иных лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.
Субъект (персональных данных) - физическое лицо, определяемое на основании персональных данных, обрабатываемых в Администрации.
1.8.Настоящее Положение и изменения к нему утверждаются распоряжением Администрации.
1.9.Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно, до замены его новым Положением.
1.10.Настоящее Положение является обязательным для исполнения всеми работниками Администрации, непосредственно осуществляющими обработку персональных данных и (или) имеющими доступ к персональным данным. Все работники Администрации должны быть ознакомлены с настоящим Положением и изменениями к нему под роспись.
1.11. Настоящее Положение подлежит пересмотру в ходе периодического анализа со стороны руководства Администрации, а также в случаях изменения законодательства Российской Федерации в области персональных данных.
1.12. Настоящее положение подлежит опубликованию на официальном сайте Администрации в течение 10 дней после его утверждения.

2.СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1.В Администрации обрабатываются персональные данные следующих групп субъектов:
- работников, а также родственников работников, бывших работников, муниципальных служащих, физических лиц, с которыми заключен договор гражданско-правового характера; граждан, включенных в кадровый резерв; граждан, претендующих на включение в кадровый резерв; граждан, не допущенных к участию в конкурсах; граждан, участвовавших в конкурсах, но не прошедших конкурсный отбор; граждан, претендующих на замещение вакантной должности муниципальной службы; уволенных муниципальных служащих Администрации;
- граждан, обращающихся в Администрацию за предоставлением государственных и муниципальных услуг, посетителей сайта;
- недееспособных совершеннолетних граждан; ограниченно дееспособных совершеннолетних граждан; опекунов/попечителей; близких родственников недееспособных/ограниченно дееспособных совершеннолетних граждан, родителей (законных представителей) несовершеннолетних;
2.2.В Администрации к персональным данным работников (бывших работников), муниципальных служащих относятся следующие сведения:
- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- адрес проживания, регистрации;
- семейное, социальное, имущественное положение;
- сведения об образовании (наименования оконченных учебных заведений, факультет, специальность, год окончания), информация о дополнительном образовании, повышении квалификации, аттестации;
- профессия;
- доходы, полученные в Администрации;
- специальность;
- гражданство;
- паспортные данные;
- СНИЛС;
-ИНН;
- пол;
- трудовой и общий стаж;
- сведения о детях (количество, возраст);
- социальные льготы;
- сведения о воинском учете;
- контактные телефоны;
- фотография;
- сумма дохода;
- сумма вычета;
- номер лицевого счета;
- стаж работы;

реквизиты страхового свидетельства обязательного пенсионного страхования;
- прежнее место работы (структурное подразделение), наименование структурного подразделения, наименование должности;
- уровень владения иностранными языками;
- профессиональные навыки;
- информация об аттестации (дата аттестации, решение комиссии, номер, дата протокола);
- информация о повышении квалификации (дата начала и окончания обучения, вид повышения квалификации, наименование образовательного учреждения, серия, №, дата выдачи документа об образовании);
- сведения о профессиональной переподготовке (дата начала и окончания обучения, специальность (направление, профессия), серия, номер, дата выдачи документа);
- информация о наградах (поощрениях), почетных званиях (наименование награды, номер и дата выдачи документа), размер вознаграждения;
- данные об отпусках (вид отпуска, период, дата начала и окончания отпуска);
- отметки о явках и неявках на работу по числам месяца, количество неявок, причины неявок;
- количество отработанных часов за месяц, количество выходных и праздничных дней;
- сведения о социальных льготах, на которые работник имеет право в соответствии с законодательством (наименование льготы, номер и дата выдачи документа);
- номер, дата трудового договора;
- испытательный срок;
- серия и номер трудовой книжки или вкладыша в неё;
- основание прекращения (расторжения) трудового договора (увольнения), причина увольнения, дата увольнения, номер и дата приказа;
- сведения о судимости в соответствии с законодательством РФ.
- данные свидетельств о браке и (или) о расторжении брака, о смене фамилии.
- сведения о доходах, расходах, об имуществе и обязательствах имущественного характера, а также о доходах, расходах, об имуществе и обязательствах имущественного характера супруги (супруга) и несовершеннолетних детей;
- сведения, содержащиеся в служебном контракте (трудовом договоре), дополнительных соглашениях к служебному контракту (трудовому договору);
- сведения об участии в выборных органах (с указанием времени пребывания, наименование органа);
- сведения о классном чине гражданской службы Российской Федерации (дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине гражданской службы субъекта Российской Федерации), квалификационном разряде гражданской службы (квалификационном разряде или классном чине муниципальной службы), кем и когда присвоены;
адрес электронной почты;
реквизиты банковской карты.
2.3. К документам (в бумажном и (или) электронном виде), содержащим персональные данные работников Администрации, относятся:
- паспорт или иной документ, удостоверяющий личность;
- свидетельство о постановке на учет в налоговом органе и присвоении ИНН;
- страховое пенсионное свидетельство;
- документ воинского учета;
- документы об образовании, о квалификации или наличии специальных знаний или специальной подготовки;
- документы, содержащие сведения о заработной плате, доплатах и надбавках;
- заявление о приеме на работу;
- трудовой контракт (договор);
- приказ (распоряжение) о приеме
- личная карточка сотрудника;
- личное дело сотрудника;
- трудовая книжка;
- приказ (распоряжение) о переводе сотрудника на другую работу;
- приказ (распоряжение) о предоставлении отпуска работнику;
- график отпусков;
- заявление о приеме;
- заявление об увольнении;
- приказ (распоряжение) о прекращении (расторжении) трудового договора с работником (увольнении);
- приказ (распоряжение) о направлении работника в командировку;
- командировочное удостоверение;
- служебное задание для направления в командировки и отчет о его выполнении;
- приказ (распоряжение) о поощрении (наказании) работника;
- справка с места работы;
- справка о доходах физического лица Ф № 2-НДФЛ;
- список работников, подлежащих обязательному медицинскому страхованию;
сведения о доходах, расходах, об имуществе и обязательствах имущественного характера, а также о доходах, расходах, об имуществе и обязательствах имущественного характера супруги (супруга) и несовершеннолетних детей
- резюме;
2.4. К персональным данным граждан, обращающихся в Администрацию за предоставлением государственных и муниципальных услуг, в отношении которых составлены записи актов гражданского состояния, относятся следующие сведения:
фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; адрес; семейное положение; социальное положение; имущественное положение; образование; профессия; доходы; национальная принадлежность; место работы и должность (или источник дохода) указывается для актовых записей, составленных до 1999 года; - причина смерти (медицинский диагноз) при государственной регистрации рождения: - фамилия, имя, отчество, пол, дата и место рождения ребенка, мертворожденный, живорожденный, количество родившихся детей (один, двойня или более детей), сведения о документе, подтверждающем факт рождения ребенка; - сведения о документе, являющемся основанием для внесения сведений

об отце; - фамилия, имя, отчество и место жительства заявителя либо наименование и юридический адрес органа или организации, заявивших о рождении ребенка; - серия и номер выданного свидетельства о рождении сведения о документе, подтверждающем прекращение предыдущего брака, в случае, если лицо (лица), заключившее брак, состояло в браке ранее; реквизиты документов, удостоверяющих личности заключивших брак; дата составления и номер записи акта о заключении брака; серия и номер выданного свидетельства о браке, сведения о документе, являющемся основанием для государственной регистрации расторжения брака; дата прекращения брака; реквизиты документов, удостоверяющих личности расторгнувших брак; серия и номер свидетельства о расторжении брака, фамилия, имя, отчество, дата и место рождения ребенка (до и после усыновления); место жительства усыновителя (усыновителей); реквизиты решения суда об установлении усыновления ребенка; серия и номер выданного свидетельства об усыновлении, фамилия, имя, отчество (до установления отцовства), пол, дата и место рождения ребенка; дата составления, номер записи акта о рождении и наименование органа записи актов гражданского состояния, которым произведена государственная регистрация рождения ребенка; фамилия, имя, отчество ребенка после установления отцовства; серия и номер выданного свидетельства об установлении отцовства, при государственной регистрации смерти: фамилия, имя, отчество, дата и место рождения, последнее место жительства, пол, гражданство, национальность (если сведения о национальности указаны в документе, удостоверяющем личность умершего), дата и место смерти умершего; причина смерти (на основании документа, подтверждающего факт смерти); реквизиты документа, подтверждающего факт смерти; фамилия, имя, отчество, место жительства заявителя либо наименование и юридический адрес органа, организации или учреждения, сделавших заявление о смерти; серия и номер выданного свидетельства о смерти; фамилия, имя, отчество, место жительства лица, которому выдано свидетельство о смерти.
2.5. К персональным данным посетителей сайта относятся:
Фамилия, имя, отчество, адрес электронной почты, номер телефона.
2.6. К персональным данным граждан, обращающихся за получением государственных и муниципальных услуг в сфере опеки и попечительства, недееспособных совершеннолетних граждан; ограниченно дееспособных совершеннолетних граждан; опекунов/попечителей; близких родственников недееспособных/ограниченно дееспособных совершеннолетних граждан, родителей (законных представителей) несовершеннолетних относятся: ФИО; дата рождения; свидетельство о рождении; паспортные данные; реквизиты документа, удостоверяющего личность; место рождения; адрес регистрации; адрес места жительства; место учебы; место работы; сведения о составе семьи; сведения о жилом помещении или ином недвижимом имуществе.
2.7. К персональным данным граждан, обращающихся за получением муниципальных услуг в сфере земельных и имущественных правоотношений относятся:
ФИО; паспортные данные; ИНН; дата рождения; место жительства; адрес регистрации; фактический (почтовый) адрес; сведения об имуществе (размер арендной платы, площадь земельного участка, срок аренды, кадастровый номер участка, категория земли, местоположение участка, цель использования); код арендатора; наименование арендатора; сведения о земельном участке (площадь, кадастровая стоимость, годовая арендная плата).

3. ОСНОВНЫЕ ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обработка персональных данных осуществляется на основе следующих принципов:
3.1. Обработка персональных данных осуществляется на законной и справедливой основе.
3.2. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
3.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
3.4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.
3.5. Содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточными по отношению к заявленным целям их обработки.
3.6. При обработке персональных данных обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор принимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных.
3.7. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого является субъект персональных данных. Обрабатываемые персональные данные в Администрации подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. В целях обеспечения прав и свобод человека и гражданина работники Администрации при обработке персональных данных субъектов персональных данных, обязаны соблюдать следующие общие требования:
4.1.1. Обработка персональных данных осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, их обучении и продвижении по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности персональных данных.
4.1.2. При определении объема и содержания, обрабатываемых персональных данных работники Администрации должны руководствоваться Конституцией Российской Федерации, Трудовым Кодексом Российской Федерации и иными федеральными законами.
4.1.3. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».
4.1.4. Обработка персональных данных в Администрации осуществляется только специально уполномоченными лицами, перечень которых утверждается внутренним приказом, при этом указанные в приказе работники должны иметь право получать только те персональные данные субъекта, которые необходимы для выполнения непосредственных должностных обязанностей.
4.1.5. Использование персональных данных возможно только в соответствии с целями, определившими их получение. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации.

4.1.6. При принятии решений, затрагивающих интересы субъекта, работники оператора не имеют права основываться на персональных данных субъекта, полученных исключительно в результате их автоматизированной обработки.
4.2. Получение персональных данных.
4.2.1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.
4.2.2. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:
- фамилию, имя, отчество, адрес субъекта, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также способ его отзыва;
- подпись субъекта персональных данных.
4.2.3. Для осуществления обработки персональных данных субъектов персональных данных оператору необходимо получать согласие на обработку их персональных данных, и на передачу персональных данных третьим лицам по форме, представленной в Приложении № 1 к настоящему Положению.
4.2.4. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. Форма отзыва согласия на обработку персональных данных представлена в Приложении № 2 к настоящему Положению. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».
4.2.5. При возникновении необходимости получения персональных данных субъекта от третьих лиц, от субъекта должно быть получено письменное согласие. Форма согласия субъекта на получение его персональных данных от третьих лиц представлена в Приложении №3 к настоящему Положению.
4.2.6. В случае получения персональных данных от третьего лица субъект, персональные данные которого были получены, должен быть уведомлен об этом. Форма уведомления представлена в Приложении № 4 к настоящему Положению.
4.2.7. В уведомлении необходимо сообщить о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа субъекта дать письменное согласие на их получение.
4.2.8. Сведения, которые характеризуют физиологические и биологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные), и которые используются Администрацией для установления личности субъекта персональных данных, могут обрабатываться в Администрации только при наличии согласия субъекта в письменной форме.
Оператор не вправе отказывать в обслуживании в случае отказа субъекта персональных данных предоставить биометрические персональные данные и (или) дать согласие на обработку персональных данных, если в соответствии с федеральным законом получение оператором согласия на обработку персональных данных не является обязательным.
4.2.9. В случае смерти субъекта согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом при его жизни.
4.2.10. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.
4.3. Доступ к персональным данным.
4.3.1. Перечень работников (фамилии, имена, отчества и должности), осуществляющих обработку персональных данных, как в бумажном, так и в электронном виде и (или) имеющих доступ к персональным данным, утверждается внутренним приказом. При этом указанные лица должны иметь право получать только те персональные данные субъектов, которые необходимы для выполнения непосредственных должностных обязанностей. Доступ к персональным данным работников Администрации, не входящих в вышеуказанный перечень, запрещается.
4.3.2. Процедура оформления доступа к персональным данным включает в себя:
- ознакомление работников с настоящим Положением, инструкцией пользователя ИСПДн, Политикой информационной безопасности и другими нормативными актами, регулирующими обработку и защиту персональных данных в Администрации, под роспись;
- подписание работником Соглашения о неразглашении персональных данных работника. Форма о соблюдении конфиденциальности персональных данных представлена в Приложении № 6 к настоящему Положению.
4.3.3. Выдача документов, содержащих персональные данные работников осуществляется в соответствии со ст. 62 Трудового кодекса РФ с соблюдением следующей процедуры:
- заявление работника о выдаче того или иного документа на имя специалиста по кадрам;

- выдача заверенной копии (в количестве экземпляров, необходимом работнику) заявленного документа, либо справки о заявленном документе или сведениях, содержащихся в нем;
- внесения соответствующих записей в Журнал учета выданной информации.
4.3.4. Всем работникам оператора снимать какие-либо копии, делать выписки, изымать документы (либо их копии) из личного дела категорически запрещено.
4.4. Обеспечение конфиденциальности персональных данных.
4.4.1. Персональные данные относятся к категории конфиденциальной информации.
4.4.2. Работниками оператора, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных. Работники Оператора получившие доступ к персональным данным, не раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.
4.4.3. Администрация вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным органом или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению Администрации, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом.
В поручении должны быть определены перечень персональных данных, перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели их обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных, требования, предусмотренные частью 5 статьи 18 и статьей 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», обязанность по запросу оператора персональных данных в течение срока действия поручения, в том числе до обработки персональных данных, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения требований, установленных в соответствии с настоящей статьей, обязанность обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона, в том числе требование об уведомлении оператора о случаях, предусмотренных частью 3.1 статьи 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».
4.4.4. В целях информационного обеспечения деятельности структурных подразделений и работников оператора могут быть созданы общедоступные источники персональных данных (стенды, папки в кабинетах, информация на сайте, справочники, адресные книги и др.). В общедоступные источники персональных данных с письменного согласия работника могут включаться его фамилия, имя, отчество, год и место рождения, абонентский номер, сведения о профессии и иные персональные данные. Сведения о работнике могут быть в любое время исключены из общедоступных источников персональных данных по требованию работника, суда или иных уполномоченных государственных органов.
4.5. **Права и обязанности сторон при обработке персональных данных.**
4.5.1. Работники оператора обязаны предоставлять в отдел кадров и только достоверные, документированные персональные данные и своевременно сообщать об изменении своих персональных данных.
4.5.2. Каждый субъект персональных данных имеет право:
- на получение полной информации о своих персональных данных и на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных действующим законодательством;
Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:
- подтверждение факта обработки персональных данных оператором;
- правовое основание и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Администрацией или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных действующим Федеральным законом;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Администрации, если обработка поручена или будет поручена такому лицу;
- информацию о способах исполнения оператором обязанностей, установленных статьей 18.1 152-ФЗ «О персональных данных»;
- иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и другими федеральными законами.
4.5.3. Субъект персональных данных вправе требовать от работников оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
4.5.4. Субъект персональных данных вправе заявить о своем несогласии при отказе работников Администрации исключить или исправить персональные данные (в письменной форме с соответствующим обоснованием такого несогласия).
4.5.5. Запрашиваемая субъектом информация должна быть предоставлена субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.
Запрашиваемая информация предоставляется субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя.
Запрос должен содержать:
1) номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя;

2) сведения о дате выдачи указанного документа и выдавшем его органе;
3) сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором
4) подпись субъекта персональных данных или его законного представителя.
Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.
Сведения, указанные 4.5.5 настоящего положения, предоставляются субъекту персональных данных или его представителю оператором в течение десяти рабочих дней с момента обращения либо получения оператором запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.
Оператор предоставляет сведения, указанные в п. 4.5.5 настоящего положения, субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.
4.5.6. В случае, если запрашиваемая информация, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения данных сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней (далее – нормированный срок запроса) после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого является субъект персональных данных.
4.5.7. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения данных сведений, а также в целях ознакомления с обрабатываемыми персональными данными до истечения тридцати дней, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос субъекта персональных данных наряду с необходимой для запроса информации должен содержать обоснование направления повторного запроса
4.5.8. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, условиям повторного запроса. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Администрации.
4.5.9. Оператор обязан безвозмездно предоставить субъекту возможность ознакомления с персональными данными, относящимися к соответствующему субъекту, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом сведений, подтверждающих, что персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах Администрация обязана уведомить субъекта и третьих лиц, которым персональные данные этого субъекта были переданы. Форма уведомления представлена в Приложении № 4 к настоящему Положению.
4.5.10. Все обращения работников персональных данных по вопросам, касающимся обработки персональных данных, фиксируются ответственным лицом за организацию обработки персональных данных в Журнале учета обращений субъектов персональных данных (работников) по вопросам обработки персональных данных и для получения доступа к своим персональным данным.
4.5.11. Форма журнала представлена в Приложении № 8 к настоящему Положению.
4.5.12. Для регламентации порядка учета обращений граждан для получения доступа к своим персональным данным разработана Инструкция по учету обращений работников для доступа к своим персональным данным, с которой ознакамливаются все работники оператора под роспись
4.5.13. **Права субъектов персональных данных при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации.**
4.5.13.1 Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации оператором не осуществляется.
4.5.14. Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных
4.5.14.1. Принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы оператором не осуществляется.
4.5.15. Право на обжалование действий или бездействий Оператора.
4.5.15.1. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.
4.5.15.2. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.
4.6. Обязанности оператора
4.6.1. Обязанности оператора при сборе персональных данных.
4.6.1.1. При сборе персональных данных оператор предоставляет субъекту персональных данных по его просьбе запрашиваемую субъектом информацию.
4.6.1.2. Если в соответствии с федеральным законом предоставление персональных данных и (или) получение оператором согласия на обработку персональных данных являются обязательными, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку.
4.6.1.3. Если персональные данные получены не от субъекта персональных данных, оператор до начала обработки таких персональных предоставляет субъекту персональных данных следующую информацию (далее – информация, сообщаемая при получении персональных данных не от субъекта персональных данных):

1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
2) цель обработки персональных данных и ее правовое основание;
перечень персональных данных;
3) предполагаемые пользователи персональных данных;
4) установленные настоящим Федеральным законом права субъекта персональных данных;
5) источник получения персональных данных.
4.6.1.4. Оператор не предоставляет субъекту информацию, сообщаемую при получении персональных данных не от субъекта персональных данных, в случаях, если:
1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных оператором;
2) персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
3) обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 152-ФЗ «О персональных данных»;
4) Оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;
5) предоставление субъекту персональных данных информации, сообщаемой при получении персональных данных не от субъекта персональных данных, нарушает права и законные интересы третьих лиц.
4.6.1.5. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации в следующих информационных системах:
4.6.1.5.1. Информационные системы персональных данных «Администрация» (подсистемы «Сайт», «Обращения граждан», «Опека и попечительство») с использованием баз данных, находящихся на территории России.
4.6.1.5.2. Информационные системы персональных данных «Имущественные и земельные отношения», «ЗАГС» с использованием баз данных, находящихся на территории России.
4.6.1.5.3. Местонахождение центра(ов) обработки данных и сведения об организации, ответственной за хранение данных, определены внутренними документами Администрации.
4.6.2. Меры, направленные на обеспечение выполнения Оператором своих обязанностей.
4.6.2.1. Оператор принимает меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом или другими федеральными законами. К таким мерам, в частности, относятся:
1) назначение ответственного за организацию обработки персональных данных;
2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, определяющих для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений. Такие документы и локальные акты не могут содержать положения, ограничивающие права субъектов персональных данных, а также возлагающие на операторов не предусмотренные законодательством Российской Федерации полномочия и обязанности;
3) применение правовых, организационных и технических мер по обеспечению безопасности персональных;
4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных требованиям к защите персональных данных, Положению, локальным актам оператора;
5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;
6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, Положением, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.
7) Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети, в том числе на страницах принадлежащего оператору сайта в информационно-телекоммуникационной сети «Интернет», с использованием которых осуществляется сбор персональных данных, документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.
4.6.3. Меры по обеспечению безопасности персональных данных при их обработке
4.6.3.1. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.
4.6.3.2. Обеспечение безопасности персональных данных достигается, в частности:
1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
5) учетом машинных носителей персональных данных;
6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;
7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.
4.6.3.3. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.
4.6.3.4. Оператор обязан в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.
4.6.4. **Обязанности оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных.**
4.6.4.1. Оператор обязан сообщить в порядке, предусмотренном статьей 14 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.
4.6.4.2. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий десяти рабочих дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.
4.6.4.3. Оператор предоставляет безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Администрация вносит в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор уничтожает такие персональные данные. Оператор уведомляет субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.
4.6.4.4. Оператор сообщает в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение десяти рабочих дней с даты получения такого запроса. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес уполномоченного органа по защите прав субъектов персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.
4.6.5. **Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных.**
4.6.5.1. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя, либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных, оператор осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения, или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.
4.6.5.2.В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов уточняет персональные данные либо обеспечить их уточнение (если

обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.
4.6.5.3. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных или обеспечивает прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные или обеспечивает их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор уведомляет субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.
4.6.5.4. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, оператор обязан с момента выявления такого инцидента оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:
1) в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;
2) в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).
4.6.5.5. В случае достижения цели обработки персональных данных оператор прекращает обработку персональных данных или обеспечивает ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.
4.6.5.6. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор прекращает их обработку или обеспечивает прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.
4.6.5.7. В случае обращения субъекта персональных данных к оператору с требованием о прекращении обработки персональных данных оператор обязан в срок, не превышающий десяти рабочих дней с даты получения оператором соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных пунктами 2 - 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных». Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.
4.6.5.8. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пункте 4.6.5.4. настоящего Положения, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.
4.6. Передача персональных данных.
4.6.1. При передаче персональных данных субъекта работники оператора обязаны соблюдать следующие требования:
- не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта (Приложение № 1 к настоящему Положению) или его законного представителя, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, предусмотренных Трудовым Кодексом Российской Федерации или иными федеральными законами.
- предупреждать лица, получающие персональные данные субъектов, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц обеспечения конфиденциальности полученных персональных данных;
- не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия;
- передавать персональные данные субъекта представителям субъектов в порядке, установленном Трудовым Кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функций;
- не отвечать на вопросы, связанные с передачей персональных данных субъекта по телефону или факсу, за исключением случаев, связанных с выполнением соответствующими работниками своих непосредственных должностных обязанностей, адресатам в чью компетенцию входит получение такой информации.
4.6.2. В целях обеспечения контроля правомерности использования переданных по запросам персональных данных лицами, их получившими, сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в их

предоставлении, а также состав переданной информации фиксируются в Журнале учета передачи персональных данных. Форма журнала учета передачи персональных данных представлена в Приложении №9 к настоящему Положению.

4.7. Хранение персональных данных.

4.7.1. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижению целей обработки или в случае утраты необходимости в достижении этих целей.

В Администрации хранение персональных данных субъектов может осуществляться на бумажных и электронных носителях, доступ к которым ограничен списком лиц, допущенных к обработке персональных данных.

4.7.2. Все электронные носители персональных данных подлежат строгому учету. Форма Журнала учета электронных носителей приведена в Приложении 10 к настоящему Положению.

4.7.3. Хранение персональных данных субъектов должно происходить в порядке, исключающем их утрату или их неправомерное использование.

4.7.4. Персональные данные субъектов, содержащиеся на бумажных носителях и отчуждаемых электронных носителях информации, должны храниться в сейфах или запираемых шкафах, установленных в пределах контролируемой зоны оператора.

4.7.5. Персональные данные субъектов, содержащиеся на электронных носителях информации, должны храниться на автоматизированных рабочих местах и серверах информационных систем персональных данных Администрации, установленных в пределах контролируемой зоны оператора.

Все меры, направленные на соблюдение конфиденциальности при сборе, обработке и хранении персональных данных субъекта, распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

1.1. 4.7.6. Все хранимые или используемые СЗИ (средства защиты информации), эксплуатационная и техническая документация к ним подлежат поэкземплярному учету и выдаются под расписку в Журнале поэкземплярного учета СЗИ, эксплуатационной и технической документации к ним пользователям СЗИ, несущим персональную ответственность за их сохранность. Форма соответствующего Журнала приведена в Приложении №11 к настоящему Положению.

1.2. 4.7.7. Все хранимые или используемые криптосредства (средства криптографической защиты информации), эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету и выдаются под расписку в Журнале поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов ответственным пользователем криптосредств пользователям криптосредств, несущим персональную ответственность за их сохранность. Форма соответствующего Журнала приведена в Приложении №12 к настоящему Положению. Ответственный пользователь криптосредств заводит и ведет на каждого пользователя криптосредств Лицевой счет, в котором регистрирует числящиеся за ними криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы. Форма Лицевого счета пользователя криптосредств приведена в Приложении №13.

1.3. 4.7.8. Хранение персональных данных субъектов должно происходить в порядке, исключающем их утрату или их неправомерное использование.

1.4. 4.7.9. Персональные данные субъектов, содержащиеся на бумажных носителях и отчуждаемых машинных носителях информации, должны храниться в сейфах или запираемых шкафах, установленных в пределах контролируемой зоны оператора. Все хранилища должны быть учтены, и соответствующая запись внесена в Журнал учета хранилищ (Приложение №14).

4.8. Уничтожение персональных данных.

4.8.1. Обрабатываемые персональные данные должен уничтожить оператор (или обеспечить уничтожение, если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в следующих случаях:

- в случае достижения цели обработки персональных данных - в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных;
- в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных - в срок, не превышающий тридцати дней с даты поступления указанного отзыва;
- в случае выявления неправомерной обработки с персональными данными и невозможности устранения допущенных нарушений - в срок, не превышающий трех рабочих дней с даты этого выявления.

4.8.2. После уничтожения персональных данных необходимо уведомить об этом субъекта персональных данных или его законного представителя. А в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган. Форма уведомления представлена в Приложении №6 к настоящему Положению.

4.8.3. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренным законодательством РФ и региональным законодательством об архивном деле.

4.8.4. В случае отсутствия возможности уничтожения персональных данных в течении указанных выше сроков, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

4.8.5. Уничтожение персональных данных производится на основании Акта уничтожения персональных данных. Форма Акта уничтожения предусмотрена в Приложении № 7 к настоящему Положению.

4.9. Уточнение (обновление, изменение) персональных данных.

Исходя из того, что персональные данные содержатся во многих документах оператора, при уточнении (обновлении, изменении) персональных данных, изменения вносятся следующим образом:

- в личную карточку работника. В соответствии с п. 1 Указаний, утвержденных Постановления Госкомстата Российской Федерации от 05.01.2004 №1, при изменении сведений о работнике в его личную карточку вносятся новые данные, которые заверяются подписью специалиста по кадрам.
- в трудовую книжку. В соответствии с п. 7. (приказ Министерство труда и социальной защиты Российской Федерации от 19 мая 2021 г. №320н об утверждении формы, порядка ведения и хранения трудовых книжек) Изменения записей в трудовых книжках о фамилии, имени, отчестве и дате рождения производятся на основании паспорта, свидетельств о рождении, о регистрации брака, о расторжении брака, о перемене имени и других документов и со ссылкой на их номер, дату и орган, выдавший документ.

Указанные изменения вносятся на первую страницу (титульный лист) трудовой книжки. Одной чертой зачеркивается прежняя фамилия или имя, отчество (при наличии), дата рождения и записываются новые данные. Ссылки на соответствующие документы делаются на внутренней стороне обложки трудовой книжки и заверяются подписью работодателя или специально уполномоченного им лица и печатью организации (или печатью кадровой службы) (при наличии печати).
Изменение (дополнение) на первой странице (титульном листе) трудовой книжки записей о полученных новых образовании, профессии, специальности осуществляется путем дополнения имеющихся записей (если они уже имеются) или заполнения соответствующих строк без зачеркивания ранее внесенных записей.
В случае изменения сведений, содержащих персональные данные (фамилия, имя, отчество, адрес, абонентский номер, паспортные данные, сведения об образовании, семейном положении (при выявлении противопоказаний для выполнения служебных обязанностей (работы), обусловленных трудовым договором (контрактом) работники обязаны своевременно сообщать о таких изменениях (как правило, в 3-х дневный срок) в отдел кадров оператора.
В целях уточнения (обновления, изменения) персональных данных и для внесения изменений в документы оператора, содержащие персональные данные работника, необходимо в произвольной форме составлять приказ об изменении персональных данных конкретного работника. На основании этого приказа будут вноситься изменения во все остальные соответствующие документы. Внесенные изменения необходимо заверить подписью ответственного работника и печатью Администрации.

5. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ.

5.1. Оператор при обработке персональных данных обязано принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.
5.2. Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных, используемых в процессе деятельности Администрации.
5.3. Основными организационными мерами по защите персональных данных оператора являются:
- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое, избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- обеспечение знания работником требований нормативно-методических документов по защите информации и сохранении тайны;
- обеспечение наличия необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- грамотная организация процесса уничтожения информации;
- организация регулярной воспитательной и разъяснительной работы с работниками оператора по предупреждению утраты и утечки сведений при работе с конфиденциальными документами, содержащими персональные данные;
- разработка комплекта внутренних документов оператора, регламентирующих процессы обработки персональных данных.
5.4. В качестве дополнительных организационных мер защиты персональных данных оператором создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ к персональным данным с целью овладения ценными сведениями и их использования, а также их искажения, уничтожения, подмены, фальсификации содержания реквизитов документа и т.д.
Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности оператора: клиенты, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов, содержащих персональные данные.
Для защиты персональных данных от несанкционированного доступа оператором необходимо обеспечить:
- охрану в дневное время в помещении оператора (в контролируемую зону),
- постоянную работоспособность пожарной и охранной сигнализации.
5.5. В качестве технических мер защиты персональных данных оператором должны применяться:
- антивирусная защита;
- межсетевые экраны;
- разграничение прав доступа (пароли);
- специализированные средства защиты информации от несанкционированного доступа.
5.6. После установки (обновления) программного обеспечения, администратор безопасности должен произвести требуемые настройки средств управления доступом к компонентам ПЭВМ и проверить работоспособность программного обеспечения и правильность его настройки и произвести соответствующую запись в Журнале учета нештатных ситуаций ПЭВМ, выполнения профилактических работ, установки и модификации программных средств ПЭВМ. Формат записей Журнала учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств ПЭВМ приведен в Приложении № 15.
5.7. Администратор безопасности должен проводить периодическое тестирование технических и программных средств защиты и вносить результаты в Журнал периодического тестирования средств защиты информации, форма которого представлена в Приложении № 16, а также производить проверку электронных журналов и вносить запись в соответствующий Журнал (Приложение № 17).
5.8. В целях организации контроля за обеспечением безопасности персональных данных в Администрации распоряжением создается постоянно действующая Комиссия по обеспечению безопасности персональных данных (далее Комиссия).
5.8.1. Комиссия является совещательным органом при руководителе Администрации.
5.8.2. Решения Комиссии вступают в силу после их утверждения руководителем оператора.
5.9. Основные задачи Комиссии.
Основными задачами Комиссии являются:
5.9.1. Организация и проведение экспертизы ценности документов на стадии делопроизводства при составлении номенклатуры дел и формировании дел.
5.9.2. Организация и проведение экспертизы ценности документов на стадии подготовки их к архивному хранению.

5.9.3. Организация и проведение отбора и подготовки документов к передаче на государственное хранение, в том числе научно-технической, аудиовизуальной и другой специальной документации.
5.9.4. Организация и приведение документооборота оператора в соответствии с актуальными требованиями законодательства о персональных данных.
5.9.5. Проведение классификации ИСПДн.

6. ВЗАИМОДЕЙСТВИЕ С КОНТРОЛЬНО-НАДЗОРНЫМИ ОРГАНАМИ

6.1. При поступлении запроса от уполномоченного органа по защите прав субъектов персональных данных (Роскомнадзор) оператор обязан сообщить информацию, необходимую для осуществления деятельности указанного органа, в течение десяти рабочих дней с даты получения такого запроса. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес уполномоченного органа по защите прав субъектов персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.
6.2. В случае выявления недостоверных персональных данных или неправомерных действий с ними по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.
В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.
В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить по запросу Роскомнадзор.
6.3. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, оператор обязан с момента выявления такого инцидента оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:
1) в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;
2) в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).
6.4.При проведении контрольно-надзорных мероприятий за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных, осуществляемых федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности (ФСБ России) и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации (ФСТЭК России), представители вышеуказанных контрольно-надзорных органов не имеют права на ознакомление с персональными данными, обрабатываемыми в информационных системах персональных данных.
6.5**.** При проведении контрольно-надзорных мероприятий в отношении оператора и контрольно-надзорными органами, не осуществляющими контроль и надзор в сфере обработки персональных данных, представители вышеуказанных контрольно-надзорных органов имеют право на доступ к персональным данным только в сфере своей компетенции и в пределах своих полномочий в соответствии с законодательством Российской Федерации.

7.ОБЩЕДОСТУПНЫЕ ИСТОЧНИКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. В целях информационного обеспечения деятельности структурных подразделений и работников оператора могут создаваться общедоступные источники персональных данных, такие как официальный интернет-сайт Оператора. С письменного согласия работника его персональные данные могут быть включены в такие общедоступные базы.
7.2. Персональные данные работника могут быть в любое время исключены из общедоступных источников персональных данных по его требованию либо по решению руководителя оператора, либо суда или иных уполномоченных государственных органов.

8. ОСОБЕННОСТИ ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМ ЛИЦАМ

8.1. Доступ со стороны третьих лиц к персональных данным осуществляется только с письменного согласия субъекта персональных данных, за исключением случаев, когда такой доступ необходим в целях предупреждения угрозы жизни и здоровью работника или других лиц, и иных случаев, установленных законодательством Российской Федерации.

8.2. Оператор обязан сообщать персональные данные по надлежаще оформленным запросам суда, прокуратуры и правоохранительных органов.
8.3. При передаче персональных данных оператор соблюдает следующие условия:
8.3.1. Не сообщать персональные данные третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в случаях, установленных законодательством Российской Федерации;
8.3.2. Не сообщать персональные данные субъекта персональных данных в коммерческих целях без его письменного согласия;
8.3.3. Предупредить лиц, получивших персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено;
8.3.4. Осуществлять передачу персональных данных субъектов в пределах и за пределы Администрации в соответствии с настоящим Положением;
8.3.5. Разрешать доступ к персональным данным, только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции;
8.3.6. Передавать персональные данные представителям субъекта в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций.
8.4. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным органом или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом. В поручении оператора должны быть определены перечень персональных данных, перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели их обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных, требования, предусмотренные частью 5 статьи 18 и статьей 18.1 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», обязанность по запросу оператора персональных данных в течение срока действия поручения оператора, в том числе до обработки персональных данных, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения оператора требований, установленных в соответствии с настоящей статьей, обязанность обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 настоящего Федерального закона, в том числе требование об уведомлении оператора о случаях, предусмотренных частью 3.1 статьи 21 настоящего Федерального закона.

9. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

9.1. Каждый работник оператора, получающий доступ к конфиденциальному документу, содержащему персональные данные, или осуществляющий обработку с использованием ИСПДн несет персональную ответственность за сохранность носителя и конфиденциальность информации.
9.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работников, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами и полную материальную ответственность в случае причинения их действиями ущерба в соответствии с п.7 ст. 243 Трудового кодекса Российской Федерации.
9.3. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», а также требований к защите персональных данных, установленных в соответствии с Законом, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

10. ОСОБЕННОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, РАЗРЕШЕННЫХ СУБЪЕКТОМ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ РАСПРОСТРАНЕНИЯ

10.1. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных. Оператор обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.
10.2. В случае раскрытия персональных данных неопределенному кругу лиц самим субъектом персональных данных без предоставления оператору согласия, предусмотренного настоящим разделом, обязанность предоставить доказательства законности последующего распространения или иной обработки таких персональных данных лежит на каждом лице, осуществившем их распространение или иную обработку.
10.3. В случае, если персональные данные оказались раскрытыми неопределенному кругу лиц вследствие правонарушения, преступления или обстоятельств непреодолимой силы, обязанность предоставить доказательства законности последующего распространения или иной обработки таких персональных данных лежит на каждом лице, осуществившем их распространение или иную обработку.
10.4. В случае, если из предоставленного субъектом персональных данных согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, не следует, что субъект персональных данных согласился с распространением персональных данных, такие персональные данные обрабатываются оператором, которому они предоставлены субъектом персональных данных, без права распространения.
10.5. В случае если из предоставленного субъектом персональных данных согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, не следует, что субъект персональных данных не установил запреты и условия на обработку персональных данных, предусмотренные 11.9 настоящего раздела, или если в

предоставленном субъектом персональных данных таком согласии не указаны категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты в соответствии с частью 11.9 настоящего раздела, такие персональные данные обрабатываются оператором, которому они предоставлены субъектом персональных данных, без передачи (распространения, предоставления, доступа) и возможности осуществления иных действий с персональными данными неограниченному кругу лиц.
10.6. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, может быть предоставлено оператору:
1) непосредственно;
2) с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных.
10.7. Правила использования информационной системы уполномоченного органа по защите прав субъектов персональных данных, в том числе порядок взаимодействия субъекта персональных данных с оператором, определяются уполномоченным органом по защите прав субъектов персональных данных.
10.8. Молчание или бездействие субъекта персональных данных ни при каких обстоятельствах не может считаться согласием на обработку персональных данных, разрешенных субъектом персональных данных для распространения.
10.9. В согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения, субъект персональных данных вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц. Отказ оператора в установлении субъектом персональных данных запретов и условий, предусмотренных настоящим разделом, не допускается.
10.10. Оператор обязан в срок не позднее трех рабочих дней с момента получения соответствующего согласия субъекта персональных данных опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения.
10.11. Установленные субъектом персональных данных запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) персональных данных, разрешенных субъектом персональных данных для распространения, не распространяются на случаи обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации.
10.12. Передача (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения, должна быть прекращена в любое время по требованию субъекта персональных данных. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта персональных данных, а также перечень персональных данных, обработка которых подлежит прекращению. Указанные в данном требовании персональные данные могут обрабатываться только оператором, которому оно направлено.
10.13. Действие согласия субъекта персональных данных на обработку персональных данных, разрешенных субъектом персональных данных для распространения, прекращается с момента поступления оператору требования, указанного в части 10.12 настоящего раздела.
10.14. Субъект персональных данных вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных субъектом персональных данных для распространения, к любому лицу, обрабатывающему его персональные данные, в случае несоблюдения положений настоящего раздела или обратиться с таким требованием в суд. Данное лицо обязано прекратить передачу (распространение, предоставление, доступ) персональных данных в течение трех рабочих дней с момента получения требования субъекта персональных данных или в срок, указанный во вступившем в законную силу решении суда, а если такой срок в решении суда не указан, то в течение трех рабочих дней с момента вступления решения суда в законную силу.

11. ПОЛИТИКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ на сайте Администрации Козловского муниципального округа Чувашской Республики.

Адрес официального веб-сайта Администрации Козловского муниципального округа Чувашской Республики: https://kozlov.cap.ru/.
11.1. Администрация Козловского муниципального округа Чувашской Республики собирает с сайта следующие категории персональных данных:
Фамилия, имя, отчество, адрес электронной почты, номер телефона.
11.2. Цель обработки персональных данных: регистрация обращений граждан.
11.3. Срок обработки персональных данных, полученных с официального сайта Администрации Козловского муниципального округа Чувашской Республики через форму «обращения граждан» до закрытия сайта.
11.4. На сайте происходит сбор и обработка обезличенных данных о посетителях (в т.ч. файлов «cookie») с помощью сервисов интернет-статистики (Яндекс Метрика).
11.5. Обезличенные данные посетителей сайта, собираемые с помощью сервисов интернет-статистики, служат для сбора информации о действиях посетителях на сайте, улучшения качества сайта и его содержания.
11.5.1. Срок обработки персональных данных, полученных с официального сайта Администрации Козловского муниципального округа Чувашской Республики через форму «обращения граждан» до завершения работы сайта.
В случае выявления неточностей в персональных данных, Пользователь может актуализировать их, направив Оператору уведомление с помощью электронной почты на электронный адрес Оператора kozlov@cap.ru, либо на почтовый адрес Оператора 429430, Чувашская Республика, Козловский р-н, г Козловка, ул. Ленина, д. 55 , с пометкой «Актуализация персональных данных».
11.5.2. Пользователь может в любой момент отозвать свое согласие на обработку персональных данных, направив Оператору уведомление с помощью электронной почты на электронный адрес Оператора kozlov@cap.ru либо на почтовый адрес Оператора 429430, Чувашская Республика, Козловский р-н, г Козловка, ул. Ленина, д. 55 , с пометкой «Отзыв согласия на обработку персональных данных».
11.5.3. Пользователь может получить любые разъяснения по интересующим вопросам, касающимся обработки его персональных данных, обратившись к Оператору с помощью электронной почты kozlov@cap.ru, либо на почтовый адрес Оператора 429430, Чувашская Республика, Козловский р-н, г Козловка, ул. Ленина, д. 55 .
11.5.4. В данном документе будут отражены любые изменения политики обработки персональных данных Оператором. В случае существенных изменений Пользователю может быть выслана информация на указанный им электронный адрес.

ПРИЛОЖЕНИЕ 1
к Положению об обработке ПДн
Форма – образец

СОГЛАСИЕ
НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

г. Козловка «___» _____ 20__ г.

Я,_____,
_____серия_____№_____выдан_____
_____, проживающий (ая) по адресу:
_____.

Настоящим даю свое согласие Администрации Козловского муниципального округа Чувашской Республики (429430, Чувашская Республика, Козловский р-н, г. Козловка, ул. Ленина, д. 55) на обработку и передачу моих персональных данных для обработки с использованием средств автоматизации, с передачей полученной информации по локальной сети учреждения и по сети интернет, а также без использования таких средств и подтверждаю, что, давая такое согласие, я действую своей волей и в своих интересах.
Согласие дается мною для целей:
ведения кадровой работы (ведение и хранение личных дел, трудовых книжек) и выполнения всех требований трудового законодательства; заключения трудовых и иных договоров; начисления и выплаты заработной платы работникам; обработки сведений по сотрудникам об их профессиональной служебной деятельности; обработки персональных данных в информационных системах (ИСПДн); оформления доверенностей; оформления документов по воинскому учету в военкоматах в установленном порядке; использования персональных данных для реализации права сотрудника на участие в деятельности первичной профсоюзной организации Администрации Козловского муниципального округа Чувашской Республики, в том числе при отчислении профсоюзных взносов; подготовки документов для прохождения обучения, аттестации, переквалификации; подготовки документов для прохождения медицинского осмотра, ведения табеля посещаемости, оформления журналов; Передача данных в: ОСФР по Чувашской Республике - Чувашии, индивидуальных сведений о начисленных страховых взносов на обязательное пенсионное страхование и данных о трудовом стаже Управление Федеральной налоговой службы по Чувашской Республике, Военный комиссариат Чувашской Республики, кредитные учреждения (банки), ПАО Акционерный коммерческий Сберегательный банк Российской Федерации (адрес: Вавилова ул., д. 19, г. Москва, 117997); АО "Россельхозбанк" (119034, город Москва, Гагаринский пер, д. 3),МКУ «ЦБО и ФХО» Козловского Муниципального округа (429430, Чувашская Республика, Козловский р-н, г Козловка, ул. Ленина, д. 55), медицинские учреждения, органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.
и распространяется на следующую информацию:
- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- адрес проживания, регистрации;
- семейное, социальное, имущественное положение;
- сведения об образовании (наименования оконченных учебных заведений, факультет, специальность, год окончания), информация о дополнительном образовании, повышении квалификации, аттестации;
- профессия;
- доходы, полученные в Администрации;
- специальность;
- гражданство;
- паспортные данные;
- СНИЛС;
-ИНН;
- пол;
- трудовой и общий стаж;
- сведения о детях (количество, возраст);
- социальные льготы;
- сведения о воинском учете;
- контактные телефоны;
- фотография;
- сумма дохода;
- сумма вычета;
- номер лицевого счета;
- стаж работы;
- реквизиты страхового свидетельства обязательного пенсионного страхования;
- прежнее место работы (структурное подразделение), наименование структурного подразделения, наименование должности;
- уровень владения иностранными языками;
- профессиональные навыки;
- информация об аттестации (дата аттестации, решение комиссии, номер, дата протокола);
- информация о повышении квалификации (дата начала и окончания обучения, вид повышения квалификации, наименование образовательного учреждения, серия, №, дата выдачи документа об образовании);
- сведения о профессиональной переподготовке (дата начала и окончания обучения, специальность (направление, профессия), серия, номер, дата выдачи документа);
- информация о наградах (поощрениях), почетных званиях (наименование награды, номер и дата выдачи документа), размер вознаграждения;
- данные об отпусках (вид отпуска, период, дата начала и окончания отпуска);

- отметки о явках и неявках на работу по числам месяца, количество неявок, причины неявок;
- количество отработанных часов за месяц, количество выходных и праздничных дней;
- сведения о социальных льготах, на которые работник имеет право в соответствии с законодательством (наименование льготы, номер и дата выдачи документа);
- номер, дата трудового договора;
- испытательный срок;
- серия и номер трудовой книжки или вкладыша в неё;
- основание прекращения (расторжения) трудового договора (увольнения), причина увольнения, дата увольнения, номер и дата приказа;
- сведения о судимости в соответствии с законодательством РФ.
- данные свидетельств о браке и (или) о расторжении брака, о смене фамилии.
- сведения о доходах, расходах, об имуществе и обязательствах имущественного характера, а также о доходах, расходах, об имуществе и обязательствах имущественного характера супруги (супруга) и несовершеннолетних детей;
- сведения, содержащиеся в служебном контракте (трудовом договоре), дополнительных соглашениях к служебному контракту (трудовому договору);
- сведения об участии в выборных органах (с указанием времени пребывания, наименование органа);
- сведения о классном чине гражданской службы Российской Федерации (дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине гражданской службы субъекта Российской Федерации), квалификационном разряде гражданской службы (квалификационном разряде или классном чине муниципальной службы), кем и когда присвоены;
- реквизиты банковской карты.

А также согласие дается мною с целью размещения следующих сведений обо мне на сайте и информационных стендах Администрации: ФИО, должность, фотографию, телефон, адрес электронной почты.

А также дополнительную информацию в соответствии с требованиями ст. 65 Трудового кодекса РФ

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая (без ограничения) сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение, а также осуществление любых иных действий с моими персональными данными с учетом действующего законодательства Российской Федерации.

Передача моих персональных данных разрешается на срок действия трудового договора.

В случае неправомерного использования предоставленных мною персональных данных согласие отзывается моим письменным заявлением.

Срок прекращения обработки персональных данных определяется законодательством об архивном деле с даты передачи карточки персонального учета работника в архив (75 лет).

_____ _____

(фамилия, инициалы) (подпись)

«____» _____20__ г

ПРИЛОЖЕНИЕ 2
к Положению об обработке ПДн
Форма – образец

Главе
Козловского муниципального округа

_____
(Ф.И.О. субъекта персональных данных)
проживающего по адресу:_____
_____
паспорт серии _____№_____
выдан_____
_____
_____

заявление.

Прошу Вас прекратить обработку моих персональных данных в связи с _____
_____
_____
(указать причину)

_____ _____
(фамилия, инициалы) (подпись)
«____» _____20__ г

ПРИЛОЖЕНИЕ 3
к Положению об обработке ПДн
Форма – образец

Согласие
субъекта персональных данных на получение персональных данных от третьих лиц

Я,_____,
_____серия_____№_____выдан_____
_____, проживающий (ая) по адресу:
_____
_____
согласен на получение Администрацией Козловского муниципального округа Чувашской Республики(429430, Чувашская Республика, Козловский р-н, г Козловка, ул. Ленина, д. 55) информации, содержащей мои персональные данные:
_____
_____
_____
(виды передаваемой информации и (или) документов)
от следующих юридических (физических) лиц:
_____
_____
_____
(Ф.И.О. или наименование третьих лиц)

с целью:
_____
_____
_____

Отзыв согласия на получение персональных данных может быть осуществлен в любое время по письменному заявлению в адрес Главы Козловского муниципального округа Чувашской Республики.

_____ _____
(фамилия, инициалы) (подпись)
«____» _____20__ г

ПРИЛОЖЕНИЕ 4
к Положению об обработке ПДн
Форма – образец

Уведомление

Уважаемый_____
_____
(Ф.И.О.)
на основании_____ Администрация Козловского муниципального округа Чувашской Республики (429430, Чувашская Республика, Козловский р-н, г Козловка, ул. Ленина, д. 55) получила от _____
_____
(наименование организации)
следующую информацию, содержащую Ваши персональные данные:
_____
_____
_____
_____
с
целью:_____
_____

Вы имеете право:
- на полную информацию о Ваших персональных данных, обрабатываемых оператором;
- на свободный бесплатный доступ к Вашим персональным данным, включая право на получение копии любой записи, содержащей Ваши персональные данные, за исключением случаев, предусмотренных действующим законодательством;
- требовать от оператора уточнения Ваших персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав, получать иную информацию, касающуюся обработки Ваших персональных данных.
-

_____ _____
(фамилия, инициалы) (подпись)
«____» _____20__ г.

Настоящее уведомление на руки получил.

_____ _____
(фамилия, инициалы) (подпись)
«____» _____20__ г.

ПРИЛОЖЕНИЕ 5
к Положению об обработке ПДн
Форма – образец

Уведомление
об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке персональных данных

Уважаемый_____
_____
(Ф.И.О.)

В связи с
_____
_____
_____
_____

сообщаем Вам, что обработка Ваших персональных данных прекращена и указанная информация подлежит уничтожению (изменению).

_____ _____
(фамилия, инициалы) (подпись)
«____» _____20__ г.

Настоящее уведомление на руки получил:

(_____ _____
(фамилия, инициалы) (подпись)
«____» _____20__ г.

ПРИЛОЖЕНИЕ 6
к Положению об обработке персональных данных
Администрации Козловского муниципального округа
Чувашской Республики
Форма – образец

Соглашение о неразглашении персональных данных

Я,_____,
_____серия_____№_____выдан_____
_____, проживающий (ая) по адресу:
_____
_____.

Предупрежден (а) о том, что на период исполнения должностных обязанностей в соответствии с должностной инструкцией мне будет предоставлен допуск к информации, содержащей персональные данные.

Я подтверждаю, что не имею права разглашать следующие сведения: фамилия, имя, отчество, год, месяц, дата и место рождения; адрес проживания, регистрации; семейное, социальное, имущественное положение; образование, профессия; специальность; гражданство; паспортные данные; СНИЛС; ИНН; пол; трудовой и общий стаж; доходы, полученные мной в данной организации; сведения о воинском учете; социальные льготы; контактные телефоны; фотография; сведения о детях; сумма дохода; сумма вычета; номер лицевого счета; уровень владения иностранными языками; стаж работы; прежнее место работы (структурное подразделение); информация об аттестации (дата аттестации, решение комиссии, номер, дата протокола); информация о повышении квалификации (дата начала и окончания обучения, вид повышения квалификации, наименование образовательного учреждения, серия, №, дата выдачи документа об образовании);сведения о профессиональной переподготовке (дата начала и окончания обучения, специальность (направление, профессия), серия, номер, дата выдачи документа); информация о наградах (поощрениях), почетных званиях (наименование награды, номер и дата выдачи документа), размер вознаграждения; данные об отпусках (вид отпуска, период, дата начала и окончания отпуска); отметки о явках и неявках на работу по числам месяца, количество неявок, причины неявок; количество отработанных часов за месяц, количество выходных и праздничных дней; сведения о социальных льготах, на которые сотрудник имеет право в соответствии с законодательством (наименование льготы, номер и дата выдачи документа); номер, дата трудового договора; испытательный срок; место назначения, дата начала и окончания, срок и цель командировки; сведения о наличии водительских прав(категория, стаж); серия и номер трудовой книжки или вкладыша в ней; основание прекращения (расторжения) трудового договора (увольнения), причина увольнения, дата увольнения, номер и дата приказа;

В связи с этим, даю обязательство, при обработке персональных данных соблюдать все описанные в Положении об обработке персональных данных требования.

Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.
2. В случае попытки посторонних лиц получить от меня информацию, содержащую персональные данные, а также в случае утери носителей информации, содержащих такие сведения, немедленно сообщить об этом лицу, ответственному за организацию обработки персональных данных.
3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.
4. Не производить преднамеренных действий, нарушающих достоверность, целостность или конфиденциальность персональных данных, хранимых или обрабатываемых в Администрации Козловского муниципального округа Чувашской Республики (429430, Чувашская Республика, Козловский р-н, г Козловка, ул. Ленина, д. 55).
5. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.
6. В течение года после прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

_____«____» _____20__ г.
(фамилия, инициалы) (подпись)

Мне известно, что нарушение этого обязательства может повлечь ответственность трудовым, административным и уголовным законодательством РФ.

С Положением об обработке персональных данных Администрации Козловского муниципального округа Чувашской Республики ознакомлен (а).

_____«____» _____20__ г.
(фамилия, инициалы) (подпись)

ПРИЛОЖЕНИЕ 7
к Положению об обработке ПДн
Форма – образец

АКТ УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Председатель комиссии:
_____
Член комиссии:
_____
Составили настоящий акт в том, что «__»_____20__г. произведено удаление персональных данных находящейся на _____
тип носителя (магнитный, бумажный)
носителе ответственного пользователя_____
(ФИО, должность)
персональных данных_____
тип удаляемых персональных данных (персональные данные субъектов ПДн)
путем_____
способ уничтожения (разрезание, удаление данных на магнитном носителе)
следующих персональных данных:

№ № п/п	Дата уничтожения	№ договора	Пояснения
1			

Председатель комиссии:

_____ _____
(фамилия, инициалы) (подпись)

Член комиссии:

_____ _____
(фамилия, инициалы) (подпись)

ПРИЛОЖЕНИЕ 8
к Положению об обработке ПДн
Форма – образец

Журнал учета обращений субъектов персональных данных (работников) по вопросам обработки персональных данных и для получения доступа к своим персональным данным

_____
(наименование организации)

_____
(адрес организации)

Журнал начат «____» _____ 20__ г.
Должность
_____ / ФИО должностного лица /

Журнал завершен «____» _____ 20__ г.
Должность
_____ / ФИО должностного лица /

На _____ листах

№ п/п	Дата, № и реквизит запроса	Сведения об обратившемся субъекте ПДн (ФИО, адрес)	Краткое содержание обращения (цель обработки (получения) ПДн	Источник получения ПДн	Сроки обработки ПДн	Отметка о предоставлении информации или отказе в ее предоставлении	Способы обработки ПДн и перечень действий с ПДн	Дата передачи / отказа в предоставлении информации	Причина отказа	Подпись ответственного лица	Примечание
1	2	3	4	5	6	7	8	9	10	11	12

ПРИЛОЖЕНИЕ 9
к Положению об обработке ПДн
Форма – образец

Журнал учета передачи персональных данных

_____
(наименование организации)

_____
(адрес организации)

Журнал начат «____» _____ 20__ г.
Должность
_____ / ФИО должностного лица /

Журнал завершен «____» _____ 20__ г.
Должность
_____ / ФИО должностного лица /

На _____ листах

№ п/п	Сведения о запрашивающем лице (ФИО, адрес)	Цель получения запрашиваемых ПДн	Источник получения ПДн	Сроки обработки ПДн	Отметка о предоставлении информации или отказе в ее предоставлении	Способы обработки ПДн и перечень действий с ПДн	Дата передачи / отказа в предоставлении информации	Подпись ответственного лица	Примечание
1	2	3	4	5	6	7	8	9	10

ПРИЛОЖЕНИЕ 10
к Положению об обработке ПДн
Форма – образец

Журнал учета электронных носителей персональных данных

_____
(наименование организации)

_____
(адрес организации)

Журнал начат «____» _____ 20__ г.
Должность
_____ / ФИО должностного лица /

Журнал завершен «____» _____ 20__ г.
Должность
_____ / ФИО должностного лица /

На _____ листах

Учетный номер	Дата постановки на учет	Вид электронного носителя	Место хранения (размещения)	Лицо, ответственное за использование и хранение					Отметка об уничтожении	
				ФИО, должность	Дата получения	Подпись	Дата возврата	Подпись	Дата и номер акта	Подпись ответственного лица
1	2	3	4	5	6	7	8	9	10	11

ПРИЛОЖЕНИЕ 11
к Положению об обработке ПДн
Форма – образец

ЖУРНАЛ
поэкземплярного учета средств защиты информации, эксплуатационной и технической документации к ним

№ п/п	Наименование СЗИ, эксплуатационной и технической документации к ним	Серийные номера СЗИ, эксплуатационной и технической документации к ним	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СЗИ			Отметка об изъятии СЗИ из аппаратных средств			Примечание
			От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СЗИ	Дата и расписка в получении	Ф.И.О. работников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СЗИ	Дата изъятия (уничтожения)	Ф.И.О. работников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	5	6	7	8	9	10	11	12	13	14	15

ПРИЛОЖЕНИЕ 12
к Положению об обработке ПДн
Форма – образец

ЖУРНАЛ
поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении	Ф.И.О. работников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. работников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

ПРИЛОЖЕНИЕ 13
к Положению об обработке ПДн
Форма – образец

ЛИЦЕВОЙ СЧЕТ
пользователя криптосредств

_____

(должность, ФИО)

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о передаче		Отметка о возврате, уничтожении		Примечание
				От кого получены	Дата и расписка в получении	Кому передано СКЗИ	Дата и расписка в передаче	Дата возврата (уничтожения)	Расписка о возврате (уничтожении)	
1	2	3	4	5	6	7	8	9	10	11

ПРИЛОЖЕНИЕ 14
к Положению об обработке ПДн
Форма – образец

Журнал учета хранилищ (сейфов)

Учетный номер	Наименование хранилища (сейф, металлический шкаф)	Инвентарный номер	Местонахождение (подразделение, номер комнаты)	Что находится (документы, изделия)	Фамилия ответственного за сейф (шкаф)	Кол-во комплектов ключей и их номера	Расписка ответственного за хранилище в получении ключа и дата	Расписка в приеме ключа и дата
1	2	3	4	5	6	7	8	9

ПРИЛОЖЕНИЕ 15
к Положению об обработке ПДн
Форма – образец

ЖУРНАЛ
учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ПЭВМ

№ п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО исполнителей и их подписи	ФИО ответственного за эксплуатацию ПЭВМ, подпись	Подпись администратора безопасности	Примечание (ссылка на заявку)
1	2	3	4	5	6	7

ПРИЛОЖЕНИЕ 16
к Положению об обработке ПДн
Форма – образец

Журнал периодического тестирования средств защиты информации

Дата тестирования	Наименование средства защиты	Цель, задачи тестирования	Результат тестирования	Фамилия, имя, отчество, должность должностного лица (должностных лиц), проводящего(их) тестирование	Подпись должностного лица (лиц), проводившего тестирование
1	2	3	4	5	6

ПРИЛОЖЕНИЕ 17
к Положению об обработке ПДн
Форма – образец

Журнал проверок электронных журналов

Дата проверки	Наименование журнала	Цель, задачи проверки	Результат проверки	Фамилия, имя, отчество, должность должностного лица (должностных лиц), проводящего(их) проверку	Подпись должностного лица (лиц), проводившего проверку
1	2	3	4	5	6

ПРИЛОЖЕНИЕ 18
к Положению об обработке ПДн
Форма – образец

СОГЛАСИЕ
НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ, РАЗРЕШЕННЫХ ДЛЯ РАСПРОСТРАНЕНИЯ

г. Козловка «___» _____ 20__ г.

Я,_____,
Фамилия, имя, отчество

контактная информация: _____
(номер телефона, адрес электронной почты или почтовый адрес)

_____.

Настоящим даю свое согласие Администрации Козловского муниципального округа Чувашской Республики(429430, Чувашская Республика, Козловский р-н, г Козловка, ул. Ленина, д. 55) ИНН2100001964, ОГРН1222100008426, на обработку моих персональных данных, разрешенных для распространения с использованием средств автоматизации, с передачей полученной информации по локальной сети учреждения и по сети интернет, а также без использования таких средств на информационном ресурсе оператора – официальном сайте по адресу: https://kozlov.cap.ru/., посредством которого будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными и подтверждаю, что, давая такое согласие, я действую своей волей и в своих интересах.

Согласие дается мною для целей:

Исполнения *приказа Роскомнадзора от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения* размещения следующих сведений обо мне на официальном сайте Администрации, расположенному по адресу: https://kozlov.cap.ru/.

Категория и перечень персональных данных, на обработку которых дается согласие: ФИО, должность, фотографию, телефон, адрес электронной почты.

Категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты, а также перечень устанавливаемых условий и запретов

_____
(Заполняется по желанию субъекта персональных данных часть 9, ст.10.1 Федерального закона от 27 июля 2006 г.№ 152-ФЗ «О персональных данных»)

условия, при которых полученные персональные данные могут передаваться оператором, осуществляющим обработку персональных данных, только по его внутренней сети, обеспечивающей доступ к информации лишь для строго определенных сотрудников, либо с использованием информационно-телекоммуникационных сетей, либо без передачи полученных персональных данных.

_____
(Заполняется по желанию субъекта персональных данных часть 9, ст.10.1 Федерального закона от 27 июля 2006 г.№ 152-ФЗ «О персональных данных»)

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая (без ограничения) сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение, а также осуществление любых иных действий с моими персональными данными с учетом действующего законодательства Российской Федерации.

Согласие на обработку моих персональных данных, разрешенных для распространения дается на срок действия трудового договора или до срока завершения работы сайта, в зависимости от того, какое событие наступит раньше.

В случае неправомерного использования предоставленных мною персональных данных согласие отзывается моим письменным заявлением.

_____«____»_____20__г.
(фамилия, инициалы) (подпись)

ПРИЛОЖЕНИЕ 19
к Положению об обработке ПДн
Форма – образец

ОБЯЗАТЕЛЬСТВО
работника Администрации Козловского муниципального округа Чувашской Республики (далее – Администрации), непосредственно осуществляющего обработку персональных данных, прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей, в случае расторжения с ним служебного контракта

Я, _____,
(фамилия, имя, отчество полностью)
_____
(наименование должности и структурного подразделения)
_____
обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной служебного контракта (трудового договора).
В соответствии со статьей 7 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией, и обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставшие известными мне в связи с исполнением должностных обязанностей.
Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к ответственности в соответствии с законодательством Российской Федерации.

"__" _____ 20__ года _____ _____
(подпись) (фамилия, инициалы)

ПРИЛОЖЕНИЕ 20
к Положению об обработке ПДн
Форма – образец

РАЗЪЯСНЕНИЕ
субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

Мне, _____,
(фамилия, имя, отчество)
разъяснены юридические последствия отказа предоставить свои персональные данные _____.
(указать)
В соответствии со статьями 26 и 42 Федерального закона от 27.07.2004 №79-ФЗ «О государственной гражданской службе Российской Федерации», Положением о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела, утвержденным Указом Президента Российской Федерации от 30.05.2005 №609, определен перечень персональных данных, которые субъект персональных данных обязан предоставить в связи с поступлением на государственную гражданскую службу или прохождением государственной гражданской службы.
Без предоставления субъектом персональных данных обязательных для заключения служебного контракта сведений служебный контракт не может быть заключен.
На основании пункта 11 части 1 статьи 33 Федерального закона от 27.07.2004 №79-ФЗ «О государственной гражданской службе Российской Федерации» служебный контракт прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность замещения должности государственной гражданской службы.

"__" _____ 20__ года _____ _____
(подпись) (фамилия, инициалы)

ПРИЛОЖЕНИЕ 21
к Положению об обработке ПДн
Форма – образец

ПЕРЕЧЕНЬ
должностей муниципальных служащих Администрации Козловского муниципального округа Чувашской Республики, ответственных
за проведение мероприятий по обезличиванию персональных данных

№ п/п	Должность
1.	Глава Козловского муниципального округа Чувашской Республики
2.	Пресс-секретарь главы МО
3.	Первый заместитель главы администрации МО - начальник Управления по благоустройству и развитию территорий
4.	Заместитель главы администрации МО по экономике и сельскому хозяйству - начальник отдела экономики, инвестиционной деятельности, земельных и имущественных отношений
5.	Заместитель главы администрации МО по социальным вопросам - начальник отдела образования и молодежной политики
6.	Советник главы администрации МО по работе с молодежью
7.	Управляющий делами МО - начальник отдела организационно-контрольной и кадровой работы
8.	Заместитель начальника отдела организационно-контрольной и кадровой работы
9.	Начальник отдела правового обеспечения и цифрового развития
10.	Главный специалист-эксперт отдела правового обеспечения и цифрового развития
11.	Ведущий специалист-эксперт отдела правового обеспечения и цифрового развития
12.	Заведующий сектором цифрового развития и информационных технологий
13	Ведущий специалист-эксперт сектора цифрового развития и информационных технологий
14.	Начальник отдела ЗАГС
15.	Ведущий специалист-эксперт отдела ЗАГС
16.	Главный специалист-эксперт отдела образования и молодежной политики
17.	Заведующий сектором опеки и попечительства
18.	Главный специалист-эксперт сектора опеки и попечительства
19.	Главный специалист-эксперт - ответственный секретарь комиссии по делам несовершеннолетних и защите их прав
20.	Начальник отдела культуры, спорта, социального развития и архивного дела
21.	Главный специалист-эксперт отдела культуры, спорта, социального развития и архивного дела
22.	Заместитель начальника отдела экономики, инвестиционной деятельности, земельных и имущественных отношений
23.	Главный специалист-эксперт отдела экономики, инвестиционной деятельности, земельных и имущественных отношений
24.	Заведующий сектором организации и проведения муниципальных закупок
25.	Главный специалист-эксперт сектора организации и проведения муниципальных закупок
26.	Начальник отдела сельского хозяйства и экологии
27.	Заместитель начальника отдела сельского хозяйства и экологии
28.	Ведущий специалист-эксперт отдела сельского хозяйства и экологии
29.	Заведующий сектором земельных и имущественных отношений
30.	Главный специалист-эксперт сектора земельных и имущественных отношений
31.	Начальник отдела строительства, дорожного хозяйства и ЖКХ
32.	Заместитель начальника отдела строительства, дорожного хозяйства и ЖКХ
33.	Главный специалист-эксперт отдела строительства, дорожного хозяйства и ЖКХ
34	Заведующий сектором дорожного хозяйства
35.	Ведущий специалист-эксперт сектором дорожного хозяйства
36.	Начальник отдела по мобилизационной работе
37.	Ведущий специалист-эксперт по мобилизационной работе
38.	Заведующий сектором по ГО ЧС
39.	Инспектор ВУС
40.	Начальник финансового отдела
41.	Заместитель начальника - главный бухгалтер
42.	Главный специалист-эксперт финансового отдела
43.	Ведущий специалист-эксперт финансового отдела
44.	Начальник-главный бухгалтер центра бухгалтерского обслуживания и финансово - хозяйственного обеспечения
45.	Ведущий экономист
46.	Ведущий специалист по кадрам

ПРИЛОЖЕНИЕ 22
к Положению об обработке ПДн
Форма – образец

ПЕРЕЧЕНЬ
должностей муниципальных служащих Администрации Козловского муниципального округа Чувашской Республики, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

№ п/п	Должность
1.	Глава Козловского муниципального округа Чувашской Республики
2.	Пресс-секретарь главы МО
3.	Первый заместитель главы администрации МО - начальник Управления по благоустройству и развитию территорий
4.	Заместитель главы администрации МО по экономике и сельскому хозяйству - начальник отдела экономики, инвестиционной деятельности, земельных и имущественных отношений
5.	Заместитель главы администрации МО по социальным вопросам - начальник отдела образования и молодежной политики
6.	Советник главы администрации МО по работе с молодежью
7.	Управляющий делами МО - начальник отдела организационно-контрольной и кадровой работы
8.	Заместитель начальника отдела организационно-контрольной и кадровой работы
9.	Начальник отдела правового обеспечения и цифрового развития
10.	Главный специалист-эксперт отдела правового обеспечения и цифрового развития
11.	Ведущий специалист-эксперт отдела правового обеспечения и цифрового развития
12.	Заведующий сектором цифрового развития и информационных технологий
13	Ведущий специалист-эксперт сектора цифрового развития и информационных технологий
14.	Начальник отдела ЗАГС
15.	Ведущий специалист-эксперт отдела ЗАГС
16.	Главный специалист-эксперт отдела образования и молодежной политики
17.	Заведующий сектором опеки и попечительства
18.	Главный специалист-эксперт сектора опеки и попечительства
19.	Главный специалист-эксперт - ответственный секретарь комиссии по делам несовершеннолетних и защите их прав
20.	Начальник отдела культуры, спорта, социального развития и архивного дела
21.	Главный специалист-эксперт отдела культуры, спорта, социального развития и архивного дела
22.	Заместитель начальника отдела экономики, инвестиционной деятельности, земельных и имущественных отношений
23.	Главный специалист-эксперт отдела экономики, инвестиционной деятельности, земельных и имущественных отношений
24.	Заведующий сектором организации и проведения муниципальных закупок
25.	Главный специалист-эксперт сектора организации и проведения муниципальных закупок
26.	Начальник отдела сельского хозяйства и экологии
27.	Заместитель начальника отдела сельского хозяйства и экологии
28.	Ведущий специалист-эксперт отдела сельского хозяйства и экологии
29.	Заведующий сектором земельных и имущественных отношений
30.	Главный специалист-эксперт сектора земельных и имущественных отношений
31.	Начальник отдела строительства, дорожного хозяйства и ЖКХ
32.	Заместитель начальника отдела строительства, дорожного хозяйства и ЖКХ
33.	Главный специалист-эксперт отдела строительства, дорожного хозяйства и ЖКХ
34	Заведующий сектором дорожного хозяйства
35.	Ведущий специалист-эксперт сектором дорожного хозяйства
36.	Начальник отдела по мобилизационной работе
37.	Ведущий специалист-эксперт по мобилизационной работе
38.	Заведующий сектором по ГО ЧС
39.	Инспектор ВУС
40.	Начальник финансового отдела
41.	Заместитель начальника - главный бухгалтер
42.	Главный специалист-эксперт финансового отдела
43.	Ведущий специалист-эксперт финансового отдела
44.	Начальник-главный бухгалтер центра бухгалтерского обслуживания и финансово - хозяйственного обеспечения
45.	Ведущий экономист
46.	Ведущий специалист по кадрам

ПРИЛОЖЕНИЕ 23
к Положению об обработке ПДн
Форма – образец

ОБЯЗАТЕЛЬСТВО
о неразглашении конфиденциальной информации

Я_____,
(фамилия, имя, отчество)

исполняющий должностные обязанности по занимаемой должности_____
_____ (наименование должности и структурного подразделения) _____

предупрежден(а), что на период исполнения должностных обязанностей в Администрации Козловского муниципального округа Чувашской Республики (далее – Администрация) в соответствии с должностным регламентом, мне будет предоставлен допуск к конфиденциальной информации (персональным данным), не содержащим сведений, составляющих государственную тайну. Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.
2. Не передавать и не раскрывать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.
3. В случае попытки третьих лиц получить от меня конфиденциальные сведения, сообщать непосредственному руководителю.
4. Не использовать конфиденциальные сведения с целью получения выгоды.
5. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты конфиденциальных сведений.
6. В случае моего увольнения все материальные носители, содержащие конфиденциальную информацию, которые находились в моем распоряжении передать непосредственному руководителю.
7. Об утрате или недостаче носителей конфиденциальной информации, удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о других фактах, которые могут привести к разглашению конфиденциальной информации, а также о причинах и условиях возможной утечки сведений, немедленно сообщать непосредственному руководителю.
8. После прекращения права на допуск к конфиденциальным сведениям не разглашать и не передавать третьим лицам известные мне конфиденциальные сведения.

Я предупрежден (а), что в случае нарушения данного обязательства буду привлечен (а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

_____ _____ «__» _____ 20___ г.
подпись Ф.И.О.

Приложение № 2
Утверждена
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

АДМИНИСТРАЦИИ КОЗЛОВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА ЧУВАШСКОЙ РЕСПУБЛИКИ

г. Козловка
2024 г.

Определения

В настоящем документе используются следующие термины и их определения.

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

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность и которые используются Администрацией для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных (включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию).

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

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

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

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

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых становится невозможно без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование,

распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Обозначения и сокращения

АВС – антивирусные средства
АРМ – автоматизированное рабочее место
ВТСС – вспомогательные технические средства и системы
ИСПДн – информационная система персональных данных
КЗ – контролируемая зона
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОС – операционная система
ПДн – персональные данные
ПМВ – программно-математическое воздействие
ПО – программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
САЗ – система анализа защищенности
СЗИ – средства защиты информации
СЗПДн – система (подсистема) защиты персональных данных
СОВ – система обнаружения вторжений
ТКУИ – технические каналы утечки информации
УБПДн – угрозы безопасности персональных данных

Введение

Настоящая Политика информационной безопасности (далее Политика) Администрации Козловского муниципального округа Чувашской Республики (далее Администрация), является официальным документом.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 1ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», на основании:

«Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных Заместителем директора ФСТЭК России от 15.02.2008 г.,

«Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае из использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 г. № 149/6/6-662.

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн Администрации.

Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты Администрации от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения персональных данных.

Состав объектов защиты представлен в Перечне персональных данных, указанному в Положении об обработке персональных данных.

Состав ИСПДн, подлежащих защите, представлен в Акте обследования текущего состояния технической защиты персональных данных.

Область действия

Требования настоящей Политики распространяются на всех сотрудников Администрации (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

Система защиты персональных данных

Система защиты персональных данных (СЗПДн), строится на основании:

Акта обследования текущего состояния технической защиты персональных данных;

Перечня персональных данных, подлежащих защите;

Актов классификации информационных систем персональных данных;

Частных моделей актуальных угроз и вероятного нарушителя ИСПДн;

Положения о разграничении прав доступа к персональным данным;
Руководящих документов ФСТЭК и ФСБ России.
Для обеспечения защиты ИСПДн необходимо соблюдение организационно-технических мер. Администрацией обеспечивается безопасность персональных данных в соответствии с необходимым уровнем защищенности, которая описана в Техническом задании на создание системы защиты для ИСПДн. В Администрации определены актуальные угрозы безопасности ПДн, которые описаны в Частной модели актуальных угроз и вероятного нарушителя ИСПДн.
Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.
Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.
Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.
Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.
На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Администрации. На основании анализа актуальных угроз безопасности ПДн, описанного в Частной модели актуальных угроз и вероятного нарушителя ИСПДн и Отчета о результатах проведения внутренней проверке, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по защите персональных данных.
Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а так же программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн:
АРМ пользователей;
Сервера приложений;
СУБД;
Граница ЛВС;
Каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.
В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:
антивирусные средства для рабочих станций пользователей и серверов;
средства межсетевого экранирования;
средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.
Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:
управление и разграничение доступа пользователей;
регистрацию и учет действий с информацией;
- обеспечивать целостность данных;
- производить обнаружений вторжений.
Список используемых технических средств отражается в Плане мероприятий по защите персональных данных. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Список и утверждены Глава или лицом, ответственным за обеспечение защиты ПДн.

Требования к подсистемам СЗПДн

СЗПДн включает в себя следующие подсистемы:
управления доступом, регистрации и учета;
обеспечения целостности и доступности;
антивирусной защиты;
межсетевого экранирования;
анализа защищенности;
обнаружения вторжений;
криптографической защиты.
Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определенного в Акте классификации информационных систем персональных данных. Список соответствия функций подсистем СЗПДн классу защищенности представлен в Приложении № 1.

Подсистемы управления доступом, регистрации и учета

Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:
идентификации и проверка подлинности субъектов доступа при входе в ИСПДн;
идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;
идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;
регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.
регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.
Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Так же может быть внедрено специальное техническое средство или их комплекс, осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей

пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

Подсистема обеспечения целостности и доступности

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн Администрации, а так же средств защиты, при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а так же резервированием ключевых элементов ИСПДн.

Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн Администрации.

Средства антивирусной защиты предназначены для реализации следующих функций:

резидентный антивирусный мониторинг;

антивирусное сканирование;

скрипт-блокирование;

централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;

автоматизированное обновление антивирусных баз;

ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;

автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

Подсистема межсетевого экранирования

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

фильтрации открытого и зашифрованного (закрытого) IP-трафика по следующим параметрам;

фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;

идентификации и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ;

регистрации входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова;

контроля целостности своей программной и информационной части;

фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;

регистрации и учета запрашиваемых сервисов прикладного уровня;

блокирования доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;

контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛСВ, классом не ниже 4.

Подсистема анализа защищенности

Подсистема анализа защищенности, должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

Подсистема обнаружения вторжений

Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы ИСПДн, подключенные к сетям общего пользования и (или) международного обмена.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

Подсистема криптографической защиты

Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн Администрации, при ее передачи по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется внедрением криптографических программно-аппаратных комплексов.

Пользователи ИСПДн

В ИСПДн Администрации можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

Администратора ИСПДн;

Администратора безопасности ИСПДн;

Оператора АРМ;

Администратора сети;

Технического специалиста по обслуживанию периферийного оборудования;

Программист-разработчик ИСПДн.

Данные о группах пользователях, уровне их доступа и информированности должен быть отражен в Положении о разграничении прав доступа к персональным данным.

Администратор ИСПДн

Администратор ИСПДн, сотрудник Администрации, ответственный за настройку, внедрение и сопровождение ИСПДн, обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим персональные данные.

Администратор ИСПДн обладает следующим уровнем доступа и знаний:

обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

обладает полной информацией о технических средствах и конфигурации ИСПДн;

имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

обладает правами конфигурирования и административной настройки технических средств ИСПДн.

Администратор безопасности ИСПДн

Администратор безопасности ИСПДн, сотрудник Администрации, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

Администратор безопасности ИСПДн обладает следующим уровнем доступа и знаний:

обладает правами Администратора ИСПДн;

обладает полной информацией об ИСПДн;
имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).
Администратор безопасности ИСПДн уполномочен:
реализовывать политику безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн;
осуществлять аудит средств защиты;
устанавливать доверительные отношения своей защищенной сети с сетями других Организаций.

Оператор АРМ

Оператор АРМ, сотрудник Администрации, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПДн. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.
Оператор ИСПДн обладает следующим уровнем доступа и знаний:
обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
располагает конфиденциальными данными, к которым имеет доступ.

Администратор сети

Администратор сети, сотрудник Администрации, ответственный за функционирование телекоммуникационной подсистемы ИСПДн. Администратор сети не имеет полномочий для управления подсистемами обработки данных и безопасности.
Администратор сети обладает следующим уровнем доступа и знаний:
обладает частью информации о системном и прикладном программном обеспечении ИСПДн;
обладает частью информации о технических средствах и конфигурации ИСПДн;
имеет физический доступ к техническим средствам обработки информации и средствам защиты;
знает, по меньшей мере, одно легальное имя доступа.

Технический специалист по обслуживанию периферийного оборудования

Технический специалист по обслуживанию, сотрудник Администрации, осуществляет обслуживание и настройку периферийного оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности.
Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:
обладает частью информации о системном и прикладном программном обеспечении ИСПДн;
обладает частью информации о технических средствах и конфигурации ИСПДн;
знает, по меньшей мере, одно легальное имя доступа.

Программист-разработчик ИСПДн

Программисты-разработчики (поставщики) прикладного программного обеспечения, обеспечивающие его сопровождение на защищаемом объекте. К данной группе могут относиться как сотрудники Администрации, так и сотрудники сторонних организаций.
Физическое лицо этой категории:
обладает информацией об алгоритмах и программах обработки информации на ИСПДн;
обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;
может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

Требования к персоналу по обеспечению защиты ПДн

Все сотрудники Администрации, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.
При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.
Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.
Сотрудники Администрации, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.
Сотрудники Администрации должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).
Сотрудники Администрации должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.
Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.
Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Администрации, третьим лицам.
При работе с ПДн в ИСПДн сотрудники Администрации обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.
При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.
Сотрудники Администрации должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили Политику информационной безопасности и процедуры безопасности ПДн.
Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:
Инструкция администратора ИСПДн;
Инструкция администратора безопасности ИСПДн;
Инструкция пользователя ИСПДн.
Ответственность сотрудников ИСПДн Администрации.
В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.
Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).
Администратор ИСПДн и администратор безопасности ИСПДн несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.
При нарушениях сотрудниками Администрации – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.
Приведенные выше требования нормативных документов по защите информации должны быть отражены в Положениях о подразделениях Администрации, осуществляющих обработку ПДн в ИСПДн и должностных инструкциях сотрудников Администрации.
Необходимо внести в Положения о структурных подразделениях Администрации, осуществляющих обработку ПДн в ИСПДн сведения об ответственности их руководителей и сотрудников за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

Список использованных источников

Основными нормативно-правовыми и методическими документами, на которых базируется настоящее Положение являются:
1 Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.
2 Постановление Правительства Российской Федерации от 1ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
3 «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15.09.2008 г. № 687.
4 «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утвержденные Постановлением Правительства РФ от 06.07.2008 г. № 512.
5 Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее - ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн:
6 Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г.
7 Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)
8 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г.
9 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г.

Приложение 1 к Политикой информационной безопасности

№	План - перечень технических мероприятий по обеспечении безопасности ИСПД	К3	К2	К1
I	В подсистеме управления доступом:			
1	Реализовать идентификацию и проверку подлинности субъектов доступа при входе в операционную систему ИСПДн по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;	+	+	+
2	Реализовать идентификацию терминалов, технических средств обработки ПДн, узлов ИСПДн, компьютеров, каналов связи, внешних устройств ИСПДн по их логическим именам (адресам, номерам);	-	+	+
3	Реализовать идентификацию программ, томов, каталогов, файлов, записей, полей записей по именам;	-	+	+
4	Реализовать контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;	-	+	+
5	при наличии подключения ИСПДн к сетям общего пользования должно применяться межсетевое экранирование.	Не ниже 5-го уровня защищенности	Не ниже 4-го уровня защищенности	Не ниже 3-го уровня защищенности
6	Для обеспечения безопасного межсетевого взаимодействия в ИСПДн для разных классов необходимо использовать МЭ	Не ниже 5-го уровня защищенности	Не ниже 4-го уровня защищенности	Не ниже 3-го уровня защищенности
II	Средство защиты от программно математических воздействий (ПМВ):			
1	Реализовать идентификацию и аутентификацию субъектов доступа при входе в средство защиты от программно математических воздействий (ПМВ) и перед выполнением ими любых операций по управлению функциями средства защиты от ПМВ по паролю (или с использованием иного механизма аутентификации) условно-постоянного действия длиной не менее шести буквенно-цифровых символов;	+	+	+
2	Осуществлять контроль любых действий субъектов доступа по управлению функциями средства защиты от ПМВ только после проведения его успешной аутентификации;	+	+	+
3	Предусмотреть механизмы блокирования доступа к средствам защиты от ПМВ при выполнении устанавливаемого числа неудачных попыток ввода пароля;	+	+	+
4	Необходимо проводить идентификацию файлов, каталогов, программных модулей, внешних устройств, используемых средств защиты от ПМВ;	+	+	+
III	В подсистеме регистрации и учета:			
1	Осуществлять регистрацию входа (выхода) субъекта доступа в систему (из системы), либо регистрацию загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн. В параметрах регистрации указываются дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;	+	+	+
2	Проводить учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в журнал (учетную карточку);	+	+	+
3	Проводить регистрацию входа/выхода субъектов доступа в средство защиты от ПМВ, регистрацию загрузки и инициализации этого средства и ее программного останова. В параметрах регистрации указывается время и дата входа/выхода субъекта доступа в средство защиты от ПМВ или загрузки/останова этого средства, а также идентификатор субъекта доступа, инициировавшего данные действия;	+	+	+
4	Проводить регистрацию событий проверки и обнаружения ПМВ. В параметрах регистрации указываются время и дата проверки или обнаружения ПМВ, идентификатор субъекта доступа, инициировавшего данные действия, характер выполняемых действий по проверке, тип обнаруженной вредоносной программы (ВП), результат действий средства защиты по блокированию ПМВ;	+	+	+
5	Проводить регистрацию событий по внедрению в средство защиты от ПМВ пакетов обновлений. В параметрах регистрации указываются время и дата обновления, идентификатор субъекта доступа, инициировавшего данное действие версия и контрольная сумма пакета обновления;	+	+	+
6	Проводить регистрацию событий запуска/завершения работы модулей средства защиты от ПМВ. В параметрах регистрации указываются время и дата запуска/завершения работы, идентификатор модуля, идентификатор субъекта доступа, инициировавшего данное действие, результат запуска/завершения работы;	+	+	+
7	должна проводиться регистрация событий управления субъектом доступа функциями средства защиты от ПМВ. В параметрах регистрации указываются время и дата события управления каждой функцией, идентификатор и спецификация функции, идентификатор субъекта доступа, инициировавшего данное действие, результат действия;	+	+	+

8	Проводить регистрацию событий попыток доступа программных средств к модулям средства защиты от ПМВ или специальным ловушкам. В параметрах регистрации указываются время и дата попытки доступа, идентификатор модуля, идентификатор и спецификация модуля средства защиты от ПМВ (специальной ловушки), результат попытки доступа;	+	+	+
9	Проводить регистрацию событий отката для средства защиты от ПМВ. В параметрах регистрации указываются время и дата события отката, спецификация действий отката, идентификатор субъекта доступа, инициировавшего данное действие, результат действия;	+	+	+
10	Обеспечить защиту данных регистрации от их уничтожения или модификации нарушителем;	+	+	+
11	Реализовать механизмы сохранения данных регистрации в случае сокращения отведенных под них ресурсов;	+	+	+
12	Реализовать механизмы просмотра и анализа данных регистрации и их фильтрации по заданному набору параметров;	+	+	+
13	Проводить автоматический непрерывный мониторинг событий, которые могут являться причиной реализации ПМВ (создание, редактирование, запись, компиляция объектов, которые могут содержать ВП).	+	+	+
14	Реализовать механизм автоматического анализа данных регистрации по шаблонам типовых проявлений ПМВ с автоматическим их блокированием и уведомлением администратора безопасности;	+	+	+
15	Проводить несколько видов учета (дублирующих) с регистрацией выдачи (приема) носителей информации;	+	+	+
16	Осуществлять регистрацию входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы.	-	+	+
17	Осуществлять регистрацию выдачи печатных (графических) документов на «твердую» копию. В параметрах регистрации указываются (дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи – логическое имя (номер) внешнего устройства, краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа, идентификатор субъекта доступа, запросившего документ;	-	+	+
18	Осуществлять регистрацию запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный – несанкционированный),	-	+	+
19	Осуществлять регистрацию попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная – несанкционированная), идентификатор субъекта доступа, спецификация защищаемого файла;	-	+	+
20	Осуществлять регистрацию попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, компьютерам, узлам сети ИСПДн, линиям (каналам) связи, внешним устройствам компьютеров, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная – несанкционированная), идентификатор субъекта доступа, спецификация защищаемого объекта – логическое имя (номер);	-	+	+
21	Проводить учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);	-	+	+
22	Осуществлять очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти компьютеров и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов, информации);	-	+	+
IV	В подсистеме обеспечения целостности:			
1	Обеспечить целостность программных средств защиты в составе СЗПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗПДн, целостность программной среды обеспечивается отсутствием в ИСПДн средств разработки и отладки программ;	+	+	+
2	Осуществлять физическую охрану ИСПДн (устройств и носителей информации), предусматривающая контроль доступа в помещения ИСПДн посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации;	+	+	+
3	Проводить периодическое тестирование функций СЗПДн при изменении программной среды и персонала ИСПДн с помощью тест-программ, имитирующих попытки НСД;	+	+	+
4	должны быть в наличии средства восстановления СЗПДн, предусматривающие ведение двух копий программных средств	+	+	+

	защиты информации, их периодическое обновление и контроль работоспособности;			
5	Проводить проверку целостности модулей средства защиты от ПМВ, необходимых для его корректного функционирования, при его загрузке с использованием контрольных сумм;	+	+	+
6	Обеспечить возможность восстановления средства защиты от ПМВ, предусматривающая ведение двух копий программного средств защиты, его периодическое обновление и контроль работоспособности;	+	+	+
7	Реализовать механизмы проверки целостности пакетов обновлений средства защиты от ПМВ с использованием контрольных сумм;	+	+	+
8	Проводить резервное копирование ПДн на отчуждаемые носители информации;	-	+	+
V	В подсистеме антивирусной защиты:			
1	Проводить автоматическую проверку на наличие ВП или последствий ПМВ при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать ВП, по их типовым шаблонам и с помощью эвристического анализа;	+	+	+
2	Реализовать механизмы автоматического блокирования обнаруженных ВП путем их удаления из программных модулей или уничтожения;	+	+	+
3	Регулярно выполнять (при первом запуске средств защиты ПДн от ПМВ и с устанавливаемой периодичностью) проверка на предмет наличия в них ВП;	+	+	+
4	Должна инициироваться автоматическая проверка ИСПДн на предмет наличия ВП при выявлении факта ПМВ;	+	+	+
5	Реализовать механизм отката для устанавливаемого числа операций удаления ВП из оперативной или постоянной памяти, из программных модулей и прикладных программ или программных средств, содержащих ВП.	+	+	+
6	Дополнительно в ИСПДн должен проводиться непрерывный автоматический мониторинг информационного обмена с внешней сетью с целью выявления ВП.	+	+	+
VI	Контроль отсутствия НДВ в ПО СЗИ			
1	Для программного обеспечения, используемого при защите информации в ИСПДн (средств защиты информации – СЗИ, в том числе и встроенных в общесистемное и прикладное программное обеспечение – ПО), должен быть обеспечен соответствующий уровень контроля отсутствия в нем НДВ (не декларированных возможностей).	+	+	+
VII	Обнаружение вторжений в ИСПДн			
	Обнаружение вторжений должно обеспечиваться путем использования в составе ИСПДн программных или программно-аппаратных средств (систем) обнаружения вторжений (СОВ).	+	+	+
1	Необходимо обязательное использование системы обнаружения сетевых атак, использующие сигнатурные методы анализа	+	-	-
2	Необходимо обязательное использование системы обнаружения сетевых атак, использующие сигнатурные методы анализа и методы выявления аномалий	-	+	+
VIII	Защита ИСПДн от ПЭМИН			
1	Для обработки информации необходимо использовать СВТ, удовлетворяющие требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (например, ГОСТ 29216 91, ГОСТ Р 50948-2001, ГОСТ Р 50949-2001, ГОСТ Р 50923 96, СанПиН 2.2.2.542 96).	+	+	+
IX	Оценка соответствия ИСПДн требованиям безопасности ПДн			
1	Провести обязательную сертификацию (аттестацию) по требованиям безопасности информации;	-	+	+
2	Декларировать соответствие или обязательную сертификацию (аттестацию) по требованиям безопасности информации (по решению оператора);	+	-	-

Примечание: Для ИСПДн 4 класса перечень мероприятий по защите ПДн определяется в зависимости от ущерба который может быть нанесен в следствии несанкционированного или непреднамеренного доступа к ПДн.

Приложение № 3
Утверждено
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ПОЛОЖЕНИЕ
о разграничении прав доступа к персональным данным
Администрации Козловского муниципального округа Чувашской Республики

г. Козловка
2024 г.

Общие положения.

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» в рамках реализации мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах было разработано настоящее Положение. В данном документе представлен список лиц ответственных за обработку персональных данных в информационных системах персональных данных, список лиц, имеющих доступ к персональным данным в ИСПДн, а также их уровень прав доступа к обрабатываемым персональным данным.

Матрица доступа ИСПДн.

Перечень внутренних и внешних носителей, перефирийного оборудования, а также наличие программного обеспечения для работы с ИСПДн на АРМ Администрации Козловского муниципального округа Чувашской Республики (Администрации Козловского муниципального округа Чувашской Республики) приведены в Таблице 1.

Условные обозначения:
«+» – наличествует;
«-» – отсутствует;

1. Права доступа сотрудников к конкретным периферийным устройствам определяются администратором безопасности в соответствии с уровнем доступа конкретного сотрудника с учетом производственной необходимости в рабочем порядке.
2. Учет определяемых прав и вносимых в них изменений ведет администратор безопасности информационных систем персональных данных.
3. Перечень лиц, имеющих доступ к программным и техническим средствам ИСПДн, и их АРМ приведен в таблице 2.
4. Перечень лиц, участвующих в обработке персональных данных в ИСПДн представлен в таблице 3.

Таблица 1

АРМ (Имя компьютера)	Жесткий магнитный диск на АРМ	Внешний носитель			Периферийное оборудование	Администрация	Опека и попечительство	Имущественные и земельные отношения	ЗАГС
		DVD	Flash-накопители	FDD	Принтеры				
computer 1	+	+	+	-	+	+	-	-	-
computer 2	+	+	+	-	+	+	-	-	-
computer 3	+	+	+	-	+	+	-	-	-
computer 4	+	+	+	-	+	+	-	-	-
computer 5	+	+	+	-	+	+	-	-	-
computer 6	+	+	+	-	+	+	-	-	-
computer 7	+	+	+	-	+	-	-	+	-
computer 8	+	+	+	-	+	-	-	+	-
computer 9	+	+	+	-	+	-	-	+	-
computer 10	+	+	+	-	+	-	-	+	-
computer 11	+	+	+	-	+	-	-	+	-
computer 12	+	+	+	-	+	-	-	+	-
computer 13	+	+	+	-	+	+	-	-	-
computer 14	+	+	+	-	+	+	-	-	-
computer 15	+	+	+	-	+	+	-	-	-
computer 16	+	+	+	-	+	+	-	-	-
computer 17	+	+	+	-	+	+	-	-	-
computer 18	+	+	+	-	+	+	-	-	-
computer 19	+	+	+	-	+	+	-	-	-
computer 20	+	+	+	-	+	+	-	-	-
computer 21	+	+	+	-	+	+	-	-	-
computer 22	+	+	+	-	+	+	-	-	-
computer 23	+	+	+	-	+	+	-	-	-
computer 24	+	+	+	-	+	+	-	-	-
computer 25	+	+	+	-	+	+	-	-	-
computer 26	+	+	+	-	+	+	-	-	-
computer 27	+	+	+	-	+	+	-	-	-
computer 28	+	+	+	-	+	+	-	-	-
computer 29	+	+	+	-	+	+	-	-	-
computer 30	+	+	+	-	+	+	-	-	-
computer 31	+	+	+	-	+	+	-	-	-
computer 32	+	+	+	-	+	+	-	-	-
computer 33	+	+	+	-	+	+	-	-	-
computer 34	+	+	+	-	+	+	-	-	-
computer 35	+	+	+	-	+	+	-	-	-
computer 36	+	+	+	-	+	+	-	-	-
computer 37	+	+	+	-	+	+	-	-	-
computer 38	+	+	+	-	+	+	-	-	-
computer 39	+	+	+	-	+	+	-	-	-
computer 40	+	+	+	-	+	+	-	-	-
computer 41	+	+	+	-	+	+	-	-	-
computer 42	+	+	+	-	+	+	-	-	-
computer 43	+	+	+	-	+	+	-	-	-
computer 44	+	+	+	-	+	+	-	-	-
computer 45	+	+	+	-	+	+	-	-	-

АРМ (Имя компьютера)	Жесткий магнитный диск на АРМ	Внешний носитель			Периферийное оборудование	Администрация	Опека и попечительство	Имущественные и земельные отношения	ЗАГС
		DVD	Flash-накопители	FDD	Принтеры				
computer 46	+	+	+	-	+	+	-	-	-
computer 47	+	+	+	-	+	+	-	-	-
computer 48	+	+	+	-	+	+	-	-	-
computer 49	+	+	+	-	+	+	-	-	+
computer 50	+	+	+	-	+	+	-	-	+
computer 51	+	+	+	-	+	+	-	-	+
computer 52	+	+	+	-	+	+	-	-	-
computer 53	+	+	+	-	+	+	-	-	-
computer 54	+	+	+	-	+	-	-	-	+
computer 55	+	+	+	-	+	-	-	-	+
computer 56	+	+	+	-	+	-	+	-	-
computer 57	+	+	+	-	+	-	+	-	-
computer 58	+	+	+	-	+	+	-	-	-
computer 59	+	+	+	-	+	+	-	+	+
computer 60	+	+	+	-	+	+	-	+	+
computer 61	+	+	+	-	+	+	-	+	+
computer 62	+	+	+	-	+	+	-	-	-
computer 63	+	+	+	-	+	+	-	-	-
computer 64	+	+	+	-	+	+	-	-	-
computer 65	+	+	+	-	+	+	-	-	-
computer 66	+	+	+	-	+	+	-	-	-
computer 67	+	+	+	-	+	+	-	-	-
computer 68	+	+	+	-	+	+	-	-	-
computer 69	+	+	+	-	+	+	-	-	-
computer 70	+	+	+	-	+	+	-	-	-
computer 71	+	+	+	-	+	+	-	-	-
computer 72	+	+	+	-	+	+	-	-	-
computer 73	+	+	+	-	+	+	-	-	-
computer 74	+	+	+	-	+	+	-	-	-
computer 75	+	+	+	-	+	+	-	-	-
computer 76	+	+	+	-	+	+	-	-	-
computer 77	+	+	+	-	+	+	-	-	-
computer 78	+	+	+	-	+	+	-	-	-
computer 79	+	+	+	-	+	+	-	-	-
computer 80	+	+	+	-	+	+	-	-	-
computer 81	+	+	+	-	+	+	-	-	-
computer 82	+	+	+	-	+	+	-	-	-
computer 83	+	+	+	-	+	+	-	-	-
computer 84	+	+	+	-	+	+	-	-	-
computer 85	+	+	+	-	+	+	-	-	-
computer 86	+	+	+	-	+	+	-	-	-
computer 87	+	+	+	-	+	+	-	-	-
computer 88	+	+	+	-	+	+	-	-	-

Перечень лиц, имеющих доступ к программным и техническим средствам ИСПДн

Таблица 2.

№ п/п	ФИО	АРМ (имя компьютера)	Расположение
		computer 1	
		computer 2	
		computer 3	
		computer 4	
		computer 5	
		computer 6	
		computer 7	
		computer 8	
		computer 9	
		computer 10	
		computer 11	
		computer 12	
		computer 13	
		computer 14	
		computer 15	
		computer 16	
		computer 17	
		computer 18	
		computer 19	
		computer 20	
		computer 21	
		computer 22	
		computer 23	
		computer 24	
		computer 25	
		computer 26	
		computer 27	
		computer 28	
		computer 29	
		computer 30	
		computer 31	
		computer 32	
		computer 33	
		computer 34	
		computer 35	
		computer 36	
		computer 37	
		computer 38	
		computer 39	
		computer 40	
		computer 41	
		computer 42	
		computer 43	
		computer 44	
		computer 45	
		computer 46	
		computer 47	
		computer 48	
		computer 49	
		computer 50	
		computer 51	
		computer 52	
		computer 53	
		computer 54	
		computer 55	
		computer 56	
		computer 57	
		computer 58	
		computer 59	
		computer 60	
		computer 61	
		computer 62	
		computer 63	
		computer 64	
		computer 65	

№ п/п	ФИО	АРМ (имя компьютера)	Расположение
		computer 66	
		computer 67	
		computer 68	
		computer 69	
		computer 70	
		computer 71	
		computer 72	
		computer 73	
		computer 74	
		computer 75	
		computer 76	
		computer 77	
		computer 78	
		computer 79	
		computer 80	
		computer 81	
		computer 82	
		computer 83	
		computer 84	
		computer 85	
		computer 86	
		computer 87	
		computer 88	

Приложение № 4
Утверждена
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ИНСТРУКЦИЯ
ПО УЧЕТУ ОБРАЩЕНИЙ СОТРУДНИКОВ ДЛЯ ДОСТУПА К СВОИМ ПЕРСОНАЛЬНЫМ ДАННЫМ

г. Козловка
2024 г.

1. Настоящая инструкция разработана в соответствии с требованиями статьи 14 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», и определяет порядок учета обращений граждан для получения доступа к своим персональным данным в «Журнале учета обращений сотрудников для получения доступа к своим персональным данным».
2. Основанием для предоставления субъекту доступа к своим персональным данным является его обращение либо запрос субъекта персональных данных или его законного представителя. Запрос должен содержать:
1) номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя;
2) сведения о дате выдачи указанного документа и выдавшем его органе;
3) сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором
4) подпись субъекта персональных данных или его законного представителя.
Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.
3. Субъект персональных данных имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:
1) подтверждение факта обработки персональных данных оператором;
2) правовое основание и цели обработки персональных данных;
3) применяемые оператором способы обработки персональных данных;
4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
6) сроки обработки персональных данных, в том числе сроки их хранения;
7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;
8) информацию об осуществленной или предполагаемой трансграничной передаче данных;
9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
10) иные сведения, предусмотренные Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.
4. В случае, если вышеуказанные сведения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Администрацию Козловского муниципального округа Чувашской Республики или направить ему повторный запрос в целях получения данных сведений (см. п. 3 Инструкции), и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого является субъект персональных данных.
5. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения данных сведений (см. п. 3 Инструкции), а также в целях ознакомления с обрабатываемыми персональными данными до истечения тридцати дней, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос субъекта персональных данных наряду со сведениями, указанными в п. 2 Инструкции, должен содержать обоснование направления повторного запроса.
6. Выдача документов, содержащих персональные данные работников осуществляется в соответствии со ст. 62 Трудового кодекса РФ с соблюдением следующей процедуры:
- заявление сотрудника о выдаче того или иного документа на имя Главы Козловского муниципального округа Чувашской Республики;
- выдача заверенной копии (в количестве экземпляров, необходимом сотруднику) заявленного документа, либо справки о заявленном документе или сведениях, содержащихся в нем;
- внесения соответствующих записей в Журнал учета выданной информации.
7. Решение о предоставлении субъекту доступа (либо отказе в доступе) к персональным данным принимает ответственный за организацию обработки персональных в Администрации Козловского муниципального округа Чувашской Республики.
8. Все случаи предоставления субъекту доступа к персональным данным либо отказа от такого доступа регистрируются в «Журнале учета обращений субъектов ПДн (сотрудников) по вопросам обработки персональных данных и для получения доступа к своим персональным данным».
Инструкция разработана:
Начальник отдела правового обеспечения и цифрового развития администрации
Козловского муниципального округа Чувашской Республики _____ / _____

Приложение № 5
Утверждено
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

Техническое задание на создание системы защиты
для ИСПДн «Администрация», «Опека и попечительство», «Имущественные и земельные отношения»

г. Козловка
2024 г.

СПИСОК СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

АВС – антивирусные средства
АРМ – автоматизированное рабочее место
АС – автоматизированная система
АСЗИ – автоматизированная система в защищенном исполнении
ИСПДн – информационная система персональных данных
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
ОС – операционная система
ПДн – персональные данные
ПМВ – программно-математическое воздействие
ПО – программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
САЗ – система анализа защищенности
СЗИ – средства защиты информации
СЗПДн – система (подсистема) защиты персональных данных
СКЗИ – средства криптографической защиты информации
СОВ – система обнаружения вторжений
ТС – техническое средство
УБПДн – угрозы безопасности персональных данных

НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Настоящий документ составлен в соответствии со следующими действующими нормативно-методическими документами в области защиты персональных данных:
[1] – Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
[2] – Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
[3] – Постановление Правительства Российской Федерации об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных от 1 ноября 2012 г.№1119;
[4] –Приказ ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
[5] – Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 15 февраля 2008г. заместителем директора ФСТЭК России).

ОБОСНОВАНИЕ РАЗРАБОТКИ СИСТЕМЫ ЗАЩИТЫ

В информационных системах «Администрация», «Опека и попечительство», «Имущественные и земельные отношения» предполагается обработка персональных данных. Информационные системы «Администрация», «Опека и попечительство», «Имущественные и земельные отношения» попадают под действие закона [2]. В соответствии с [3] требуется обеспечить безопасность персональных данных. Безопасность персональных данных обеспечивается выполнением комплекса организационных и технических мер защиты, которые определяются в соответствии с нормативно-методическими документами ФСТЭК России и ФСБ России.
Система защиты должна разрабатываться с целью предотвращения ущерба от возможной реализации нарушений характеристик безопасности. Угрозы безопасности определены в «Модели угроз информационной систем» (далее Модель угроз).
Настоящий документ разработан для решения следующих задач:
– разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;
– создание регламента проведения мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
– недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
– создание регламента мероприятий, обеспечивающих контроль за обеспечением уровня защищенности персональных данных.

ИСХОДНЫЕ ДАННЫЕ

Описание информационных систем персональных данных «Администрация», «Опека и попечительство», «Имущественные и земельные отношения» приведено в Модели угроз.

Перечень требований безопасности персональных данных, предусмотренный нормативно-методическими документами для ИСПДн с заданными параметрами представлен в таблице.
Защита информации от выявленных угроз сводится к принятию организационных и технических мер, которые позволяют избавиться от тех или иных компонентов угроз.
В таблице представлен список требований, которые нужно выполнить для нейтрализации угроз данной ИСПДн.

№ п/п	Требование
1	**2**
1.	фильтрация на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов)
2.	идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия
3.	регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана)
4.	контроль целостности программной и информационной части межсетевого экрана
5.	фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств
6.	восстановление свойств межсетевого экрана после сбоев и отказов оборудования
7.	регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления
8.	использование средств антивирусной защиты
9.	использование в составе информационной системы программных или программно-аппаратных средств (систем) анализа защищенности. Средства (системы) анализа защищенности должны обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атаки на систему
10.	использование в составе информационной системы программных или программно-аппаратных средств (систем) обнаружения вторжений
11.	Для выбора и реализации методов и способов защиты информации в информационной системе оператором или уполномоченным лицом требуется назначить структурное подразделение или должностное лицо (работника), ответственные за обеспечение безопасности персональных данных
12.	обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними
13.	учет лиц, допущенных к работе с персональными данными в информационной системе; лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного оператором или уполномоченным лицом
14.	разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений
15.	регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы
16.	при регистрации входа (выхода) пользователя в систему (из системы) либо регистрации загрузки и инициализации операционной системы и ее программного останова в параметрах регистрации дополнительно указывается результат попытки входа (успешная или неуспешная)
17.	при регистрации входа (выхода) пользователя в систему (из системы) либо регистрации загрузки и инициализации операционной системы и ее программного останова в параметрах регистрации дополнительно указывается идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа
18.	учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме)
19.	размещение устройств вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы, в помещениях, в которых они установлены, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные
20.	идентификация и проверка подлинности пользователя при входе в систему информационной системы по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов
21.	при идентификации и проверке подлинности пользователя при входе в систему должен дополнительно использоваться идентификатор (код)
22.	физическая охрана информационной системы (технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации
23.	периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа
24.	наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности
25.	обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой

№ п/п	Требование
1	2
	информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по контрольным суммам компонентов средств защиты информации, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации
26.	физическая охрана технических средств информационных систем (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания

ПЕРЕЧЕНЬ ПРЕДЛАГАЕМЫХ К ИСПОЛЬЗОВАНИЮ СЕРТИФИЦИРОВАННЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

В данном разделе представлены средства защиты информации для реализации технических мер защиты. Специалисты оператора оставляют за собой право выбора тех или иных средств защиты, исходя из особенностей работы информационной системы.

№ п/п	Тип СЗИ	СЗИ	Описание СЗИ	Сертификат
1.	сертифицированные средства защиты информации от несанкционированного доступа	Блокхост-Сеть	Средство защиты информации от несанкционированного доступа; производитель: ООО «Газинформсервис»	ФСТЭК, №1517, от 30.11.2007
2.	сертифицированные средства защиты информации от несанкционированного доступа	Secret Net 5.1	Средство защиты информации от несанкционированного доступа; производитель: ООО «Код Безопасности»	ФСТЭК, №1912, от 17.09.2009
3.	сертифицированные средства защиты информации от несанкционированного доступа	Dallas Lock 7.5	Средство защиты информации от несанкционированного доступа; производитель ООО «Конфидент»	ФСТЭК, №1685, от 18.09.2008
4.	сертифицированные средства защиты информации от несанкционированного доступа	Страж NT 3.0	Средство защиты информации от несанкционированного доступа; производитель: ЗАО «НПЦ «Модуль»	ФСТЭК, №2145, от 30.07.2010
5.	сертифицированные средства защиты информации от несанкционированного доступа	Dr.Web Enterprise Security Suite	Средство защиты информации от несанкционированного доступа; производитель: «Доктор Веб»	ФСТЭК, №2446, от 20.09.2011
6.	сертифицированные средства защиты информации от несанкционированного доступа	Security Studio	Средство защиты информации от несанкционированного доступа; производитель: ООО «Код Безопасности»	ФСТЭК, №1597, от 24.04.2008

Допускается применение прочих сертифицированных средств защиты информации, если это требуется исходя из особенностей функционирования системы. Полный реестр сертифицированных средств защиты информации представлен на сайте ФСТЭК России.

Приложение № 6
Утверждена
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ИНСТРУКЦИЯ
АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ (ИСПДН)

г. Козловка
2024 г.

1. Общие положения

1.1. Администратор безопасности ИСПДн (далее Администратор) назначается распоряжением Администрации Козловского муниципального округа Чувашской Республики (далее Администрация).
1.2. Администратор подчиняется Главе Козловского муниципального округа Чувашской Республики.
1.3. Администратор в своей работе руководствуется настоящей инструкцией, Политикой информационной безопасности, а также другими руководящими и нормативными документами ФСТЭК России и регламентирующими документами Администрации.
1.4. Администратор отвечает за поддержание необходимого уровня безопасности объектов защиты.
1.5. Администратор является ответственным должностным лицом Администрации, уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ИСПДн и ее ресурсов на этапах промышленной эксплуатации и модернизации.
1.6. Администратор должен иметь специальное рабочее место, размещенное в здании Администрации так, чтобы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.
1.7. Рабочее место Администратора должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое), подключением к ИСПДн, а так же средствами контроля за техническими средствами защиты.
1.8. Администратор осуществляет методическое руководство Операторов и Администраторов ИСПДн, в вопросах обеспечения безопасности персональных данных.
1.9. Требования Администратора, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.
1.10. Администратор несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

2. Должностные обязанности

Администратор обязан:

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

2.2. Осуществлять установку, настройку и сопровождение технических средств защиты.

2.3. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.

2.4. Участвовать в приемке новых программных средств.

2.5. Обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.

2.6. Уточнять в установленном порядке обязанности пользователей ИСПДн по обработке объектов защиты.

2.7. Вести контроль над процессом осуществления резервного копирования объектов защиты.

2.8. Осуществлять контроль над выполнением Плана мероприятий по защите персональных данных.

2.9. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.

2.10. Контролировать неизменность состояния средств защиты их параметров и режимов защиты.

2.11. Контролировать физическую сохранность средств и оборудования ИСПДн.

2.12. Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а так же правильность работы с элементами ИСПДн и средствами защиты.

2.13. Контролировать исполнение пользователями парольной политики.

2.14. Контролировать работу пользователей в сетях общего пользования и (или) международного обмена.

2.15. Своевременно анализировать журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений.

2.16. Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.

2.17. Не допускать к работе на элементах ИСПДн посторонних лиц.

2.18. Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты ИСПДн.

2.19. Оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты.

2.20. Периодически представлять руководству отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации.

2.21. В случае отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.22. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

3. Права

Администратор ИСПДн имеет право:

3.1. Знакомиться с проектами распоряжений и постановлений Администрации Козловского муниципального округа Чувашской Республики, касающихся его деятельности.

3.2. Вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с предусмотренными настоящей инструкцией обязанностями.

3.3. В пределах своей компетенции сообщать своему непосредственному руководителю обо всех выявленных в процессе осуществления должностных обязанностей недостатках в деятельности организации (его структурных подразделениях) и вносить предложения по их устранению.

3.4. Запрашивать лично или по поручению своего непосредственного руководителя от специалистов подразделений информацию и документы, необходимые для выполнения его должностных обязанностей.

3.5. Привлекать специалистов всех (отдельных) структурных подразделений к решению задач, возложенных на него (если это предусмотрено положениями о структурных подразделениях, если нет — то с разрешения их руководителей).

3.6. Требовать от своего непосредственного руководителя оказания содействия в исполнении им своих должностных обязанностей и прав.

4. Ответственность

Администратор ИСПДн несет ответственность:

4.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией — в пределах, определенных действующим трудовым законодательством Российской Федерации.

4.2. За правонарушения, совершенные в процессе осуществления своей деятельности — в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

4.3. За причинение материального ущерба — в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

4.4. За разглашение конфиденциальной информации, содержащей персональные данные – в пределах, определенных действующим административным, уголовным, трудовым, и гражданским законодательством:

4.4.1. Администратор ИСПДн, получающий доступ к конфиденциальной информации, содержащей персональные данные, несет персональную ответственность за сохранность носителя и конфиденциальность информации.

С инструкцией ознакомлен (а) и обязуюсь хранить на рабочем месте

_____ _____«____» _____20__ г.

(фамилия, инициалы) (подпись)

Один экземпляр инструкции на руки получил

_____ _____«____» _____20__ г.

(фамилия, инициалы) (подпись)

Инструкция разработана:

Начальник отдела правового обеспечения и цифрового развития администрации

Козловского муниципального округа Чувашской Республики _____/_____

Приложение № 7
Утверждена
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ИНСТРУКЦИЯ
АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ (ИСПДН)
«АДМИНИСТРАЦИЯ»

г. Козловка
2024 г.

Общие положения

1.1. Администратор ИСПДн «Администрация» (далее Администратор) назначается распоряжением Администрации Козловского муниципального округа Чувашской Республики (далее Администрация).
1.2. Администратор подчиняется Главе Козловского муниципального округа Чувашской Республики.
1.3. Администратор в своей работе руководствуется настоящей инструкцией, Политикой информационной безопасности, а также другими руководящими и нормативными документами ФСТЭК России и регламентирующими документами Общества.
1.4. Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, при обработке персональных данных.
1.5. Методическое руководство работой Администратора осуществляется ответственным за обеспечение защиты персональных данных.

2. Должностные обязанности

Администратор обязан:
2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.
2.2. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:
программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное программное обеспечение);
аппаратных средств;
аппаратных и программных средств защиты.
2.3. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.
2.4. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.
2.5. Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.
2.6. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.
2.7. Проводить периодический контроль принятых мер по защите, в пределах возложенных на него функций.
2.8. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля Оператором ИСПДн.
2.9. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.
2.10. Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.
2.11. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.
2.12. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие специальные исследования и специальную проверку.
2.13. Присутствовать при выполнении технического обслуживания элементов ИСПДн, сторонними физическими людьми и организациями.
2.14. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

3. Права

Администратор имеет право:
3.1. Знакомиться с проектами распоряжений и постановлений Администрации Козловского муниципального округа Чувашской Республики, касающихся его деятельности.
3.2. Вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с предусмотренными настоящей инструкцией обязанностями.
3.3. В пределах своей компетенции сообщать своему непосредственному руководителю обо всех выявленных в процессе осуществления должностных обязанностей недостатках в деятельности организации (его структурных подразделениях) и вносить предложения по их устранению.
3.4. Запрашивать лично или по поручению своего непосредственного руководителя от специалистов подразделений информацию и документы, необходимые для выполнения его должностных обязанностей.
3.5. Привлекать специалистов всех (отдельных) структурных подразделений к решению задач, возложенных на него (если это предусмотрено положениями о структурных подразделениях, если нет — то с разрешения их руководителей).
3.6. Требовать от своего непосредственного руководителя оказания содействия в исполнении им своих должностных обязанностей и прав.

4. Ответственность

Администратор несет ответственность:
4.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией — в пределах, определенных действующим трудовым законодательством Российской Федерации.
4.2. За правонарушения, совершенные в процессе осуществления своей деятельности — в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.
4.3. За причинение материального ущерба — в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.
4.4. За разглашение конфиденциальной информации, содержащей персональные данные – в пределах, определенных действующим административным, уголовным, трудовым и гражданским законодательством РФ.
4.4.1. Администратор ИСПДн, получающий доступ к конфиденциальной информации, содержащей персональные данные, несет персональную ответственность за сохранность носителя и конфиденциальность информации.
С инструкцией ознакомлен (а) и обязуюсь хранить на рабочем месте

_____«____» _____20__ г.
(фамилия, инициалы)(подпись)

Один экземпляр инструкции на руки получил

_____«____» _____20__ г.
(фамилия, инициалы)(подпись)

Инструкция разработана:
Начальник отдела правового обеспечения
и цифрового развития администрации
Козловского муниципального округа
Чувашской Республики _____ /_____

Приложение № 8
Утверждена
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ИНСТРУКЦИЯ
АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ (ИСПДН) «ОПЕКА И ПОПЕЧИТЕЛЬСТВО»

г. Козловка
2024 г.

1. Общие положения

1.1. Администратор ИСПДн «Опека и попечительство» (далее Администратор) назначается распоряжением Администрации Козловского муниципального округа Чувашской Республики (далее Администрация).
1.2. Администратор подчиняется Главе Козловского муниципального округа Чувашской Республики.
1.3. Администратор в своей работе руководствуется настоящей инструкцией, Политикой информационной безопасности, а также другими руководящими и нормативными документами ФСТЭК России и регламентирующими документами Общества.
1.4. Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, при обработке персональных данных.
1.5. Методическое руководство работой Администратора осуществляется ответственным за обеспечение защиты персональных данных.

2. Должностные обязанности

Администратор обязан:
2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.
2.2. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:
программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное программное обеспечение);
аппаратных средств;
аппаратных и программных средств защиты.
2.3. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.
2.4. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.
2.5. Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.
2.6. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.
2.7. Проводить периодический контроль принятых мер по защиты, в пределах возложенных на него функций.
2.8. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля Оператором ИСПДн.
2.9. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

2.10. Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.
2.11. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.
2.12. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие специальные исследования и специальную проверку.
2.13. Присутствовать при выполнении технического обслуживания элементов ИСПДн, сторонними физическими людьми и организациями.
2.14. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

3. Права

Администратор имеет право:
3.1. Знакомиться с проектами распоряжений и постановлений Администрации Козловского муниципального округа Чувашской Республики, касающихся его деятельности.
3.2. Вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с предусмотренными настоящей инструкцией обязанностями.
3.3. В пределах своей компетенции сообщать своему непосредственному руководителю обо всех выявленных в процессе осуществления должностных обязанностей недостатках в деятельности организации (его структурных подразделениях) и вносить предложения по их устранению.
3.4. Запрашивать лично или по поручению своего непосредственного руководителя от специалистов подразделений информацию и документы, необходимые для выполнения его должностных обязанностей.
3.5. Привлекать специалистов всех (отдельных) структурных подразделений к решению задач, возложенных на него (если это предусмотрено положениями о структурных подразделениях, если нет — то с разрешения их руководителей).
3.6. Требовать от своего непосредственного руководителя оказания содействия в исполнении им своих должностных обязанностей и прав.

4. Ответственность

Администратор несет ответственность:
4.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией — в пределах, определенных действующим трудовым законодательством Российской Федерации.
4.2. За правонарушения, совершенные в процессе осуществления своей деятельности — в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.
4.3. За причинение материального ущерба — в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.
4.4. За разглашение конфиденциальной информации, содержащей персональные данные – в пределах, определенных действующим административным, уголовным, трудовым и гражданским законодательством РФ.
4.4.1. Администратор ИСПДн, получающий доступ к конфиденциальной информации, содержащей персональные данные, несет персональную ответственность за сохранность носителя и конфиденциальность информации.

С инструкцией ознакомлен (а) и обязуюсь хранить на рабочем месте

_____ _____«____» _____20__ г.
(фамилия, инициалы) (подпись)

Один экземпляр инструкции на руки получил

_____ _____«____» _____20__ г.
(фамилия, инициалы) (подпись)

Инструкция разработана:

Начальник отдела правового обеспечения
и цифрового развития администрации
Козловского муниципального округа
Чувашской Республики _____ / _____

Приложение № 9
Утверждена
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ИНСТРУКЦИЯ
ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ (ИСПДН)

г. Козловка
2024 г.

1. Общие положения

1.1. Пользователь ИСПДн (далее Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.
1.2. Пользователем является каждый сотрудник Администрации Козловского муниципального округа Чувашской Республики (далее Администрация), участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.
1.3. Пользователь несет персональную ответственность за свои действия.
1.4. Пользователь в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими документами Общества.
1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

2. Должностные обязанности

Пользователь обязан:
2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.
2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него.
2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных, а также руководящих и организационно-распорядительных документов.
2.4. Соблюдать требования парольной политики (раздел 3).
2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других (раздел 4).
2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).
2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью Администрации Козловского муниципального округа Чувашской Республики, а также для получений консультаций по вопросам информационной безопасности, необходимо обратиться к администратору безопасности ИСПДн.
2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к администратору ИСПДн.
2.9. Пользователям запрещается:
Разглашать защищаемую информацию третьим лицам.
Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.
Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.
Несанкционированно открывать общий доступ к папкам на своей рабочей станции.
Запрещено подключать к рабочей станции и локальной компьютерной сети Администрации Козловского муниципального округа Чувашской Республики личные внешние носители и мобильные устройства.
Отключать (блокировать) средства защиты информации.
Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн.
Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.
Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.
2.10. 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>
2.11. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций.

3.Организация парольной защиты

3.1 Личные пароли доступа к элементам ИСПДн выдаются пользователям администратором безопасности ИСПДн, администратором ИСПДн или создаются самостоятельно.
3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.
3.3. Правила формирования пароля:
Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.
Пароль должен состоять не менее чем из 6 символов.
В пароле должны присутствовать символы трех категорий из числа следующих четырех:
прописные буквы английского алфавита от A до Z;
строчные буквы английского алфавита от a до z;
десятичные цифры (от 0 до 9);
символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).
Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, 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.
3.4. Правила ввода пароля:
Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.
Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).
3.5. Правила хранение 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 регистрировать их в системе под своим паролем.
3.6. Лица, использующие паролирование, обязаны:
четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию.
своевременно сообщать администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4.Правила работы в сетях общего доступа и (или) международного обмена.

4.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.
4.2. При работе в Сети запрещается:
Осуществлять работу при отключенных средствах защиты (антивирус и других).
Передавать по Сети защищаемую информацию без использования средств шифрования.
Запрещается скачивать из Сети программное обеспечение и другие файлы.
Запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты содержащие нелегально распространяемое программное обеспечение и другие).
Запрещается нецелевое использование подключения к Сети.

5. Права

Пользователь ИСПДн имеет право:
5.1. Знакомиться с проектами распоряжений и постановлений Администрации Козловского муниципального округа Чувашской Республики касающихся его деятельности.
5.2. Вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с предусмотренными настоящей инструкцией обязанностями.
5.3. В пределах своей компетенции сообщать своему непосредственному руководителю о всех выявленных в процессе осуществления должностных обязанностей недостатках в деятельности организации (его структурных подразделениях) и вносить предложения по их устранению.
5.4. Запрашивать лично или по поручению своего непосредственного руководителя от специалистов подразделений информацию и документы, необходимые для выполнения его должностных обязанностей.
5.5. Привлекать специалистов всех (отдельных) структурных подразделений к решению задач, возложенных на него (если это предусмотрено положениями о структурных подразделениях, если нет — то с разрешения их руководителей).
5.6. Требовать от своего непосредственного руководителя оказания содействия в исполнении им своих должностных обязанностей и прав.

6. Ответственность

Пользователь ИСПДн несет ответственность:
6.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией — в пределах, определенных действующим трудовым законодательством Российской Федерации.
6.2. За правонарушения, совершенные в процессе осуществления своей деятельности — в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.
6.3. За причинение материального ущерба — в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.
6.4. За разглашение конфиденциальной информации, содержащей персональные данные – в пределах, определенных действующим административным, уголовным, трудовым и гражданским законодательством РФ.
6.4.1. Пользователь ИСПДн, получающий доступ к конфиденциальной информации, содержащей персональные данные, несет персональную ответственность за сохранность носителя и конфиденциальность информации.

Инструкция разработана:
Начальник отдела правового обеспечения
и цифрового развития администрации
Козловского муниципального округа
Чувашской Республики _____ / _____

Приложение № 10
Утверждено
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ПОЛОЖЕНИЕ О ПОСТОЯННО ДЕЙСТВУЮЩЕЙ ЭКСПЕРТНОЙ КОМИССИИ АДМИНИСТРАЦИИ КОЗЛОВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА ЧУВАШСКОЙ РЕСПУБЛИКИ

г. Козловка
2024 г.

1. Общие положения.

1.1. Постоянно действующая экспертная комиссия (ЭК) Администрации Козловского муниципального округа Чувашской Республики (далее Администрация) создается для организации и проведения методической и практической работы по экспертизе ценности документов, отбору и подготовке к передаче их на государственное хранение документов Архивного фонда ЧР, образующихся в процессе деятельности Администрации.

1.2. Постоянно действующая ЭК является совещательным органом при Главе Козловского муниципального округа Чувашской Республики. Решения комиссии вступают в силу после их утверждения Главой Козловского муниципального округа Чувашской Республики.

1.3. В своей работе ЭК руководствуется действующим законодательством Российской Федерации и Чувашской Республики об архивном деле, распоряжениями Администрации, Положением об ЭК Администрации, номенклатурой дел Администрации и иными нормативными документами со сроками хранения.

1.4. Экспертная комиссия возглавляется председателем ЭК, ее секретарем назначается, как правило, лицо, ответственное за архив Администрации.

1.5. Персональный состав ЭК назначается распоряжением Администрации из числа наиболее квалифицированных сотрудников ведущих структурных подразделений в количестве не менее 3 человек, представителя делопроизводственной службы. В состав ЭК в обязательном порядке включается лицо, ответственное за ведение архива.

1.6. В качестве экспертов к работе комиссии могут привлекаться представители любых сторонних организаций, в том числе специалисты госархива.

1.7. При выбытии одного из членов ЭК ее состав обновляется соответствующим распоряжением.

1.8. Настоящее Положение и изменения к нему утверждаются распоряжением Администрации.

1.5. Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно, до замены его новым Положением.

1.6. Настоящее Положение является обязательным для исполнения всеми членами комиссии Администрации. Все члены комиссии Администрации должны быть ознакомлены с настоящим Положением и изменениями к нему под роспись.

2. Основными задачами Комиссии являются:

2.1. Организация и проведение экспертизы ценности документов на стадии делопроизводства при составлении номенклатуры дел и формировании дел в Администрации.

2.2. Организация и проведение экспертизы ценности документов на стадии подготовки их к архивному хранению.

2.3. Организация и проведение отбора и подготовки документов к передаче на государственное хранение.

2.4. Организация и приведение документооборота Администрации в соответствии с актуальными требованиями законодательства о персональных данных.

3. Основные функции ЭК.

В соответствии с возложенными на нее задачами ЭК выполняет следующие функции:

3.1. Организует и проводит совместно с отделом организационно-контрольной и кадровой работы работу по ежегодному отбору документов Администрации для дальнейшего хранения и к уничтожению.

3.2. Осуществляет методическое руководство работой по экспертизе ценности документов Администрации и по подготовке их к архивному хранению, по разработке номенклатуры дел, дает экспертную оценку проектам нормативно-методических документов по названным вопросам.

3.3. Оказывает содействие и методическую помощь специалистам Администрации.

3.4. Рассматривает, принимает решения об одобрении и представляет:

3.4.1. На утверждение ЭК архивного учреждения, а затем на утверждение Главе Козловского муниципального округа Чувашской Республики:

- инструкцию по делопроизводству;
- номенклатуру дел;
- положение об архиве;
- положение об экспертной комиссии;
- описи дел постоянного хранения управленческой и специальной документации;
- перечни проектов, проблем (тем), научно-техническая документация по которым подлежит передаче на архивное хранение;
- акты о выделении к уничтожению документов с истекшими сроками хранения: документов со сроками хранения 10 лет и более, с отметкой "ЭК" в перечне.

3.4.2. На согласование ЭК архивного учреждения, а затем на утверждение Главе Козловского муниципального округа Чувашской Республики:

- сводную номенклатуру дел Администрации;
- описи дел по личному составу;
- акты об утрате или неисправимом повреждении документов постоянного хранения.

3.4.3. На рассмотрение ЭК архивного учреждения:

- предложения об изменении сроков хранения категорий документов, установленных перечнем, и об определении сроков хранения документов, не предусмотренных перечнем.

3.4.4. На утверждение Главе Козловского муниципального округа Чувашской Республики:

- акты о выделении к уничтожению документов с истекшими сроками хранения (кроме перечисленных в п. 3.4.1);
- акты об утрате или неисправимом повреждении документов по личному составу;
- акты ликвидации персональных данных.

3.5. Проводит для сотрудников Администрации консультации по вопросам работы с документами, участвует в проведении мероприятий по повышению их деловой квалификации.

4. Права ЭК.

Экспертная комиссия имеет право:

4.1. В пределах своей компетенции давать рекомендации структурным подразделениям и отдельным сотрудникам Администрации по вопросам разработки номенклатуры дел и формирования дел в делопроизводстве, экспертизы ценности документов, розыска недостающих дел постоянного срока хранения и дел по личному составу, упорядочения и оформления документов.

4.2. Запрашивать от руководителей структурных подразделений и отдельных сотрудников Администрации:

- письменные объяснения о причинах утраты, порчи или незаконного уничтожения документов постоянного и долговременного сроков хранения, в том числе документов по личному составу;
- предложения и заключения, необходимые для определения сроков хранения документов.
4.3. Заслушивать на своих заседаниях руководителей структурных подразделений и отдельных сотрудников Администрации о ходе подготовки документов к архивному хранению, об условиях хранения и обеспечения сохранности документов, о причинах утраты документов.
4.4. Приглашать на заседания комиссии в качестве консультантов и экспертов специалистов структурных подразделений, отдельных сотрудников Администрации, представителей учреждений Государственной архивной службы России, сторонних организаций.
4.5. ЭК в лице ее председателя имеет право не принимать к рассмотрению и возвращать для доработки некачественно и небрежно подготовленные документы.
4.6. Информировать руководство Администрации по вопросам, относящимся к компетенции комиссии.
4.7. В установленном порядке представлять свое учреждение в органах Государственной архивной службы России.

5. Организация работы ЭК.

5.1. ЭК работает по годовому плану, утвержденному Главой Козловского муниципального округа Чувашской Республики.
5.2. Вопросы, относящиеся к компетенции ЭК, рассматриваются на ее заседаниях, которые проводятся по мере необходимости, но не реже 2 раз в год. Все заседания комиссии протоколируются. Поступающие на рассмотрение ЭК документы рассматриваются на ее заседании не позднее чем через 10 дней.
5.3. Заседание ЭК и принятые на нем решения считаются правомочными, если в голосовании приняли участие не менее половины присутствующих на заседании членов ЭК. Право решающего голоса имеют только члены ЭК. Приглашенные консультанты и эксперты имеют право совещательного голоса, в голосовании не участвуют.
5.4. Решение принимается простым большинством голосов присутствующих на заседании членов. При разделении голосов поровну решение принимает председатель ЭК и руководство Администрации.
5.5. Ведение делопроизводства ЭК, хранение и использование ее документов, ответственность за их сохранность, а также контроль за исполнением принятых ЭК решений возлагаются на секретаря комиссии.

Положение разработано:

Начальник отдела правового обеспечения
и цифрового развития администрации
Козловского муниципального округа
Чувашской Республики _____ / _____

Приложение № 11
Утвержден
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ПОРЯДОК
ДОСТУПА РАБОТНИКОВ АДМИНИСТРАЦИИ КОЗЛОВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА ЧУВАШСКОЙ РЕСПУБЛИКИ В ПОМЕЩЕНИЯ, В КОТОРЫХ ВЕДЕТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

г. Козловка
2024 г.

1. Персональные данные относятся к категории конфиденциальной информации. Лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.
2. Перечень должностей работников Администрации Козловского муниципального округа Чувашской Республики (далее – Администрация), замещение которых, предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, утверждается распоряжением Администрации Козловского муниципального округа Чувашской Республики.
3. Порядок определяет правила доступа в помещения, где хранятся и обрабатываются персональные данные, в целях исключения несанкционированного доступа к персональным данным, а также обеспечения безопасности персональных данных от уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении персональных данных.
4. Помещения, в которых ведется обработка персональных данных, должны обеспечивать сохранность информации и технических средств, исключать возможность бесконтрольного проникновения в помещение и их визуального просмотра посторонними лицами.
5. Работники, имеющие доступ к персональным данным, не должны:
оставлять в свое отсутствие незапертым помещение, в котором размещены технические средства, позволяющие осуществлять обработку персональных данных;
оставлять в помещении посторонних лиц, не имеющих доступа к персональным данным в данном структурном подразделении, без присмотра.
6. Для помещений, в которых хранятся и обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей информации, содержащей персональные данные, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц. Указанный режим обеспечивается в том числе:
оснащением помещения сигнализацией в соответствии с законодательством;
обязательным запиранием помещения на ключ при выходе из него даже в рабочее время;
закрытием металлических шкафов и сейфов, где хранятся носители информации, содержащие персональные данные.

7. Доступ в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся материальные носители персональных данных (далее - помещения), в случае возникновения непредвиденных обстоятельств в нерабочее время осуществляется работником охранной организации, осуществляющей охрану здания, в котором располагаются помещения, с записью в журнале вскрытия.
8. Ответственность за соблюдение настоящего Порядка возлагается на руководителей структурных подразделений Администрации, в которых ведется обработка персональных данных и осуществляется их хранение.
9. Внутренний контроль за соблюдением порядка доступа в помещения, в которых ведется обработка персональных данных, осуществляется лицом, ответственным за организацию обработки персональных данных, или комиссией, образуемой в соответствии с распоряжением Администрации.
Документ разработан:

Начальник отдела правового обеспечения
и цифрового развития администрации
Козловского муниципального округа
Чувашской Республики _____ / _____

Приложение № 12
Утверждены
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ПРАВИЛА
РАССМОТРЕНИЯ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ
ИЛИ ИХ ПРЕДСТАВИТЕЛЕЙ В АДМИНИСТРАЦИИ КОЗЛОВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА
ЧУВАШСКОЙ РЕСПУБЛИКИ

г. Козловка
2024 г.

1. Субъект персональных данных или его представитель имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:
1) подтверждение факта обработки персональных данных;
2) правовые основания и цели обработки персональных данных;
3) применяемые способы обработки персональных данных;
4) наименование и место нахождения Администрации Козловского муниципального округа Чувашской Республики (далее - Администрация), сведения о гражданах (за исключением работников Администрации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Администрацией или на основании законодательства Российской Федерации;
5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен законодательством Российской Федерации;
6) сроки обработки персональных данных, в том числе сроки их хранения;
7) порядок осуществления субъектом персональных данных прав, предусмотренных законодательством Российской Федерации в области персональных данных;
8) сведения об осуществленной или о предполагаемой трансграничной передаче персональных данных;
9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Администрации, если обработка поручена или будет поручена такой организации или лицу;
10) иные сведения, предусмотренные Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных" или другими федеральными законами.
2. Субъект персональных данных вправе требовать от Администрации уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.
3. Сведения предоставляются субъекту персональных данных Администрацией в доступной форме без содержания персональных данных, относящихся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.
4. Сведения предоставляются субъекту персональных данных или его представителю Администрацией при обращении либо при получении запроса субъекта персональных данных или его представителя.
Запрос должен содержать:
1) номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;
2) сведения, подтверждающие участие субъекта персональных данных в отношениях с Администрацией (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Администрацией, подпись субъекта персональных данных или его представителя.
Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.
5. В случае если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Администрацию или направить повторный запрос в целях ознакомления с такими персональными данными не ранее чем через 30 календарных дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

6. Субъект персональных данных вправе обратиться повторно в Администрацию или направить повторный запрос в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 5 настоящих Правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 4 настоящих Правил, должен содержать обоснование направления повторного запроса.
7. Администрация вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 5 и 6 настоящих Правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса возлагается на Администрацию.
8. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона "О персональных данных".

Документ разработан:
Начальник отдела правового обеспечения и цифрового развития администрации
Козловского муниципального округа Чувашской Республики _____ / _____

Приложение № 13
Утверждены
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ПРАВИЛА
РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ В АДМИНИСТРАЦИИ КОЗЛОВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА ЧУВАШСКОЙ РЕСПУБЛИКИ

г. Козловка
2024 г.

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила работы с обезличенными персональными данными в Администрации Козловского муниципального округа Чувашской Республики (далее - Правила) разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
1.2. Настоящие Правила определяют порядок работы с обезличенными данными Администрации Козловского муниципального округа Чувашской Республики (далее – Администрация).

II. УСЛОВИЯ ОБЕЗЛИЧИВАНИЯ

2.1. Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.
2.2. Обезличивание персональных данных может быть проведено с целью
проведения статистического анализа, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных Администрации и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации.
2.3. Обезличивание персональных данных осуществляется в соответствии с **приказом** Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. N 996 "Об утверждении требований и методов по обезличиванию персональных данных"
2.4. Способы обезличивания при условии дальнейшей обработки персональных данных:
- уменьшение перечня обрабатываемых сведений,
- замена части сведений идентификаторами,
- обобщение - понижение точности некоторых сведений,
- понижение точности некоторых сведений,
- деление сведений на части и обработка в разных информационных системах,
- другие способы.
2.5. Методы обезличивания персональных данных:
1) метод введения идентификаторов - замена части значений персональных данных (далее - сведения) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным;
2) метод изменения состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений (понижение точности некоторых сведений). Например, данные о месте жительства могут включать страну, индекс, город, улицу, номер дома и квартиры, а может быть указан только город;
3) метод декомпозиции - деление сведений на части с последующим раздельным хранением и обработкой в разных информационных системах;
4) метод перемешивания (перестановка отдельных записей, а также групп записей в массиве персональных данных).
2.6. Решение о необходимости обезличивания персональных данных принимает Глава Козловского муниципального округа Чувашской Республики.
2.7. Руководители структурных подразделений готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания.
2.8. Сотрудники структурных подразделений, обслуживающих базы данных с персональными данными, совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом.
2.9. Обезличенные персональные данные не подлежат разглашению и нарушению их конфиденциальности.
2.10. Обезличенные персональные данные обрабатываются с использованием и без использования средств автоматизации.
2.11. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

1) парольной политики, регламентирующей требования к сложности и частоте изменения паролей, к действиям пользователей при работе с паролями;
2) антивирусной политики, устанавливающей требования к пользователям и администраторам по настройке и использованию средств антивирусной защиты;
3) правил работы со съемными носителями в порядке, определенном законодательством (если они используются);
4) правил резервного копирования;
5) правил доступа в помещения, где расположены элементы информационных систем.
2.12. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:
1) правил хранения бумажных носителей;
2) правил доступа к бумажным носителям и в помещения, где они хранятся

Документ разработан:

Заведующий сектором
цифрового развития и информационных технологий
администрации Козловского муниципального округа
Чувашской Республики _____/ _____

Приложение № 14
Утверждены
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ПРАВИЛА
ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, УСТАНОВЛЕННЫМ ФЕДЕРАЛЬНЫМ ЗАКОНОМ «О ПЕРСОНАЛЬНЫХ ДАННЫХ», В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ АДМИНИСТРАЦИИ КОЗЛОВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА ЧУВАШСКОЙ РЕСПУБЛИКИ

г. Козловка
2024 г.

1. Внутренний контроль соответствия обработки персональных данных требованиям Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, правовым актам Администрации (далее - внутренний контроль) организуется в форме периодических проверок (далее - проверки).
2. Целью внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в информационных системах персональных данных (далее — ИСПДн) Администрации Козловского муниципального округа Чувашской Республики (далее – Администрации) является предотвращение и своевременное выявление несанкционированного доступа к информации, преднамеренных воздействий на информацию, оценка эффективности ее защиты.
3. Организация и проведение контроля возлагаются на администратора безопасности ИСПДн Администрации или на комиссию по организации работ по защите персональных данных (далее - комиссия), создаваемой на время проведения проверок, распоряжением Главы Козловского муниципального округа Чувашской Республики.
4. В проведении проверки не может участвовать лицо, прямо или косвенно заинтересованное в ее результатах.
5. Проверки проводятся на основании утверждаемого Главой Козловского муниципального округа Чувашской Республики ежегодного плана осуществления внутреннего контроля (плановые проверки) режима защиты персональных данных в информационных системах персональных данных Администрации или на основании поступившего в Администрацию письменного заявления субъекта персональных данных или его представителя о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.
План осуществления внутреннего контроля в себя включает перечень направлений и (или) мероприятий проверки, периодичность и (или) сроки их проведения, перечисление ответственных лиц за проведение проверки, перечень структурных подразделений и лиц, проверяемых в ходе проверки, примечания.
6. При проведении проверки должны быть полностью, объективно и всесторонне определены:
1) порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
2) порядок и условия применения средств защиты информации;
3) эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
4) состояние учета машинных носителей персональных данных;
5) соблюдение правил доступа к персональным данным;
6) наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
7) мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
8) мероприятия по обеспечению целостности персональных данных.
7. Должностное лицо, ответственное за организацию обработки персональных данных (комиссия), имеет право:
1) запрашивать у работников Администрации информацию, необходимую для исполнения своих обязанностей;
2) требовать от уполномоченных на обработку персональных данных уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

3) принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации в области персональных данных;
4) представлять Главе Козловского муниципального округа Чувашской Республики предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
5) представлять Главе Козловского муниципального округа Чувашской Республики предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в области персональных данных.
8. В отношении персональных данных, ставших известными должностному лицу, ответственному за организацию обработки персональных данных (комиссии) в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.
9. Проверка должна быть завершена не позднее чем через десять рабочих дней со дня принятия решения о ее проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, Главе Козловского муниципального округа Чувашской Республики докладывает должностное лицо, ответственное за организацию обработки персональных данных, в форме служебной записки либо председатель комиссии в форме письменного заключения в случае проведения проверки комиссией.

Документ разработан:
Начальник отдела правового обеспечения
и цифрового развития администрации
Козловского муниципального округа
Чувашской Республики _____ / _____

Приложение № 15
Утверждена
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ИНСТРУКЦИЯ
ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В АДМИНИСТРАЦИИ КОЗЛОВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА ЧУВАШСКОЙ РЕСПУБЛИКИ

г. Козловка
2024 г.

I. Общие положения

1.1. Настоящий документ регламентирует порядок работы ответственного за обработку персональных данных (далее — Ответственное лицо) в Администрации Козловского муниципального округа Чувашской Республики (далее – Администрация), который назначается распоряжением Администрации в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Приказом ФСТЭК России от 5 февраля 2010 г. и Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правыми актами, операторами, являющимися государственными или муниципальными органами».

II. Обязанности Ответственного лица

2.1. Ответственное лицо:
2.1.1. Доводит до сведения сотрудников Администрации содержание положений законодательства Российской Федерации о персональных данных, распорядительных документов Администрации по вопросам обработки персональных данных, требований к защите персональных данных.
2.1.2. Проводит мероприятия по осуществлению внутреннего контроля за соблюдением сотрудниками Администрации законодательства Российской Федерации о персональных данных, распорядительных документов Администрации по вопросам обработки персональных данных, требований к защите персональных данных.
2.1.3. Организовывает прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществляет контроль за приемом и обработкой таких обращений и запросов.
2.1.4. Готовит распорядительные документы по вопросам обработки персональных данных, а также устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, а также определяющие политику Администрации в отношении обработки персональных данных.

III. Порядок обеспечения безопасности при обработке персональных данных

3.1. Ответственное лицо принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.
3.2. Обеспечение безопасности персональных данных достигается, в частности:
3.2.1. Определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
3.2.2. Применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований
к защите персональных данных.
3.2.3. Применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.
3.2.4. Оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.
3.2.5. Обнаружением фактов несанкционированного доступа к персональным данным и принятием мер.

3.2.6. Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
3.2.7. Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.
3.2.8. Контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.
3.3. При выявлении нарушений безопасности обработки персональных данных Ответственное лицо докладывает о выявленных нарушениях Главе Козловского муниципального округа Чувашской Республики, организует расследование в соответствии с распорядительными документами Администрации и принимает меры по их устранению.

Инструкция разработана:

Начальник отдела правового обеспечения
и цифрового развития администрации
Козловского муниципального округа
Чувашской Республики _____ / _____

Приложение № 16
Утверждена
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ РЕЗЕРВНОГО КОПИРОВАНИЯ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ И ДРУГОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В АДМИНИСТРАЦИИ КОЗЛОВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА ЧУВАШСКОЙ РЕСПУБЛИКИ

г. Козловка
2024 г.

Руководители структурных подразделений, сотрудники Администрации Козловского муниципального округа Чувашской Республики, действующие в рамках своих функциональных обязанностей и имеющие доступ к аппаратным средствам, программным средствам, программному обеспечению и информационной системе персональных данных несут персональную ответственность за свои действия и обязаны:

1. Создавать не реже одного раза в неделю резервную копию баз данных ИСПДн «Администрация» средствами программного комплекса.

2. Создавать не реже одного раза в месяц резервную копию баз данных прочих ИСПДн Администрации Козловского муниципального округа Чувашской Республики.

3. Копирование данных осуществлять на учетный носитель информации, который хранить в сейфе (металлическом шкафу).

Инструкция разработана:
Начальник отдела правового обеспечения
и цифрового развития администрации
Козловского муниципального округа
Чувашской Республики _____ / _____

Приложение № 17
Утвержден
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

АКТ
РЕЗУЛЬТАТЫ ОПРОСА О ЧАСТОТЕ (ВЕРОЯТНОСТИ) РЕАЛИЗАЦИИ УГРОЗЫ И ОПАСНОСТИ УГРОЗЫ ПО ВИДАМ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИСПДН

В соответствии с требованиями Постановления Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и методическим рекомендациями Управления ФСТЭК России по ПФО по разработке частных моделей угроз безопасности персональных данных, комиссией, назначенной распоряжением Администрации Козловского муниципального округа Чувашской Республики № 28-р от 20 декабря 2024 г. в составе:

Председатель комиссии:
Маркова Анна Александровна Начальник отдела правового обеспечения и цифрового развития администрации

Козловского муниципального округа Чувашской Республики

Члены комиссии:

Васильева Татьяна Леонидовна	Управляющий делами МО - начальник отдела организационно-контрольной и кадровой работы администрации Козловского муниципального округа Чувашской Республики
Пушков Геннадий Михайлович	Заместитель главы администрации МО по экономике и сельскому хозяйству - начальник отдела экономики, инвестиционной деятельности, земельных и имущественных отношений администрации Козловского муниципального округа Чувашской Республики
Комарова Валерия Игоревна	Заведующий сектором опеки и попечительства администрации Козловского муниципального округа Чувашской Республики
Ульданова Анастасия Витальевна	Начальник отдела ЗАГС администрации Козловского муниципального округа Чувашской Республики

Проведено изучение вероятности реализации угроз и опасности угроз по видам угроз безопасности персональных данных при их обработке в информационных системах персональных данных Администрации Козловского муниципального округа Чувашской Республики (далее − ИСПДн). Результаты по видам угроз безопасности персональных данных (далее − ПДн) отображены в Таблице 1.

Таблица 1.

Вид угрозы	Опасность (ущерб)	Вероятность	Комментарии
УГРОЗЫ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ			
Угрозы утечки акустической (речевой) информации			
Непосредственное прослушивание ПДн акустической речевой информации физическими лицами при посещении ими служебных помещений	Низкая	Маловероятно	Функций голосового ввода персональных данных и функций воспроизведения персональных данных акустическими средствами в данной ИСПДн нет
Перехват акустических сигналов с использованием направленных микрофонов (дальность перехвата до 200 м)	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за сложности ее реализации и высокой стоимости необходимой техники
Перехват акустических сигналов с использованием ненаправленных микрофонов (дальность перехвата до 10 м)	Низкая	Маловероятно	
Перехват акустических сигналов с использованием акустооптических модуляторов (оптические микрофоны, дальность перехвата - в поле акустического сигнала)	Низкая	Маловероятно	
Перехват вибрационных сигналов с использованием оптико-электронной аппаратуры дистанционного лазерного зондирования (лазерные микрофоны, дальность перехвата до 500 м)	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за сложности ее реализации и высокой стоимости необходимой техники
Перехват вибрационных сигналов с использованием вибродатчиков (контактные микрофоны, дальность перехвата до 10 м)	Низкая	Маловероятно	
Перехват электрических сигналов, возникающих в результате «микрофонного эффекта» в технических средствах обработки ПДн и ВТСС с использованием средств съема электрических сигналов с гальваническим подключением (дальность перехвата до 300 м)	Низкая	Маловероятно	
Перехват радиоизлучений, модулированных информативным сигналом, возникающих при ВЧ-облучении технических средств обработки ПДн и ВТСС с использованием ВЧ-генераторов и средств съема электрических сигналов с гальваническим подключением (ВЧ-навязывание, дальность перехвата до 300 м)	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за сложности ее реализации и высокой стоимости необходимой техники
Перехват радиоизлучений, модулированных информативным сигналом, возникающих при ВЧ-облучении технических средств обработки ПДн и ВТСС с использованием ВЧ-генераторов и приемников электромагнитного излучения (ВЧ-облучение, до 1000 м)	Низкая	Маловероятно	
Угрозы утечки видовой информации			
Непосредственный просмотр ПДн с экранов дисплеев и других средств отображения графической, видео- и буквенно-цифровой информации физическими лицами при посещении ими служебных помещений	Низкая	Высокая вероятность	Помещения, где расположена ИСПДн, могут посещаются сотрудниками, не допущенными к ИСПДн

Вид угрозы	Опасность (ущерб)	Вероятность	Комментарии
Просмотр (регистрация) ПДн с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации на расстоянии прямой видимости из-за пределов служебных помещений с использованием оптических (оптикоэлектронных) средств	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за сложности ее реализации и высокой стоимости необходимой техники
Просмотр (регистрация) ПДн с помощью специальных электронных устройств съема, внедренных в служебных помещениях (видеозакладки) или скрытно используемых физическими лицами при посещении ими служебных помещений	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за сложности ее реализации и высокой стоимости необходимой техники
Угрозы утечки информации по каналу ПЭМИН			
Перехват ПДн техническими средствами побочных электромагнитных излучений информативных сигналов от технических средств и линий передачи информации с использованием портативных сканерных приемников, цифровых анализаторов спектра, селективных микровольтметров и специальных программно-аппаратных комплексов (дальность перехвата до 1000 м)	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за сложности ее реализации и высокой стоимости необходимой техники
Перехват ПДн техническими средствами наводок информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы служебных помещений с использованием токосъемников (дальность перехвата до 300 м)	Низкая	Маловероятно	
Перехват ПДн техническими средствами радиоизлучений, модулированных информативным сигналом, возникающих в результате работы различных генераторов в составе ИСПДн или в результате паразитной генерации в узлах (элементах) технических средств с использованием портативных сканерных приемников, цифровых анализаторов спектра, селективных микровольтметров и специальных программно-аппаратных комплексов (дальность перехвата до 1000 м)	Низкая	Маловероятно	
Перехват ПДн техническими средствами радиоизлучений, формируемых за счет высокочастотного облучения технических средств ИСПДн с использованием портативных сканерных приемников, цифровых анализаторов	Низкая	Маловероятно	
спектра, селективных микровольтметров и специальных программно-аппаратных комплексов (дальность перехвата до 1000 м)	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за сложности ее реализации и высокой стоимости необходимой техники
Перехват ПДн техническими средствами оптического излучения с боковой поверхности оптического волокна в волоконно-оптической системе передачи данных	Низкая	Маловероятно	
Перехват ПДн с применением электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПДн («аппаратурные закладки»)	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за сложности ее реализации и высокой стоимости необходимой техники
УГРОЗЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ			
Угрозы непосредственного доступа			
Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой			
Получение несанкционированного доступа к настройкам конфигурации компьютера (BIOS):			
- в связи с отсутствием аутентификации пользователей компьютеров до загрузки ОС (паролей BIOS или дополнительных аппаратных средств аутентификации);	Средняя	Средняя	Необходима установка паролей на BIOS АРМ ИСПДн
- в связи с неумышленным разглашением паролей BIOS или дополнительных аппаратных средств аутентификации (записывание в доступном для нарушителя месте: на бумаге, клавиатуре и т.п.);	Низкая	Низкая	Необходима установка паролей на BIOS АРМ ИСПДн. Регулируется организационными мерами (Инструкция администратора)

Вид угрозы	Опасность (ущерб)	Вероятность	Комментарии
- путем подбора пароля BIOS (или дополнительных аппаратных средств аутентификации);	Низкая	Низкая	Необходима установка паролей на BIOS АРМ ИСПДн. Применение пароля условно-постоянного действия длиной не менее 6 буквенно-цифровых символов
- путем вскрытия корпуса компьютера и аппаратного сброса пароля BIOS;	Низкая	Низкая	Опечатывание корпуса, применение технических средств защиты от несанкционированного вскрытия системного блока
- путем использования технологического пароля BIOS;	Низкая	Низкая	Установка специализированного ПО от производителя BIOS для смены технологического пароля, обновление версии BIOS
- путем внедрения аппаратного "клавиатурного шпиона"	Низкая	Низкая	Установка программных средств виртуальной клавиатуры, либо вскрытие клавиатуры и ее проверка на предмет наличия посторонних электронных узлов с последующим пломбированием корпуса клавиатуры при помощи пломбира или стикера, проверка на наличие посторонних устройств, включенных в разрыв кабеля клавиатуры, расположенных рядом с ним или непосредственно на нем.
Загрузка сторонней ОС с внешнего носителя (для обхода средств защиты и разграничения доступа к ресурсам компьютера, реализованного на уровне ОС)	Средняя	Средняя	Необходимо установить запрет загрузки с внешних носителей в BIOS
Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы, с применением специальных программ для осуществления НСД			
Предоставление пользователям прав доступа (в том числе по видам доступа) к ПДн и другим ресурсам ИСПДн сверх необходимого для работы	Низкая	Низкая	Пользователи ИСПДн официально предупреждены о необходимости соблюдения конфиденциальности ПДн и об ответственности за допущенные нарушения
Неумышленное (случайное) копирование доступных ПДн на неучтённые (в том числе отчуждаемые) носители, в том числе печать неучтённых копий документов с ПДн	Низкая	Низкая	Пользователи ИСПДн официально предупреждены о необходимости соблюдения конфиденциальности ПДн и об ответственности за допущенные нарушения. Необходимо вести учет носителей ПДн.
Преднамеренное копирование доступных ПДн на неучтённые (в том числе отчуждаемые) носители в том числе печать неучтённых копий документов с ПДн на принтерах	Низкая	Низкая	Регулируется организационными мерами (Положение о защите персональных данных). Необходимо вести учет носителей ПДн.
Неумышленная (случайная) отправка ПДн по электронной почте	Низкая	Низкая	Пользователи ИСПДн официально предупреждены о необходимости соблюдения конфиденциальности ПДн и об ответственности за допущенные нарушения.
Преднамеренная отправка ПДн по электронной почте	Низкая	Низкая	Пользователи ИСПДн официально предупреждены о необходимости соблюдения конфиденциальности ПДн и об ответственности за допущенные нарушения.
Неумышленная (случайная) модификация (искажение) доступных ПДн	Средняя	Средняя	Необходимо осуществлять резервное копирование базы данных ИСПДн на отчуждаемый носитель
Преднамеренная модификация (искажение) доступных ПДн	Средняя	Средняя	Пользователи ИСПДн официально предупреждены о необходимости соблюдения конфиденциальности ПДн и об ответственности за допущенные нарушения. Необходимо осуществлять резервное копирование базы данных ИСПДн
Неумышленное (случайное) добавление (фальсификация) ПДн	Средняя	Средняя	Необходимо осуществлять резервное копирование базы данных ИСПДн на отчуждаемый носитель

Вид угрозы	Опасность (ущерб)	Вероятность	Комментарии
Преднамеренное добавление (фальсификация) ПДн	Средняя	Средняя	Пользователи ИСПДн официально предупреждены о необходимости соблюдения конфиденциальности ПДн и об ответственности за допущенные нарушения. Необходимо осуществлять резервное копирование базы данных ИСПДн на отчуждаемый носитель
Неумышленное (случайное) уничтожение доступных ПДн (записей, файлов, форматирование диска)	Средняя	Средняя	Необходимо осуществлять резервное копирование базы данных ИСПДн на отчуждаемый носитель
Преднамеренное уничтожение доступных ПДн (записей, файлов, форматирование диска)	Низкая	Низкая	Пользователи ИСПДн официально предупреждены о необходимости соблюдения конфиденциальности ПДн и об ответственности за допущенные нарушения. Необходимо осуществлять резервное копирование базы данных ИСПДн на отчуждаемый носитель
Разглашение (например, при разговорах, записывание на бумаге и т.п.) пользовательских имён и паролей	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Использование для входа в систему чужих идентификаторов и паролей	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Использование оборудования, оставленного без присмотра, незаблокированных рабочих станций	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Запуск сторонних программ (технологических, инструментальных и т.п.)	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Изменение настроек и режимов работы ПО, модификация ПО (удаление, искажение или подмена программных компонентов ИСПДн или СЗИ) (преднамеренное или случайное)	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Подключение к ИСПДн стороннего оборудования (компьютеров, КПК, смартфонов, телефонов, фотоаппаратов, видеокамер, USB-дисков, флэш-дисков и иных устройств, в том числе имеющих выход в беспроводные сети связи)	Низкая	Средняя	Используются лицензионное антивирусное программное обеспечение, регулируется организационно-контрольными мерами. Требуется установка СЗИ от НСД
Нарушение работоспособности технических средств	Средняя	Средняя	Необходимо осуществлять резервное копирование базы данных ИСПДн на отчуждаемый носитель
Вмешательство в работу (нарушение правил использования) средств защиты	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Несанкционированное изменение конфигурационных файлов ПО (настроек экрана, сети, прикладных программ)	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Установка программных "клавиатурных шпионов"	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Применение специально созданных для повышения своих прав и привилегий и выполнения НСД программ	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Использование нетрадиционных каналов (стеганографии) инсайдером для передачи ПДн	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за сложности ее реализации в связи с необходимостью целенаправленного привлечения квалифицированных специалистов в области стеганографии
Удаление или искажение регистрационных данных СЗИ (преднамеренное или случайное)	Низкая	Маловероятно	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Несанкционированный доступ к ПДн в бумажном виде	Низкая	Низкая	Регулируется организационными мерами: кабинеты, в которых находится ИСПДн, в отсутствие сотрудников запираются на ключ.
Ошибки при разработке программного обеспечения ИСПДн (в том числе СЗИ)	Низкая	Маловероятно	Используется только лицензионное ПО
Осуществление неавторизованных действий в серверном помещении	Низкая	Маловероятная	серверное помещение запирается на ключ.

Вид угрозы	Опасность (ущерб)	Вероятность	Комментарии
Ошибки при обслуживании серверного оборудования и проведении операций по обслуживанию прикладных систем, либо при проведении установочных работ	Средняя	Средняя	В штате есть квалифицированный системный администратор.
Ошибки при доработке программного обеспечения ИСПДн (в том числе СЗИ)	Низкая	Маловероятно	Используется только лицензионное ПО.
Хищение, утрата резервных копий носителей ПДн	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция администратора)
Нарушение порядка резервного копирования ПДн	Средняя	Низкая	
Утеря или кража оборудования распределённой ИСПДн (в том числе резервных носителей информации) при транспортировке	Низкая	Маловероятно	ИСПДн не является распределенной
Доступ к информации ИСПДн, выходящей за пределы контролируемой зоны вследствие списания (утилизации) носителей информации, содержащих ПДн	Низкая	Низкая	Регулируется организационно-контрольными мерами (Положение о защите персональных данных)
Угрозы внедрения вредоносных программ (локально)			
Запись кода вредоносного ПО в код других программ с целью получения управления при запуске зараженных файлов, создание файлов-двойников для легального ПО (классические вирусы)	Средняя	Средняя	Используются лицензионное антивирусное программное обеспечение. Необходимо постоянное обновление вирусных баз.
Передача вредоносной программой своего кода на удаленный сервер или рабочую станцию (сетевые черви)	Средняя	Средняя	
Перебор паролей, демонстрация использования недекларированных возможностей программного и аппаратно-программного обеспечения ИСПДн, демонстрация уязвимостей ИСПДн (другие вредоносные программы, предназначенные для осуществления НСД)	Низкая	Маловероятно	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Преднамеренное внесение вредоносных кодов в программы при их разработке (программные закладки)	Низкая	Маловероятно	Используется только лицензионное прикладное ПО. При построении СЗПДн необходимо использовать только сертифицированные СЗИ
Преднамеренное внедрение вредоносной программы	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя). Пользователи ИСПДн официально предупреждены о необходимости соблюдения конфиденциальности ПДн и об ответственности за допущенные нарушения
Проникновение на рабочую станцию вредоносной программы из локальной сети вследствие отключения пользователями средств антивирусной защиты	Средняя	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя) и локальной политикой безопасности АРМ
Угрозы удаленного доступа			
Анализ сетевого трафика с перехватом информации, передаваемой по локальной сети, а также во внешние сети и принимаемой из внешних сетей с помощью анализаторов пакетов ("снифферы")			
Перехват идентификаторов и паролей пользователей для последующего осуществления несанкционированного доступа к объектам сети	Средняя	Маловероятно	Необходимо использование СЗи от НСД
Перехват конфиденциальной информации, передаваемой по сети в открытом или слабо защищённом виде	Низкая	Низкая	Рекомендуется использовать сертифицированные СКЗИ. Рекомендуется разработать порядок применения СКЗИ в ИСПДн
Сканирование сети с целью сбора информации об объектах сети, выявления используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов	Низкая	Низкая	Необходимо использование СЗи от НСД
Выявление паролей			
Подбор пароля путем перебора с помощью специального программного обеспечения	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за сложности ее реализации. Политика формирования и смены паролей определена Инструкцией администратора
Перехват пароля с помощью специального программного обеспечения	Низкая	Маловероятно	
Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа	Низкая	Маловероятно	
Навязывание ложного маршрута сети путем несанкционированного использования протоколов маршрутизации			
Атаки на DNS	Низкая	Маловероятно	Члены комиссии склоняются к

Вид угрозы	Опасность (ущерб)	Вероятность	Комментарии
Атаки на ARP	Низкая	Маловероятно	маловероятности такой угрозы из-за сложности ее реализации в связи с необходимостью целенаправленного привлечения высококвалифицированных специалистов в области сетевых информационных технологий
Атака "человек посередине"	Низкая	Маловероятно	

Вид угрозы	Опасность (ущерб)	Вероятность	Комментарии
Внедрение ложного объекта сети путем использования недостатков алгоритмов удаленного поиска			
Перехват нарушителем поискового запроса и выдача на него ложного ответа, использование которого приведет к требуемому изменению маршрута	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за сложности ее реализации в связи с необходимостью целенаправленного привлечения высококвалифицированных специалистов в области сетевых информационных технологий
Внедрение ложного ARP сервера	Низкая	Маловероятно	
Внедрение ложного DNS сервера	Низкая	Маловероятно	
Реализация отказа в обслуживании			
Привлечение части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов в целях реализации скрытого отказа в обслуживании	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за сложности ее реализации в связи с необходимостью целенаправленного привлечения высококвалифицированных специалистов в области сетевых информационных технологий
Исчерпание ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание) в целях реализации явного отказа в обслуживании	Низкая	Маловероятно	
Нарушение логической связности между атрибутами, данными, объектами путем передачи нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных или идентификационной и аутентификационной информации с целью реализации явного отказа в обслуживании	Низкая	Маловероятно	
Передача пакетов с нестандартными атрибутами или имеющих длину, превышающую максимально допустимый размер с целью реализации явного отказа в обслуживании	Низкая	Маловероятно	
Удалённый запуск приложений			
Активизация распространяемых злоумышленниками файлов, содержащих несанкционированный исполняемый код, при случайном обращении к ним пользователя ("спам" - при использовании электронной почты, "фишинг" - при использовании Интернета)	Средняя	Низкая	Используются лицензионное антивирусное программное обеспечение. Необходимо постоянное обновление вирусных баз.
Переполнение буфера приложений-серверов путем использования недостатков программ, реализующих сетевые сервисы (реализация переполнения буфера и настройка системных регистров, позволяющая переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера)	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за низкой коммерческой ценности имеющейся в ИСПДн информации
Использование скрытых программных и аппаратных закладок либо используемых штатных средств управления и администрирования компьютерных сетей для получения удаленного контроля над станцией в сети	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за низкой коммерческой ценности имеющейся в ИСПДн информации
Угрозы внедрения вредоносных программ (по сети)	Средняя	Средняя	Используются лицензионное антивирусное программное обеспечение. Необходимо постоянное обновление вирусных баз.
УГРОЗЫ, НЕ ЯВЛЯЮЩИЕСЯ АТАКОЙ (НЕПРЕДНАМЕРЕННЫЕ УГРОЗЫ)			
Угрозы, не связанные с деятельностью человека: стихийные бедствия и природные явления			
Землетрясение	Низкая	Маловероятно	Географическое местоположение организации практически исключает возможность стихийных бедствий
Наводнение	Низкая	Маловероятно	
Ураган	Низкая	Маловероятно	
Угрозы социально–политического характера			
Забастовка	Низкая	Маловероятно	Социальная обстановка в организации

Вид угрозы	Опасность (ущерб)	Вероятность	Комментарии
Саботаж	Низкая	Маловероятно	спокойная
Локальный конфликт	Низкая	Маловероятно	
Террористический акт (взрывы, угрозы взрыва, захваты...)	Низкая	Маловероятно	Организация находится вне «горячих точек»
Ошибочные действия и (или) нарушения тех или иных требований лицами, санкционированно взаимодействующими с возможными объектами угроз			
Непредумышленное искажение или удаление программных компонентов АСЗИ	Низкая	Маловероятно	Регулируется организационно-контрольными мерами (Инструкция пользователя) и локальной политикой безопасности АРМ
Внедрение и использование неучтенных программ	Низкая	Маловероятно	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Игнорирование организационных ограничений (установленных правил) при работе с ресурсами АСЗИ, включая средства защиты информации			
Нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (в частности, ключевой, парольной и аутентифицирующей информации)	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя и Инструкция администратора).
Настройка и конфигурирование средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов	Низкая	Маловероятно	Регулируется организационно-контрольными мерами (Инструкция администратора)
Несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Угрозы техногенного характера			
Неисправности, сбои аппаратных средств, нестабильность параметров системы электропитания, заземления и т.д.	Низкая	Низкая	Регулярно проводятся мероприятия по пожарной безопасности, осуществляются текущие строительные, электрические и санитарно-технические ремонтные работы в помещениях организации
Помехи и наводки, приводящие к сбоям в работе аппаратных средств	Низкая	Маловероятно	
Возгорание оборудования ИСПДн	Низкая	Маловероятно	
Затопление оборудования ИСПДн	Низкая	Маловероятно	

Выводы комиссии:
1. На основании экспертной оценки членов комиссии утвердить вербальные характеристики вероятности реализации угроз и показателя опасности угроз безопасности персональных данных, обрабатываемых в ИСПДн, по видам угроз безопасности в соответствии с данными, указанными в Таблице 1.
2. Использовать сведения, указанные в Таблице 1, для определения актуальных угроз безопасности персональных данных для ИСПДн.

Председатель комиссии: _____ _____
Члены комиссии: _____ _____
_____ _____
_____ _____
_____ _____

Приложение № 18
Утверждена
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ЧАСТНАЯ МОДЕЛЬ АКТУАЛЬНЫХ УГРОЗ
И ВЕРОЯТНОГО НАРУШИТЕЛЯ
информационной системы персональных данных
«Администрация»

Маркова Анна Александровна
Начальник отдела правового обеспечения и цифрового развития администрации Козловского муниципального округа Чувашской Республики _____ подпись _____ дата

Васильева Татьяна Леонидовна
Управляющий делами МО - начальник отдела организационно-контрольной и кадровой работы администрации Козловского муниципального округа Чувашской Республики _____ подпись _____ дата

Пушков Геннадий Михайлович
Заместитель главы администрации МО по экономике и сельскому хозяйству - начальник отдела экономики, инвестиционной деятельности, земельных и имущественных отношений администрации Козловского муниципального округа Чувашской Республики _____ подпись _____ дата

Комарова Валерия Игоревна
Заведующий сектором опеки и попечительства администрации Козловского муниципального округа Чувашской Республики _____ подпись _____ дата

Ульданова Анастасия Витальевна
Начальник отдела ЗАГС администрации Козловского муниципального округа Чувашской Республики _____ подпись _____ дата

г. Козловка
2024

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники
Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.
Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
Вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.
Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.
Доступ в операционную среду компьютера (информационной системы персональных данных) - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.
Доступ к информации – возможность получения информации и ее использования.
Закладочное устройство - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).
Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.
Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.
Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.
Носитель информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.
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.
Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
Побочные электромагнитные излучения и наводки - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.
Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.
Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
Программная закладка - скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.
Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.
Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.
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.
Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.
Уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности ПДн.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ – автоматизированное рабочее место;
ВТСС – вспомогательные технические средства и системы;
ИСПДн – информационная система персональных данных;
КЗ – контролируемая зона;
НДВ – недекларированные возможности;
НСД – несанкционированный доступ;
ОБПДн – обеспечение безопасности персональных данных;
ОС – операционная система;
ПДн – персональные данные;
ПМВ – программно-математическое воздействие;
ПЭМИН – побочные электромагнитные излучения и наводки;
СВТ – средство вычислительной техники;
СЗИ – средство защиты информации;
СЭУПИ – специальные электронные устройства перехвата информации;
УБПДн – угрозы безопасности персональных данных.

1.ОБЩИЕ ПОЛОЖЕНИЯ

Частная модель актуальных угроз Администрации Козловского муниципального округа Чувашской Республики (далее Оператор) разработана в соответствии с нормативными документами ФСТЭК России:

- Базовая модель безопасности персональных данных при их обработке в информационных системах персональных данных, 2008г.;

Частная модель угроз содержит описание возможных угроз безопасности персональных данных и расчет актуальных угроз для ИСПДн Оператора.
Частная модель угроз направлена на определение возможных каналов утечки, путем анализа защищенности ИСПДн Оператора.
Под угрозами безопасности ПДн при их обработке в ИСПДн понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

В соответствии со статьей 19 Федерального закона №152-ФЗ от 27 июля 2006 г. «О персональных данных», ПДн должны быть защищены от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий. Угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн и(или) потребителей, пользующихся услугами, предоставляемыми ИСПДн в соответствии с ее назначением, так и со специально осуществляемыми неправомерными действиями иностранных государств, криминальных сообществ, отдельных организаций и граждан, а также иными источниками угроз.
Угрозы безопасности ПДн могут быть реализованы за счет утечки ПДн по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах ИСПДн, технические каналы перехвата информации при ее передаче по каналам связи, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа с использованием соответствующего программного обеспечения.

2. ОПИСАНИЕ ИСПДН

2.1. Общие характеристики ИСПДн приведены в Таблице 1

№ п/н	Характеристика	Значение характеристики
1	Состав ИСПДн	Microsoft Office (Кадры) Сайт Обращения граждан
2	Назначение	Осуществление кадрового учета; предоставление государственных услуг, обратившимся гражданам. Передача данных в государственные, муниципальные и контролирующие органы
3	Категория обрабатываемых в ИСПДн персональных данных	ИСПДн «Администрация» является информационной системой, обрабатывающей иные категории персональных данных, т.е. в ней не обрабатываются специальные категории персональных данных, биометрические персональные данные, общедоступные персональные данные.
4	Объем обрабатываемых ПДн (количество субъектов персональных данных, ПДн которых обрабатываются в ИСПДн)	Объем обрабатываемых в ИСПДн «Администрация» персональных данных менее 100000 субъектов персональных данных
5	Субъекты персональных данных	ИСПДн «Администрация» является информационной системой, обрабатывающей персональные данные субъектов персональных данных, являющихся сотрудниками оператора персональных данных; является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора персональных данных.
6	Структура ИСПДн	Локальная информационная система (используются комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа).
7	Подключение ИСПДн к сетям связи общего пользования и (или) сетям международного обмена	Имеет подключение к сетям международного информационного обмена.
8	Режим обработки персональных данных	Многопользовательский
9	Разграничение доступа	ИСПДн с разграничением прав доступа.
10	Местонахождение технических средств ИСПДн	Все средства находятся в пределах Российской Федерации.

3. ОПРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИСПДН

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн.
Актуальность угрозы определяется следующими параметрами:
– уровень исходной защищенности ИСПДн;
– частота (вероятность) реализации рассматриваемой угрозы.
Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн. Характеристики ИСПДн «Администрация» приведены в таблице:

№	Параметр	Значение	Уровень защищенности
1	Территориальное размещение	локальная ИСПДн, развернутая в пределах одного здания	Высокий
2	Наличие соединений с сетями общего пользования	ИСПДн, имеющая одноточечный выход в сеть общего пользования;	Средний
3	Встроенные (легальные) операции с записями баз персональных данных	модификация, передача	Низкий
4	Разграничение доступа к персональным данным	ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	Средний
5	Наличие соединений с другими	ИСПДн, в которой используются несколько баз ПДн,	Средний

	базами ПДн иных ИСПДн	принадлежащая организации – владельцу данной ИСПДн	
6	Уровень обобщения (обезличивания) ПДн	ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	Средний
7	Объем ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	ИСПДн, предоставляющая часть ПДн;	Средний

Соотношение характеристик ИСПДн, соответствующих разным уровням защищенности:
– 14% характеристик ИСПДн соответствуют ***высокому*** уровню защищенности;
– 72% характеристик ИСПДн соответствуют ***среднему*** уровню защищенности;
– 14% характеристик ИСПДн соответствуют ***низкому*** уровню защищенности.
Уровень исходной защищенности ИСПДн – средний (Y_1=5).
По каждому виду угрозы, экспертным путем (опрос специалистов) определены:
– опасность (ущерб) в соответствии с правилами, приведенными в таблице 2.

Таблица 2

Опасность (ущерб) угрозы и её характеристики

Опасность (ущерб) угрозы		
Низкая	**Средняя**	**Высокая**
Реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных	Реализация угрозы может привести к негативным последствиям для субъектов персональных данных	Реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных

– вероятность реализации угрозы ($Y_{2)}$ в соответствии с правилами, приведенными в таблице 3.

Таблица 3

Вероятность угрозы и её характеристики

Вероятность	**Y2**
Маловероятно	0
Низкая	2
Средняя	5
Высокая	10

С учетом полученных числовых коэффициентов Y_1 и Y_2 по каждому виду угрозы безопасности ПДн рассчитывается числовой коэффициент реализуемости угрозы Y по формуле:

$$Y = (Y_1 + Y_2)/20$$

Соответствие значения числового коэффициента реализуемости угрозы Y и его возможной реализации приведено в таблице 4.

Таблица 4

Значения реализуемости

Значение числового коэффициента реализуемости угрозы Y	**Возможность реализации угрозы**
YЄ [0 ; 0.3]	Низкая
YЄ (0.3 ; 0.6]	Средняя
YЄ (0.6 ; 0.8]	Высокая
YЄ (0.8 ; 1]	Очень высокая

Актуальность угрозы безопасности ПДн определяется на основании значения коэффициента реализуемости угрозы (Y) и показателя опасности (ущерба) угрозы по каждому ее виду. Вывод об актуальности угрозы происходит в соответствии с правилами, представленными в таблице 5.

Таблица 5

Актуальность реализации угрозы

Возможность реализации угрозы	**Опасность угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Угрозы и их характеристики представлены в таблице 6.

Таблица угроз и их характеристик приведена ниже.

Наименование угрозы	Вероятность (Y2)	Реализуемость (Y)	Опасность	Актуальность
УГРОЗЫ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ				
Угрозы утечки акустической (речевой) информации	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы утечки видовой информации	низкая вероятность (2)	низкая (0.35)	низкая	неактуальная
Угрозы утечки информации по каналу ПЭМИН	маловероятно (0)	низкая (0.25)	низкая	неактуальная
УГРОЗЫ НСД К ПДн, ОБРАБАТЫВАЕМЫМ НА АВТОМАТИЗИРОВАННОМ РАБОЧЕМ МЕСТЕ				
Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	средняя вероятность (5)	средняя (0.5)	средняя	актуальная
Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование и т.п.) операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ	средняя вероятность (5)	средняя (0.5)	средняя	актуальная
СЕТЕВЫЕ УГРОЗЫ				
Угрозы "Анализа сетевого трафика" с перехватом передаваемой по сети информации	низкая вероятность (2)	низкая (0.35)	низкая	неактуальная
Угрозы выявления паролей	низкая вероятность (2)	низкая (0.35)	средняя	неактуальная
Угрозы удаленного запуска приложений	маловероятно (0)	низкая (0.25)	средняя	неактуальная
Угрозы внедрения по сети вредоносных программ	средняя вероятность (5)	средняя (0.5)	средняя	актуальная
УГРОЗЫ ИЗ ВНЕШНИХ СЕТЕЙ				
Угрозы "Анализа сетевого трафика" с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы выявления паролей	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы получения НСД путем подмены доверенного объекта	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы типа "Отказ в обслуживании"	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы удаленного запуска приложений	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы внедрения по сети вредоносных программ	средняя вероятность (5)	средняя (0.5)	средняя	актуальная

4. МОДЕЛЬ ВЕРОЯТНОГО НАРУШИТЕЛЯ

По наличию права постоянного или разового доступа в ИСПДн нарушители подразделяются на два типа:

- нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена – внешние нарушители;
- нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн – внутренние нарушители.

Внешними нарушителями могут быть:

- криминальные структуры;
- недобросовестные партнеры;
- внешние субъекты (физические лица).

Внешний нарушитель имеет следующие возможности:

- осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
- осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;
- осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
- осуществлять несанкционированные доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами контролируемой зоны.

Категории нарушителей

№	Описание	Нарушитель может	Возможный нарушитель
1	Лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн.	- иметь доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн; - располагать фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах; - располагать именами и вести выявление паролей зарегистрированных пользователей; - изменять конфигурацию технических средств ИСПДн, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн.	Сотрудники, не участвующие в обработке ПДн
2	Зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места.	- обладает всеми возможностями лиц первой категории; - знает по меньшей мере одно легальное имя доступа; - обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн; - располагает конфиденциальными данными, к которым имеет доступ.	Сотрудники, обрабатывающие ПДн
3	Зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам	- обладает всеми возможностями лиц первой и второй категорий; - располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системам, через которую он осуществляет доступ, и составе технических средств ИСПДн; - имеет возможность прямого (физического) доступа к фрагментам технических средств ИСПДн.	Отсутствует
4	Зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн.	- обладает всеми возможностями лиц предыдущих категорий; - обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИСПДн; - обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИСПДн; - имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИСПДн; – имеет доступ ко всем техническим средствам сегмента (фрагмента) ИСПДн; – обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) ИСПДн.	Отсутствует
5	Зарегистрированные пользователи с полномочиями системного администратора ИСПДн	– обладает всеми возможностями лиц предыдущих категорий; – обладает полной информацией о системном и прикладном программном обеспечении ИСПДн; – обладает полной информацией о технических средствах и конфигурации ИСПДн; – имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн; – обладает правами конфигурирования и административной настройки технических средств ИСПДн.	Системный администратор ИСПДн
6	Зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн	– обладает всеми возможностями лиц предыдущих категорий; – обладает полной информацией об ИСПДн; – имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн; – не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).	Администратор безопасности ИСПДн
7	Программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте	– обладает информацией об алгоритмах и программах обработки информации на ИСПДн; – обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения; – может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.	Отсутствует
8	Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн	– обладает возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения; – может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты информации в ИСПДн.	Отсутствует

5. ВЫВОДЫ

5.1 В результате анализа возможных угроз безопасности персональных данных выявлено 3 актуальные угрозы безопасности:

№ п/п	Угроза	Вероятность	Опасность
1	Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	средняя вероятность (5)	средняя
2	Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование и т.п.) операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ	средняя вероятность (5)	средняя
3	Угрозы внедрения по сети вредоносных программ	средняя вероятность (5)	средняя

5.2 Выявленные актуальные угрозы безопасности ПДн в ИСПДн при их реализации могут привести к незначительным последствиям для субъектов ПДн. Необходимо провести мероприятия по устранению указанных угроз или снижению их уровня.

Приложение № 19
Утверждена
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ЧАСТНАЯ МОДЕЛЬ АКТУАЛЬНЫХ УГРОЗ
И ВЕРОЯТНОГО НАРУШИТЕЛЯ
информационной системы персональных данных
«Опека и попечительство»

Маркова Анна Александровна
Начальник отдела правового обеспечения и цифрового развития администрации Козловского муниципального округа Чувашской Республики _____ подпись _____ дата

Васильева Татьяна Леонидовна
Управляющий делами МО - начальник отдела организационно-контрольной и кадровой работы администрации Козловского муниципального округа Чувашской Республики _____ подпись _____ дата

Пушков Геннадий Михайлович
Заместитель главы администрации МО по экономике и сельскому хозяйству - начальник отдела экономики, инвестиционной деятельности, земельных и имущественных отношений администрации Козловского муниципального округа Чувашской Республики _____ подпись _____ дата

Комарова Валерия Игоревна
Заведующий сектором опеки и попечительства администрации Козловского муниципального округа Чувашской Республики _____ подпись _____ дата

Ульданова Анастасия Витальевна
Начальник отдела ЗАГС администрации Козловского муниципального округа Чувашской Республики _____ подпись _____ дата

г. Козловка
2024 г.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

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

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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.

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

Побочные электромагнитные излучения и наводки - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Программная закладка - скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

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.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности ПДн.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ – автоматизированное рабочее место;
ВТСС – вспомогательные технические средства и системы;
ИСПДн – информационная система персональных данных;
КЗ – контролируемая зона;
НДВ – недекларированные возможности;
НСД – несанкционированный доступ;
ОБПДн – обеспечение безопасности персональных данных;
ОС – операционная система;
ПДн – персональные данные;
ПМВ – программно-математическое воздействие;
ПЭМИН – побочные электромагнитные излучения и наводки;
СВТ – средство вычислительной техники;
СЗИ – средство защиты информации;
СЭУПИ – специальные электронные устройства перехвата информации;
УБПДн – угрозы безопасности персональных данных.

ОБЩИЕ ПОЛОЖЕНИЯ

Частная модель актуальных угроз Администрации Козловского муниципального округа Чувашской Республики (далее Оператор) разработана в соответствии с нормативными документами ФСТЭК России:

- Базовая модель безопасности персональных данных при их обработке в информационных системах персональных данных, 2008г.;

Частная модель угроз содержит описание возможных угроз безопасности персональных данных и расчет актуальных угроз для ИСПДн Оператора.
Частная модель угроз направлена на определение возможных каналов утечки, путем анализа защищенности ИСПДн Оператора.
Под угрозами безопасности ПДн при их обработке в ИСПДн понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.
В соответствии со статьей 19 Федерального закона №152-ФЗ от 27 июля 2006 г. «О персональных данных», ПДн должны быть защищены от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.
Угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн и (или) потребителей, пользующихся услугами, предоставляемыми ИСПДн в соответствии с ее назначением, так и со специально осуществляемыми неправомерными действиями иностранных государств, криминальных сообществ, отдельных организаций и граждан, а также иными источниками угроз.
Угрозы безопасности ПДн могут быть реализованы за счет утечки ПДн по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах ИСПДн, технические каналы перехвата информации при ее передаче по каналам связи, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа с использованием соответствующего программного обеспечения.

2. ОПИСАНИЕ ИСПДН

2.1. Общие характеристики ИСПДн приведены в Таблице 1

№ п/н	Характеристика	Значение характеристики
1	Состав ИСПДн	MS Office
2	Назначение	Осуществление деятельности в соответствие с ФЗ «Об опеке и попечительстве». Предоставление государственных услуг, обратившимся гражданам. Передача данных в государственные, муниципальные и контролирующие органы
3	Категория обрабатываемых в ИСПДн персональных данных	ИСПДн «Опека и попечительство» является информационной системой, обрабатывающей иные категории персональных данных, т.е. в ней не обрабатываются специальные категории персональных данных, биометрические персональные данные, общедоступные персональные данные.
4	Объем обрабатываемых ПДн (количество субъектов персональных данных, ПДн которых обрабатываются в ИСПДн)	Объем обрабатываемых в ИСПДн «Опека и попечительство» персональных данных менее 100000 субъектов персональных данных
5	Субъекты персональных данных	ИСПДн «Опека и попечительство» является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора персональных данных.
6	Структура ИСПДн	Локальная информационная система (используются комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа).
7	Подключение ИСПДн к сетям связи общего пользования и (или) сетям международного обмена	Имеет подключение к сетям международного информационного обмена.
8	Режим обработки персональных	Многопользовательский

	данных	
9	Разграничение доступа	ИСПДн с разграничением прав доступа.
10	Местонахождение технических средств ИСПДн	Все средства находятся в пределах Российской Федерации.

3. ОПРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИСПДН

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн.
Актуальность угрозы определяется следующими параметрами:

– уровень исходной защищенности ИСПДн;
– частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн. Характеристики ИСПДн «Бухгалтерия» приведены в таблице:

№	Параметр	Значение	Уровень защищенности
1	Территориальное размещение	локальная ИСПДн, развернутая в пределах одного здания	Высокий
2	Наличие соединений с сетями общего пользования	ИСПДн, имеющая одноточечный выход в сеть общего пользования;	Средний
3	Встроенные (легальные) операции с записями баз персональных данных	модификация, передача	Низкий
4	Разграничение доступа к персональным данным	ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	Средний
5	Наличие соединений с другими базами ПДн иных ИСПДн	ИСПДн, в которой используются несколько баз ПДн, принадлежащая организации – владельцу данной ИСПДн	Средний
6	Уровень обобщения (обезличивания) ПДн	ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	Средний
7	Объем ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	ИСПДн, предоставляющая часть ПДн;	Средний

Соотношение характеристик ИСПДн, соответствующих разным уровням защищенности:

– 14% характеристик ИСПДн соответствуют ***высокому*** уровню защищенности;
– 72% характеристик ИСПДн соответствуют ***среднему*** уровню защищенности;
– 14% характеристик ИСПДн соответствуют ***низкому*** уровню защищенности.

Уровень исходной защищенности ИСПДн – средний (Y_1=5).
По каждому виду угрозы, экспертным путем (опрос специалистов) определены:

– опасность (ущерб) в соответствии с правилами, приведенными в таблице 2.

Таблица 2

Опасность (ущерб) угрозы и её характеристики

Опасность (ущерб) угрозы		
Низкая	**Средняя**	**Высокая**
Реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных	Реализация угрозы может привести к негативным последствиям для субъектов персональных данных	Реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных

– вероятность реализации угрозы ($Y_{2)}$ в соответствии с правилами, приведенными в таблице 3.

Таблица 3

Вероятность угрозы и её характеристики

Вероятность	**Y2**
Маловероятно	0
Низкая	2
Средняя	5
Высокая	10

С учетом полученных числовых коэффициентов Y_1 и Y_2 по каждому виду угрозы безопасности ПДн рассчитывается числовой коэффициент реализуемости угрозы Y по формуле:

$$Y = (Y_1 + Y_2)/20$$

Соответствие значения числового коэффициента реализуемости угрозы Y и его возможной реализации приведено в таблице 4.

Таблица 4

Значения реализуемости

Значение числового коэффициента реализуемости угрозы Y	**Возможность реализации угрозы**
Y∈ [0 ; 0.3]	Низкая
Y∈ (0.3 ; 0.6]	Средняя
Y∈ (0.6 ; 0.8]	Высокая
Y∈ (0.8 ; 1]	Очень высокая

Актуальность угрозы безопасности ПДн определяется на основании значения коэффициента реализуемости угрозы (Y) и показателя опасности (ущерба) угрозы по каждому ее виду. Вывод об актуальности угрозы происходит в соответствии с правилами, представленными в таблице 5.

Таблица 5

Актуальность реализации угрозы

Возможность реализации угрозы	**Опасность угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Угрозы и их характеристики представлены в таблице 6.

Таблица угроз и их характеристик приведена ниже.

Наименование угрозы	Вероятность (Y2)	Реализуемость (Y)	Опасность	Актуальность
УГРОЗЫ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ				
Угрозы утечки акустической (речевой) информации	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы утечки видовой информации	низкая вероятность (2)	низкая (0.35)	низкая	неактуальная
Угрозы утечки информации по каналу ПЭМИН	маловероятно (0)	низкая (0.25)	низкая	неактуальная
УГРОЗЫ НСД К ПДн, ОБРАБАТЫВАЕМЫМ НА АВТОМАТИЗИРОВАННОМ РАБОЧЕМ МЕСТЕ				
Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	средняя вероятность (5)	средняя (0.5)	средняя	актуальная
Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование и т.п.) операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ	средняя вероятность (5)	средняя (0.5)	средняя	актуальная
СЕТЕВЫЕ УГРОЗЫ				
Угрозы "Анализа сетевого трафика" с перехватом передаваемой по сети информации	низкая вероятность (2)	низкая (0.35)	низкая	неактуальная
Угрозы выявления паролей	низкая вероятность (2)	низкая (0.35)	средняя	неактуальная
Угрозы удаленного запуска приложений	маловероятно (0)	низкая (0.25)	средняя	неактуальная
Угрозы внедрения по сети вредоносных программ	средняя вероятность (5)	средняя (0.5)	средняя	актуальная
УГРОЗЫ ИЗ ВНЕШНИХ СЕТЕЙ				
Угрозы "Анализа сетевого трафика" с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы выявления паролей	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы получения НСД путем подмены доверенного объекта	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы типа "Отказ в обслуживании"	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы удаленного запуска приложений	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы внедрения по сети вредоносных программ	средняя вероятность (5)	средняя (0.5)	средняя	актуальная

4. МОДЕЛЬ ВЕРОЯТНОГО НАРУШИТЕЛЯ

По наличию права постоянного или разового доступа в ИСПДн нарушители подразделяются на два типа:

- нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена – внешние нарушители;
- нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн – внутренние нарушители.

Внешними нарушителями могут быть:

- криминальные структуры;
- недобросовестные партнеры;
- внешние субъекты (физические лица).

Внешний нарушитель имеет следующие возможности:

- осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
- осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;
- осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
- осуществлять несанкционированные доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами контролируемой зоны.

Категории нарушителей

№	Описание	Нарушитель может	Возможный нарушитель
1	Лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн.	– иметь доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн; – располагать фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах; – располагать именами и вести выявление паролей зарегистрированных пользователей; – изменять конфигурацию технических средств ИСПДн, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн.	Сотрудники, не участвующие в обработке ПДн
2	Зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места.	– обладает всеми возможностями лиц первой категории; – знает по меньшей мере одно легальное имя доступа; – обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн; – располагает конфиденциальными данными, к которым имеет доступ.	Сотрудники, обрабатывающие ПДн
3	Зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам	– обладает всеми возможностями лиц первой и второй категорий; – располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системам, через которую он осуществляет доступ, и составе технических средств ИСПДн; – имеет возможность прямого (физического) доступа к фрагментам технических средств ИСПДн.	Отсутствует
4	Зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн.	– обладает всеми возможностями лиц предыдущих категорий; – обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИСПДн; – обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИСПДн; – имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИСПДн; – имеет доступ ко всем техническим средствам сегмента (фрагмента) ИСПДн; – обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) ИСПДн.	Отсутствует
5	Зарегистрированные пользователи с полномочиями системного администратора ИСПДн	– обладает всеми возможностями лиц предыдущих категорий; – обладает полной информацией о системном и прикладном программном обеспечении ИСПДн; – обладает полной информацией о технических средствах и конфигурации ИСПДн; – имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн; – обладает правами конфигурирования и административной настройки технических средств ИСПДн.	Системный администратор ИСПДн
6	Зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн	– обладает всеми возможностями лиц предыдущих категорий; – обладает полной информацией об ИСПДн; – имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн; – не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).	Администратор безопасности ИСПДн
7	Программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте	– обладает информацией об алгоритмах и программах обработки информации на ИСПДн; – обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения; – может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.	Отсутствует
8	Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн	– обладает возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения; – может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты информации в ИСПДн.	Отсутствует

5. ВЫВОДЫ

5.1 В результате анализа возможных угроз безопасности персональных данных выявлено 3 актуальные угрозы безопасности:

№ п/п	Угроза	Вероятность	Опасность
	Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	средняя вероятность (5)	средняя
	Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование и т.п.) операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ	средняя вероятность (5)	средняя
	Угрозы внедрения по сети вредоносных программ	средняя вероятность (5)	средняя

5.2 Выявленные актуальные угрозы безопасности ПДн в ИСПДн при их реализации могут привести к незначительным последствиям для субъектов ПДн. Необходимо провести мероприятия по устранению указанных угроз или снижению их уровня.

Приложение № 20
Утвержден
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

Акт
определения уровня защищенности
персональных данных в информационной системе
персональных данных «Администрация»
(ИСПДн «Администрация»)
Администрации Козловского муниципального округа Чувашской Республики

г. Козловка 18.12.2024

Комиссия в составе:
Председатель комиссии:

Маркова Анна Александровна	Начальник отдела правового обеспечения и цифрового развития администрации Козловского муниципального округа Чувашской Республики

Члены комиссии:

Васильева Татьяна Леонидовна	Управляющий делами МО - начальник отдела организационно-контрольной и кадровой работы администрации Козловского муниципального округа Чувашской Республики
Пушков Геннадий Михайлович	Заместитель главы администрации МО по экономике и сельскому хозяйству - начальник отдела экономики, инвестиционной деятельности, земельных и имущественных отношений администрации Козловского муниципального округа Чувашской Республики
Комарова Валерия Игоревна	Заведующий сектором опеки и попечительства администрации Козловского муниципального округа Чувашской Республики
Ульданова Анастасия Витальевна	Начальник отдела ЗАГС администрации Козловского муниципального округа Чувашской Республики

рассмотрела следующие исходные данные на информационную систему персональных данных (ИСПДн):
1. Наименование ИСПДн и состав программного обеспечения, используемого для обработки персональных данных.
ИСПДн «Администрация» в составе:
MS Office (Кадры),
Сайт
Обращений граждан
2. Категория обрабатываемых персональных данных.
ИСПДн «Администрация» является информационной системой, обрабатывающей иные категории персональных данных, т.е. в ней не обрабатываются специальные категории персональных данных, биометрические персональные данные, общедоступные персональные данные.
3. Объем обрабатываемых персональных данных.
Объем обрабатываемых в **ИСПДн «Администрация»** персональных данных менее 100000 субъектов персональных данных
4. Субъекты персональных данных.
ИСПДн «Администрация» является информационной системой, обрабатывающей персональные данные субъектов персональных данных, являющихся сотрудниками оператора персональных данных.
5. Актуальные угрозы безопасности персональных данных.

Для **ИСПДн «Администрация»** актуальны угрозы 3-го типа, т.е. угрозы не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

6. Структура информационной системы.
Локальная информационная система (используются комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа).

7. Подключение информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена.
Имеет подключение к сетям международного информационного обмена.

8. Режим обработки персональных данных.
Многопользовательский.

9. Разграничение доступа.
ИСПДн с разграничением прав доступа.

10. Местонахождение технических средств информационной системы.
Все средства находятся в пределах Российской Федерации.

Заключение комиссии:
В соответствии с пунктом 12 постановления Правительства Российской Федерации от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", признать необходимым обеспечение 4-го уровня защищенности персональных данных при их обработке в ИСПДн «Администрация».

Председатель комиссии: _____ _____
Члены комиссии: _____ _____
_____ _____
_____ _____
_____ _____

Приложение № 21
Утвержден
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

Акт
определения уровня защищенности
персональных данных в информационной системе
персональных данных «Опека и попечительство»
(ИСПДн «Опека и попечительство»)
Администрации Козловского муниципального округа Чувашской Республики

г. Козловка 18.12.2024

Комиссия в составе:
Председатель комиссии:

Маркова Анна Александровна	Начальник отдела правового обеспечения и цифрового развития администрации Козловского муниципального округа Чувашской Республики

Члены комиссии:

Васильева Татьяна Леонидовна	Управляющий делами МО - начальник отдела организационно-контрольной и кадровой работы администрации Козловского муниципального округа Чувашской Республики
Пушков Геннадий Михайлович	Заместитель главы администрации МО по экономике и сельскому хозяйству - начальник отдела экономики, инвестиционной деятельности, земельных и имущественных отношений администрации Козловского муниципального округа Чувашской Республики
Комарова Валерия Игоревна	Заведующий сектором опеки и попечительства администрации Козловского муниципального округа Чувашской Республики
Ульданова Анастасия Витальевна	Начальник отдела ЗАГС администрации Козловского муниципального округа Чувашской Республики

рассмотрела следующие исходные данные на информационную систему персональных данных (ИСПДн):
Наименование ИСПДн и состав программного обеспечения, используемого для обработки персональных данных.
ИСПДн «Опека и попечительство» в составе:
MS Office

Категория обрабатываемых персональных данных.

ИСПДн «Опека и попечительство» является информационной системой, обрабатывающей специальные категории персональных данных, т.е. в ней обрабатываются персональные данные, касающиеся, национальной принадлежности, состояния здоровья, субъектов персональных данных.

Объем обрабатываемых персональных данных.
Объем обрабатываемых в **ИСПДн «Опека и попечительство»** персональных данных менее 100000 субъектов персональных данных

Субъекты персональных данных.
ИСПДн «Опека и попечительство» является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора персональных данных.

Актуальные угрозы безопасности персональных данных.
Для **ИСПДн «Опека и попечительство»** актуальны угрозы 3-го типа, т.е. угрозы не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Структура информационной системы.
Локальная информационная система (используются комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа).

Подключение информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена.
Имеет подключение к сетям международного информационного обмена.

Режим обработки персональных данных.
Многопользовательский.

Разграничение доступа.
ИСПДн с разграничением прав доступа.

Местонахождение технических средств информационной системы.
Все средства находятся в пределах Российской Федерации.

Заключение комиссии:
В соответствии с пунктом 12 постановления Правительства Российской Федерации от 1 ноября 2012 г. №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», признать необходимым обеспечение 4-го уровня защищенности персональных данных при их обработке в ИСПДн «Опека и попечительство».

Председатель комиссии: _____ _____
Члены комиссии: _____ _____
_____ _____
_____ _____
_____ _____

Приложение № 22
Утверждена
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ИНСТРУКЦИЯ
АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ (ИСПДН)
«ИМУЩЕСТВЕННЫЕ И ЗЕМЕЛЬНЫЕ ОТНОШЕНИЯ»

г. Козловка
2024 г.

1. Общие положения

1.1. Администратор ИСПДн «Имущественные и земельные отношения» (далее Администратор) назначается распоряжением Администрации Козловского муниципального округа Чувашской Республики (далее Администрация).
1.2. Администратор подчиняется Главе Козловского муниципального округа Чувашской Республики.
1.3. Администратор в своей работе руководствуется настоящей инструкцией, Политикой информационной безопасности, а также другими руководящими и нормативными документами ФСТЭК России и регламентирующими документами Общества.
1.4. Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, при обработке персональных данных.
1.5. Методическое руководство работой Администратора осуществляется ответственным за обеспечение защиты персональных данных.

2. Должностные обязанности

Администратор обязан:
2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.
2.2. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:
программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное программное обеспечение);
аппаратных средств;
аппаратных и программных средств защиты.
2.3. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.
2.4. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.
2.5. Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.
2.6. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.
2.7. Проводить периодический контроль принятых мер по защиты, в пределах возложенных на него функций.
2.8. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля Оператором ИСПДн.
2.9. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.
2.10. Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.
2.11. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.
2.12. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие специальные исследования и специальную проверку.
2.13. Присутствовать при выполнении технического обслуживания элементов ИСПДн, сторонними физическими людьми и организациями.
2.14. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

3. Права

Администратор имеет право:
3.1. Знакомиться с проектами распоряжений и постановлений Администрации Козловского муниципального округа Чувашской Республики, касающихся его деятельности.
3.2. Вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с предусмотренными настоящей инструкцией обязанностями.
3.3. В пределах своей компетенции сообщать своему непосредственному руководителю обо всех выявленных в процессе осуществления должностных обязанностей недостатках в деятельности организации (его структурных подразделениях) и вносить предложения по их устранению.
3.4. Запрашивать лично или по поручению своего непосредственного руководителя от специалистов подразделений информацию и документы, необходимые для выполнения его должностных обязанностей.
3.5. Привлекать специалистов всех (отдельных) структурных подразделений к решению задач, возложенных на него (если это предусмотрено положениями о структурных подразделениях, если нет — то с разрешения их руководителей).
3.6. Требовать от своего непосредственного руководителя оказания содействия в исполнении им своих должностных обязанностей и прав.

4. Ответственность

Администратор несет ответственность:
4.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией — в пределах, определенных действующим трудовым законодательством Российской Федерации.
4.2. За правонарушения, совершенные в процессе осуществления своей деятельности — в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.
4.3. За причинение материального ущерба — в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

4.4. За разглашение конфиденциальной информации, содержащей персональные данные – в пределах, определенных действующим административным, уголовным, трудовым и гражданским законодательством РФ.
4.4.1. Администратор ИСПДн, получающий доступ к конфиденциальной информации, содержащей персональные данные, несет персональную ответственность за сохранность носителя и конфиденциальность информации.

С инструкцией ознакомлен (а) и обязуюсь хранить на рабочем месте

_____ _____«____» _____20__ г.
(фамилия, инициалы) (подпись)

Один экземпляр инструкции на руки получил

_____ _____«____» _____20__ г.
(фамилия, инициалы) (подпись)

Инструкция разработана:

Начальник отдела правового обеспечения
и цифрового развития администрации
Козловского муниципального округа
Чувашской Республики _____ / _____

Приложение № 23
Утверждена
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ЧАСТНАЯ МОДЕЛЬ АКТУАЛЬНЫХ УГРОЗ
И ВЕРОЯТНОГО НАРУШИТЕЛЯ
информационной системы персональных данных
«Имущественные и земельные отношения»

Маркова Анна Александровна
Начальник отдела правового обеспечения и цифрового развития администрации Козловского муниципального округа Чувашской Республики _____ подпись _____ дата

Васильева Татьяна Леонидовна
Управляющий делами МО - начальник отдела организационно-контрольной и кадровой работы администрации Козловского муниципального округа Чувашской Республики _____ подпись _____ дата

Пушков Геннадий Михайлович
Заместитель главы администрации МО по экономике и сельскому хозяйству - начальник отдела экономики, инвестиционной деятельности, земельных и имущественных отношений администрации Козловского муниципального округа Чувашской Республики _____ подпись _____ дата

Комарова Валерия Игоревна
Заведующий сектором опеки и попечительства администрации Козловского муниципального округа Чувашской Республики _____ подпись _____ дата

Ульданова Анастасия Витальевна
Начальник отдела ЗАГС администрации Козловского муниципального округа Чувашской Республики _____ подпись _____ дата

г. Козловка
2024 г.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

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

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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.

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

Побочные электромагнитные излучения и наводки - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Программная закладка - скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

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.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности ПДн.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ – автоматизированное рабочее место;
ВТСС – вспомогательные технические средства и системы;
ИСПДн – информационная система персональных данных;
КЗ – контролируемая зона;
НДВ – недекларированные возможности;
НСД – несанкционированный доступ;
ОБПДн – обеспечение безопасности персональных данных;
ОС – операционная система;
ПДн – персональные данные;
ПМВ – программно-математическое воздействие;
ПЭМИН – побочные электромагнитные излучения и наводки;
СВТ – средство вычислительной техники;
СЗИ – средство защиты информации;
СЭУПИ – специальные электронные устройства перехвата информации;
УБПДн – угрозы безопасности персональных данных.

1.ОБЩИЕ ПОЛОЖЕНИЯ

Частная модель актуальных угроз Администрации Козловского муниципального округа Чувашской Республики (далее Оператор) разработана в соответствии с нормативными документами ФСТЭК России:

- Базовая модель безопасности персональных данных при их обработке в информационных системах персональных данных, 2008г.;

Частная модель угроз содержит описание возможных угроз безопасности персональных данных и расчет актуальных угроз для ИСПДн Оператора.
Частная модель угроз направлена на определение возможных каналов утечки, путем анализа защищенности ИСПДн Оператора.
Под угрозами безопасности ПДн при их обработке в ИСПДн понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.
В соответствии со статьей 19 Федерального закона №152-ФЗ от 27 июля 2006 г. «О персональных данных», ПДн должны быть защищены от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий. Угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн и (или) потребителей, пользующихся услугами, предоставляемыми ИСПДн в соответствии с ее назначением, так и со специально осуществляемыми неправомерными действиями иностранных государств, криминальных сообществ, отдельных организаций и граждан, а также иными источниками угроз.
Угрозы безопасности ПДн могут быть реализованы за счет утечки ПДн по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах ИСПДн, технические каналы перехвата информации при ее передаче по каналам связи, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа с использованием соответствующего программного обеспечения.

2. ОПИСАНИЕ ИСПДН

2.1. Общие характеристики ИСПДн приведены в Таблице 1

№ п/н	Характеристика	Значение характеристики
1	Состав ИСПДн	MS Office
2	Назначение	Предоставление государственных услуг, обратившимся гражданам. Передача данных в государственные, муниципальные и контролирующие органы
3	Категория обрабатываемых в ИСПДн персональных данных	ИСПДн «Имущественные и земельные отношения» является информационной системой, обрабатывающей иные категории персональных данных, т.е. в ней не обрабатываются специальные категории персональных данных, биометрические персональные данные, общедоступные персональные данные.
4	Объем обрабатываемых ПДн (количество субъектов персональных данных, ПДн которых обрабатываются в ИСПДн)	Объем обрабатываемых в ИСПДн «Имущественные и земельные отношения» персональных данных менее 100000 субъектов персональных данных
5	Субъекты персональных данных	ИСПДн «Имущественные и земельные отношения» является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора персональных данных.
6	Структура ИСПДн	Локальная информационная система (используются комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа).
7	Подключение ИСПДн к сетям связи общего пользования и (или) сетям международного обмена	Имеет подключение к сетям международного информационного обмена.
8	Режим обработки персональных данных	Многопользовательский

9	Разграничение доступа	ИСПДн с разграничением прав доступа.
10	Местонахождение технических средств ИСПДн	Все средства находятся в пределах Российской Федерации.

3. ОПРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИСПДН

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн.

Актуальность угрозы определяется следующими параметрами:

– уровень исходной защищенности ИСПДн;

– частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн. Характеристики ИСПДн «Бухгалтерия» приведены в таблице:

№	Параметр	Значение	Уровень защищенности
1	Территориальное размещение	локальная ИСПДн, развернутая в пределах одного здания	Высокий
2	Наличие соединений с сетями общего пользования	ИСПДн, имеющая одноточечный выход в сеть общего пользования;	Средний
3	Встроенные (легальные) операции с записями баз персональных данных	модификация, передача	Низкий
4	Разграничение доступа к персональным данным	ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	Средний
5	Наличие соединений с другими базами ПДн иных ИСПДн	ИСПДн, в которой используются несколько баз ПДн, принадлежащая организации – владельцу данной ИСПДн	Средний
6	Уровень обобщения (обезличивания) ПДн	ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	Средний
7	Объем ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	ИСПДн, предоставляющая часть ПДн;	Средний

Соотношение характеристик ИСПДн, соответствующих разным уровням защищенности:

– 14% характеристик ИСПДн соответствуют ***высокому*** уровню защищенности;

– 72% характеристик ИСПДн соответствуют ***среднему*** уровню защищенности;

– 14% характеристик ИСПДн соответствуют ***низкому*** уровню защищенности.

Уровень исходной защищенности ИСПДн – средний (Y_1=5).

По каждому виду угрозы, экспертным путем (опрос специалистов) определены:

– опасность (ущерб) в соответствии с правилами, приведенными в таблице 2.

Таблица 2

Опасность (ущерб) угрозы и её характеристики

Опасность (ущерб) угрозы		
Низкая	**Средняя**	**Высокая**
Реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных	Реализация угрозы может привести к негативным последствиям для субъектов персональных данных	Реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных

– вероятность реализации угрозы ($Y_{2)}$ в соответствии с правилами, приведенными в таблице 3.

Таблица 3

Вероятность угрозы и её характеристики

Вероятность	**Y2**
Маловероятно	0
Низкая	2
Средняя	5
Высокая	10

С учетом полученных числовых коэффициентов Y_1 и Y_2 по каждому виду угрозы безопасности ПДн рассчитывается числовой коэффициент реализуемости угрозы Y по формуле:

$$Y = (Y_1 + Y_2)/20$$

Соответствие значения числового коэффициента реализуемости угрозы Y и его возможной реализации приведено в таблице 4.

Таблица 4

Значения реализуемости

Значение числового коэффициента реализуемости угрозы Y	**Возможность реализации угрозы**

Y∈ [0 ; 0.3]	Низкая
Y∈ (0.3 ; 0.6]	Средняя
Y∈ (0.6 ; 0.8]	Высокая
Y∈ (0.8 ; 1]	Очень высокая

Актуальность угрозы безопасности ПДн определяется на основании значения коэффициента реализуемости угрозы (Y) и показателя опасности (ущерба) угрозы по каждому ее виду. Вывод об актуальности угрозы происходит в соответствии с правилами, представленными в таблице 5.

Таблица 5

Актуальность реализации угрозы

Возможность реализации угрозы	**Опасность угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Угрозы и их характеристики представлены в таблице 6.

Таблица угроз и их характеристик приведена ниже.

Наименование угрозы	Вероятность (Y2)	Реализуемость (Y)	Опасность	Актуальность
УГРОЗЫ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ				
Угрозы утечки акустической (речевой) информации	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы утечки видовой информации	низкая вероятность (2)	низкая (0.35)	низкая	неактуальная
Угрозы утечки информации по каналу ПЭМИН	маловероятно (0)	низкая (0.25)	низкая	неактуальная
УГРОЗЫ НСД К ПДн, ОБРАБАТЫВАЕМЫМ НА АВТОМАТИЗИРОВАННОМ РАБОЧЕМ МЕСТЕ				
Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	средняя вероятность (5)	средняя (0.5)	средняя	актуальная
Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование и т.п.) операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ	средняя вероятность (5)	средняя (0.5)	средняя	актуальная
СЕТЕВЫЕ УГРОЗЫ				
Угрозы "Анализа сетевого трафика" с перехватом передаваемой по сети информации	низкая вероятность (2)	низкая (0.35)	низкая	неактуальная
Угрозы выявления паролей	низкая вероятность (2)	низкая (0.35)	средняя	неактуальная
Угрозы удаленного запуска приложений	маловероятно (0)	низкая (0.25)	средняя	неактуальная
Угрозы внедрения по сети вредоносных программ	средняя вероятность (5)	средняя (0.5)	средняя	актуальная
УГРОЗЫ ИЗ ВНЕШНИХ СЕТЕЙ				
Угрозы "Анализа сетевого трафика" с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы выявления паролей	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы получения НСД путем подмены доверенного объекта	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы типа "Отказ в обслуживании"	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы удаленного запуска приложений	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы внедрения по сети вредоносных программ	средняя вероятность (5)	средняя (0.5)	средняя	актуальная

4. МОДЕЛЬ ВЕРОЯТНОГО НАРУШИТЕЛЯ

По наличию права постоянного или разового доступа в ИСПДн нарушители подразделяются на два типа:

- нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена – внешние нарушители;
- нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн – внутренние нарушители.

Внешними нарушителями могут быть:

- криминальные структуры;
- недобросовестные партнеры;
- внешние субъекты (физические лица).

Внешний нарушитель имеет следующие возможности:

- осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
- осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;
- осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
- осуществлять несанкционированные доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами контролируемой зоны.

Категории нарушителей

№	Описание	Нарушитель может	Возможный нарушитель
1	Лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн.	– иметь доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн; – располагать фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах; – располагать именами и вести выявление паролей зарегистрированных пользователей; – изменять конфигурацию технических средств ИСПДн, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн.	Сотрудники, не участвующие в обработке ПДн
2	Зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места.	– обладает всеми возможностями лиц первой категории; – знает по меньшей мере одно легальное имя доступа; – обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн; – располагает конфиденциальными данными, к которым имеет доступ.	Сотрудники, обрабатывающие ПДн
3	Зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам	– обладает всеми возможностями лиц первой и второй категорий; – располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системам, через которую он осуществляет доступ, и составе технических средств ИСПДн; – имеет возможность прямого (физического) доступа к фрагментам технических средств ИСПДн.	Отсутствует
4	Зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн.	– обладает всеми возможностями лиц предыдущих категорий; – обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИСПДн; – обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИСПДн; – имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИСПДн; – имеет доступ ко всем техническим средствам сегмента (фрагмента) ИСПДн; – обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) ИСПДн.	Отсутствует
5	Зарегистрированные пользователи с полномочиями системного администратора ИСПДн	– обладает всеми возможностями лиц предыдущих категорий; – обладает полной информацией о системном и прикладном программном обеспечении ИСПДн; – обладает полной информацией о технических средствах и конфигурации ИСПДн; – имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн; – обладает правами конфигурирования и административной настройки технических средств ИСПДн.	Системный администратор ИСПДн
6	Зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн	– обладает всеми возможностями лиц предыдущих категорий; – обладает полной информацией об ИСПДн; – имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн; – не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).	Администратор безопасности ИСПДн
7	Программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте	– обладает информацией об алгоритмах и программах обработки информации на ИСПДн; – обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения; – может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.	Отсутствует
8	Разработчики и лица, обеспечивающие	– обладает возможностями внесения закладок в технические средства ИСПДн на стадии их	Отсутствует

	поставку, сопровождение и ремонт технических средств на ИСПДн	разработки, внедрения и сопровождения; – может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты информации в ИСПДн.	

5. ВЫВОДЫ

5.1 В результате анализа возможных угроз безопасности персональных данных выявлено 3 актуальные угрозы безопасности:

№ п/п	Угроза	Вероятность	Опасность
	Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	средняя вероятность (5)	средняя
	Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование и т.п.) операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ	средняя вероятность (5)	средняя
	Угрозы внедрения по сети вредоносных программ	средняя вероятность (5)	средняя

5.2 Выявленные актуальные угрозы безопасности ПДн в ИСПДн при их реализации могут привести к незначительным последствиям для субъектов ПДн. Необходимо провести мероприятия по устранению указанных угроз или снижению их уровня.

Приложение № 24
Утвержден
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

Акт
определения уровня защищенности
персональных данных в информационной системе
персональных данных «Имущественные и земельные отношения»
(ИСПДн «Имущественные и земельные отношения»)
Администрации Козловского муниципального округа
Чувашской Республики

г. Козловка 18.12.2024

Комиссия в составе:
Председатель комиссии:

Маркова Анна Александровна	Начальник отдела правового обеспечения и цифрового развития администрации Козловского муниципального округа Чувашской Республики

Члены комиссии:

Васильева Татьяна Леонидовна	Управляющий делами МО - начальник отдела организационно-контрольной и кадровой работы администрации Козловского муниципального округа Чувашской Республики
Пушков Геннадий Михайлович	Заместитель главы администрации МО по экономике и сельскому хозяйству - начальник отдела экономики, инвестиционной деятельности, земельных и имущественных отношений администрации Козловского муниципального округа Чувашской Республики
Комарова Валерия Игоревна	Заведующий сектором опеки и попечительства администрации Козловского муниципального округа Чувашской Республики
Ульданова Анастасия Витальевна	Начальник отдела ЗАГС администрации Козловского муниципального округа Чувашской Республики

рассмотрела следующие исходные данные на информационную систему персональных данных (ИСПДн):

Наименование ИСПДн и состав программного обеспечения, используемого для обработки персональных данных.
ИСПДн «Имущественные и земельные отношения» в составе:
MS Office

Категория обрабатываемых персональных данных.
ИСПДн «Имущественные и земельные отношения» является информационной системой, обрабатывающей специальные категории персональных данных, т.е. в ней обрабатываются персональные данные, касающиеся, национальной принадлежности, состояния здоровья, субъектов персональных данных.

Объем обрабатываемых персональных данных.
Объем обрабатываемых в **ИСПДн «Имущественные и земельные отношения»** персональных данных менее 100000 субъектов персональных данных

Субъекты персональных данных.
ИСПДн «Имущественные и земельные отношения» является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора персональных данных.

Актуальные угрозы безопасности персональных данных.
Для **ИСПДн «Имущественные и земельные отношения»** актуальны угрозы 3-го типа, т.е. угрозы не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Структура информационной системы.
Локальная информационная система (используются комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа).

Подключение информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена.
Имеет подключение к сетям международного информационного обмена.

Режим обработки персональных данных.
Многопользовательский.

Разграничение доступа.
ИСПДн с разграничением прав доступа.

Местонахождение технических средств информационной системы.
Все средства находятся в пределах Российской Федерации.

Заключение комиссии:
В соответствии с пунктом 12 постановления Правительства Российской Федерации от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», признать необходимым обеспечение 4-го уровня защищенности персональных данных при их обработке в ИСПДн «Имущественные и земельные отношения».

Председатель комиссии: _____ _____
Члены комиссии: _____ _____
_____ _____
_____ _____
_____ _____

Приложение № 25
Утверждены
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ПРАВИЛА ОЦЕНКИ ВРЕДА, КОТОРЫЙ МОЖЕТ БЫТЬ ПРИЧИНЕН СУБЪЕКТАМ ПЕРСОНАЛЬНЫХ ДАННЫХ В СЛУЧАЕ НАРУШЕНИЯ ТРЕБОВАНИЙ ПО ОБРАБОТКЕ И ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

г. Козловка
2024 г.

1. Общие положения
1.1. Настоящие Правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных (далее - Правила) определяют порядок оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» (далее - Закон), и отражают соотношение указанного возможного вреда и принимаемых Администрацией Козловского муниципального округа Чувашской Республики (далее – Оператор) мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом.
1.2. Настоящие Правила разработаны в соответствии с действующим законодательством Российской Федерации в области обработки и защиты персональных данных.
2. Основные понятия
2.1. В настоящих Правилах используются основные понятия:
2.1.1. Информация - сведения (сообщения, данные) независимо от формы их представления;
2.1.2. Безопасность информации - состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность;
2.1.3. Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
2.1.4. Целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими право на такое изменение;
2.1.5. Доступность информации - состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно;

2.1.6. Убытки - расходы, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено;
2.1.7. Моральный вред - физические или нравственные страдания, причиняемые действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом;
2.1.8. Оценка возможного вреда - определение уровня вреда на основании учета причиненных убытков и морального вреда, нарушения конфиденциальности, целостности и доступности персональных данных.
3. Методика оценки возможного вреда субъектам персональных данных
3.1. Вред субъекту персональных данных возникает в результате неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.
3.2. Перечисленные неправомерные действия определяются как следующие нарушения безопасности информации:
3.2.1. Неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности персональных данных;
3.2.2. Неправомерное уничтожение и блокирование персональных данных является нарушением доступности персональных данных;
3.2.3. Неправомерное изменение персональных данных является нарушением целостности персональных данных;
3.2.4. Нарушение права субъекта требовать от оператора уточнения его персональных данных, их блокирования или уничтожение является нарушением целостности информации;
3.2.5. Нарушение права субъекта на получение информации, касающейся обработки его персональных данных, является нарушением доступности персональных данных;
3.2.6. Обработка персональных данных, выходящая за рамки установленных и законных целей обработки, в объеме больше необходимого для достижения установленных и законных целей и дольше установленных сроков является нарушением конфиденциальности персональных данных;
3.2.7. Неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных;
3.2.8. Принятие решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающие его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных без согласия на то в письменной форме субъекта персональных данных или непредусмотренное федеральными законами, является нарушением конфиденциальности
персональных данных.
3.3. Субъекту персональных данных может быть причинен вред в форме:
3.3.1. Убытков -расходов, которые лицо, чье право нарушено, понеслоили должно будет понести для восстановления нарушенного права, утраты илиповреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено;
3.3.2. Морального вреда -физических или нравственных страданий, причиняемых действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.
3.4. В оценке возможного вреда Оператор исходит из следующего способа учета последствий допущенного нарушения принципов обработки персональных данных:
3.4.1. Низкий уровень возможного вреда -последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, либо только нарушение доступности персональных данных;
3.4.2. Средний уровень возможного вреда -последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, повлекшее убытки и моральный вред, либо только нарушение доступности персональных данных, повлекшее убытки и моральный вред, либо только нарушение конфиденциальности персональных данных;
3.4.3. Высокий уровень возможного вреда - во всех остальных случаях.
4. Порядок проведения оценки возможного вреда, а также соотнесения возможного вреда и реализуемых Оператором мер
4.1. Оценка возможного вреда субъектам персональных данных осуществляется ответственным за организацию обработки персональных данных, в соответствии с методикой, описанной в разделе 3 настоящих Правил, и на основании экспертных значений, приведенных в Приложении 1.
4.2. Состав реализуемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом, определяется лицом, ответственным в Администрации Козловского муниципального округа Чувашской Республики за организацию обработки персональных данных, исходя из правомерности и разумной достаточности указанных мер.

Приложение 1 к правилам

Оценка вреда, который может быть причинен субъектам персональных данных, а также соотнесение возможного вреда и реализуемых Оператором мер

№ п/п	Требования Федерального закона «О персональных данных», которые могут быть нарушены	Возможные нарушение безопасности информации и причиненный субъекту вред		Уровень возможного вреда	Принимаемые меры по обеспечению выполнения обязанностей оператора персональных данных
1	Порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение	Убытки и моральный вред	+	средний	В соответствии с законодательством в области защиты информации и Положением об обработке персональных данных
		Целостность	-		
		Доступность	-		
		Конфиденциальность	+		

	которых обеспечивает установленные уровни защищенности персональных данных;				
2	Порядок и условия применения средств защиты информации;	Убытки и моральный вред	+	средний	В соответствии с технической документацией на систему защиты ИСПДн
		Целостность	+		
		Доступность			
		Конфиденциальность			
3	Эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;	Убытки и моральный вред	+	высокий	Проведение проверки эффективности мер защиты ИСПДн
		Целостность	+		
		Доступность	+		
		Конфиденциальность	+		
4	Состояние учета машинных носителей персональных данных;	Убытки и моральный вред		низкий	Журнал учета машинных носителей персональных данных
		Целостность	+		
		Доступность			
		Конфиденциальность			
5	Соблюдение правил доступа к персональным данным;	Убытки и моральный вред	+	высокий	В соответствии с принятыми организационными мерами и в соответствии с системой разграничения доступа
		Целостность	+		
		Доступность			
		Конфиденциальность	+		
6	Наличие(отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;	Убытки и моральный вред	+	средний	Мониторинг средств защиты информации на наличие фактов доступа к ПДн
		Целостность			
		Доступность			
		Конфиденциальность	+		
7	Мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;	Убытки и моральный вред		низкий	Применение резервного копирования
		Целостность	+		
		Доступность	+		
		Конфиденциальность			
8	Осуществление мероприятий по обеспечению целостности персональных данных.	Убытки и моральный вред		низкий	Организация режима доступа к техническим и программным средствам
		Целостность	+		
		Доступность			
		Конфиденциальность			

Приложение № 26
Утвержден
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

Акт
определения уровня защищенности
персональных данных в информационной системе
персональных данных «ЗАГС» (ИСПДн «ЗАГС»)
Администрации Козловского муниципального округа Чувашской Республики

г. Козловка 18.12.2024

Комиссия в составе:

Председатель комиссии:	
Маркова Анна Александровна	Начальник отдела правового обеспечения и цифрового развития администрации Козловского муниципального округа Чувашской Республики
Члены комиссии:	
Васильева Татьяна Леонидовна	Управляющий делами МО - начальник отдела организационно-контрольной и кадровой работы администрации Козловского муниципального округа Чувашской Республики
Пушков Геннадий Михайлович	Заместитель главы администрации МО по экономике и сельскому хозяйству - начальник отдела экономики, инвестиционной деятельности, земельных и имущественных отношений администрации Козловского муниципального округа Чувашской Республики
Комарова Валерия Игоревна	Заведующий сектором опеки и попечительства администрации Козловского муниципального округа Чувашской Республики
Ульданова Анастасия Витальевна	Начальник отдела ЗАГС администрации Козловского муниципального округа Чувашской Республики

рассмотрела следующие исходные данные на информационную систему персональных данных (ИСПДн):

Наименование ИСПДн и состав программного обеспечения, используемого для обработки персональных данных.
ИСПДн «ЗАГС» в составе:
МАИС «ЗАГС»

Категория обрабатываемых персональных данных.
ИСПДн «ЗАГС» является информационной системой, обрабатывающей специальные категории персональных данных, т.е. в ней обрабатываются персональные данные, касающиеся, национальной принадлежности, состояния здоровья, субъектов персональных данных.

Объем обрабатываемых персональных данных.
Объем обрабатываемых в **ИСПДн «ЗАГС»** персональных данных менее 100000 субъектов персональных данных

Субъекты персональных данных.
ИСПДн «ЗАГС» является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора персональных данных.

Актуальные угрозы безопасности персональных данных.
Для **ИСПДн «ЗАГС»** актуальны угрозы 3-го типа, т.е. угрозы не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Структура информационной системы.
Локальная информационная система (используются комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа).

Подключение информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена.
Имеет подключение к сетям международного информационного обмена.

Режим обработки персональных данных.
Многопользовательский.

Разграничение доступа.
ИСПДн с разграничением прав доступа.

Местонахождение технических средств информационной системы.
Все средства находятся в пределах Российской Федерации.

Заключение комиссии:
В соответствии с пунктом 12 постановления Правительства Российской Федерации от 1 ноября 2012 г. №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», признать необходимым обеспечение 3-го уровня защищенности персональных данных при их обработке в ИСПДн «ЗАГС».

Председатель комиссии: _____ _____
Члены комиссии: _____ _____
_____ _____
_____ _____
_____ _____

Приложение № 27
Утверждено
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

Техническое задание на создание системы защиты для информационных систем персональных данных «ЗАГС»

г. Козловка
2024 г.

СПИСОК СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

АВС	– антивирусные средства
АРМ	– автоматизированное рабочее место
АС	– автоматизированная система
АСЗИ	– автоматизированная система в защищенном исполнении
ИСПДн	– информационная система персональных данных
ЛВС	– локальная вычислительная сеть
МЭ	– межсетевой экран
ОС	– операционная система
ПДн	– персональные данные
ПМВ	– программно-математическое воздействие
ПО	– программное обеспечение
ПЭМИН	– побочные электромагнитные излучения и наводки
САЗ	– система анализа защищенности
СЗИ	– средства защиты информации
СЗПДн	– система (подсистема) защиты персональных данных
СКЗИ	– средства криптографической защиты информации
СОВ	– система обнаружения вторжений
ТС	– техническое средство
УБПДн	– угрозы безопасности персональных данных

НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Настоящий документ составлен в соответствии со следующими действующими нормативно-методическими документами в области защиты персональных данных:
[1] – Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
[2] – Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
[3] – Постановление Правительства Российской Федерации об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных от 1 ноября 2012 г.№1119;
[4] –Приказ ФСТЭК от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных
[5] – Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 15 февраля 2008г. заместителем директора ФСТЭК России).

ОБОСНОВАНИЕ РАЗРАБОТКИ СИСТЕМЫ ЗАЩИТЫ

В информационных системах «ЗАГС» предполагается обработка персональных данных. Информационная системы «ЗАГС» попадает под действие закона [2]. В соответствии с [3] требуется обеспечить безопасность персональных данных. Безопасность персональных данных обеспечивается выполнением комплекса организационных и технических мер защиты, которые определяются в соответствии с нормативно-методическими документами ФСТЭК России и ФСБ России.
Система защиты должна разрабатываться с целью предотвращения ущерба от возможной реализации нарушений характеристик безопасности. Угрозы безопасности определены в «Модели угроз информационной системы» (далее Модель угроз).
Настоящий документ разработан для решения следующих задач:
– разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;
– создание регламента проведения мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
– недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
– создание регламента мероприятий, обеспечивающих контроль за обеспечением уровня защищенности персональных данных.

ИСХОДНЫЕ ДАННЫЕ

Описание информационной системы персональных данных «ЗАГС» приведено в Модели угроз.
Перечень требований безопасности персональных данных, предусмотренный нормативно-методическими документами для ИСПДн с заданными параметрами представлен в таблице.
Защита информации от выявленных угроз сводится к принятию организационных и технических мер, которые позволяют избавиться от тех или иных компонентов угроз.

В таблице представлен список требований, которые нужно выполнить для нейтрализации угроз данной ИСПДн.

№ п/п	Требование
1	**2**
1.	фильтрация на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов)
2.	идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия
3.	регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана)
4.	контроль целостности программной и информационной части межсетевого экрана
5.	фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств
6.	восстановление свойств межсетевого экрана после сбоев и отказов оборудования
7.	регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления
8.	использование средств антивирусной защиты
9.	использование в составе информационной системы программных или программно-аппаратных средств (систем) анализа защищенности. Средства (системы) анализа защищенности должны обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атаки на систему
10.	использование в составе информационной системы программных или программно-аппаратных средств (систем) обнаружения вторжений
11.	Для выбора и реализации методов и способов защиты информации в информационной системе оператором или уполномоченным лицом требуется назначить структурное подразделение или должностное лицо (работника), ответственные за обеспечение безопасности персональных данных
12.	обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними
13.	учет лиц, допущенных к работе с персональными данными в информационной системе; лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного оператором или уполномоченным лицом
14.	разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений
15.	регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы
16.	при регистрации входа (выхода) пользователя в систему (из системы) либо регистрации загрузки и инициализации операционной системы и ее программного останова в параметрах регистрации дополнительно указывается результат попытки входа (успешная или неуспешная)
17.	при регистрации входа (выхода) пользователя в систему (из системы) либо регистрации загрузки и инициализации операционной системы и ее программного останова в параметрах регистрации дополнительно указывается идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа
18.	учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме)
19.	размещение устройств вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы, в помещениях, в которых они установлены, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные
20.	идентификация и проверка подлинности пользователя при входе в систему информационной системы по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов
21.	при идентификации и проверке подлинности пользователя при входе в систему должен дополнительно использоваться идентификатор (код)
22.	физическая охрана информационной системы (технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации
23.	периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа
24.	наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности
25.	обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по контрольным суммам компонентов средств защиты информации, а целостность

№ п/п	Требование
1	2
	программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации
26.	физическая охрана технических средств информационных систем (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания

ПЕРЕЧЕНЬ ПРЕДЛАГАЕМЫХ К ИСПОЛЬЗОВАНИЮ СЕРТИФИЦИРОВАННЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

В данном разделе представлены средства защиты информации для реализации технических мер защиты. Специалисты оператора оставляют за собой право выбора тех или иных средств защиты, исходя из особенностей работы информационной системы.

№ п/п	Тип СЗИ	СЗИ	Описание СЗИ	Сертификат
1.	сертифицированные средства защиты информации от несанкционированного доступа	Блокхост-Сеть	Средство защиты информации от несанкционированного доступа; производитель: ООО «Газинформсервис»	ФСТЭК, №1517, от 30.11.2007
2.	сертифицированные средства защиты информации от несанкционированного доступа	Secret Net 5.1	Средство защиты информации от несанкционированного доступа; производитель: ООО «Код Безопасности»	ФСТЭК, №1912, от 17.09.2009
3.	сертифицированные средства защиты информации от несанкционированного доступа	Dallas Lock 7.5	Средство защиты информации от несанкционированного доступа; производитель ООО «Конфидент»	ФСТЭК, №1685, от 18.09.2008
4.	сертифицированные средства защиты информации от несанкционированного доступа	Страж NT 3.0	Средство защиты информации от несанкционированного доступа; производитель: ЗАО «НПЦ «Модуль»	ФСТЭК, №2145, от 30.07.2010
5.	сертифицированные средства защиты информации от несанкционированного доступа	Dr.Web Enterprise Security Suite	Средство защиты информации от несанкционированного доступа; производитель: «Доктор Веб»	ФСТЭК, №2446, от 20.09.2011
6.	сертифицированные средства защиты информации от несанкционированного доступа	Security Studio	Средство защиты информации от несанкционированного доступа; производитель: ООО «Код Безопасности»	ФСТЭК, №1597, от 24.04.2008

Допускается применение прочих сертифицированных средств защиты информации, если это требуется исходя из особенностей функционирования системы. Полный реестр сертифицированных средств защиты информации представлен на сайте ФСТЭК России.

Приложение № 28
Утверждена
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ЧАСТНАЯ МОДЕЛЬ АКТУАЛЬНЫХ УГРОЗ
И ВЕРОЯТНОГО НАРУШИТЕЛЯ
информационной системы персональных данных
«ЗАГС»

Маркова Анна Александровна
Начальник отдела правового обеспечения и цифрового развития администрации Козловского муниципального округа Чувашской Республики _____ подпись _____ дата

Васильева Татьяна Леонидовна
Управляющий делами МО - начальник отдела организационно-контрольной и кадровой работы администрации Козловского муниципального округа Чувашской Республики _____ подпись _____ дата

Пушков Геннадий Михайлович
Заместитель главы администрации МО по экономике и сельскому хозяйству - начальник отдела экономики, инвестиционной деятельности, земельных и имущественных отношений администрации Козловского муниципального округа Чувашской Республики _____ подпись _____ дата

Комарова Валерия Игоревна
Заведующий сектором опеки и попечительства администрации Козловского муниципального округа Чувашской Республики _____ подпись _____ дата

Ульданова Анастасия Витальевна
Начальник отдела ЗАГС администрации Козловского муниципального округа Чувашской Республики _____ подпись _____ дата

г. Козловка
2024 г.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.
Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.
Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
Вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.
Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.
Доступ в операционную среду компьютера (информационной системы персональных данных) - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.
Доступ к информации – возможность получения информации и ее использования.
Закладочное устройство - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).
Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.
Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.
Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.
Носитель информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.
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.
Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
Побочные электромагнитные излучения и наводки - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.
Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.
Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
Программная закладка - скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.
Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.
Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.
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.
Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.
Уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности ПДн.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ – автоматизированное рабочее место;
ВТСС – вспомогательные технические средства и системы;
ИСПДн – информационная система персональных данных;
КЗ – контролируемая зона;
НДВ – недекларированные возможности;
НСД – несанкционированный доступ;
ОБПДн – обеспечение безопасности персональных данных;
ОС – операционная система;
ПДн – персональные данные;
ПМВ – программно-математическое воздействие;
ПЭМИН – побочные электромагнитные излучения и наводки;
СВТ – средство вычислительной техники;
СЗИ – средство защиты информации;
СЭУПИ – специальные электронные устройства перехвата информации;
УБПДн – угрозы безопасности персональных данных.

1.ОБЩИЕ ПОЛОЖЕНИЯ

Частная модель актуальных угроз Администрации Козловского муниципального округа Чувашской Республики (далее Оператор) разработана в соответствии с нормативными документами ФСТЭК России:

- Базовая модель безопасности персональных данных при их обработке в информационных системах персональных данных, 2008г.;

Частная модель угроз содержит описание возможных угроз безопасности персональных данных и расчет актуальных угроз для ИСПДн Оператора.

Частная модель угроз направлена на определение возможных каналов утечки, путем анализа защищенности ИСПДн Оператора.

Под угрозами безопасности ПДн при их обработке в ИСПДн понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

В соответствии со статьей 19 Федерального закона №152-ФЗ от 27 июля 2006 г. «О персональных данных», ПДн должны быть защищены от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн и(или) потребителей, пользующихся услугами, предоставляемыми ИСПДн в соответствии с ее назначением, так и со специально осуществляемыми неправомерными действиями иностранных государств, криминальных сообществ, отдельных организаций и граждан, а также иными источниками угроз.

Угрозы безопасности ПДн могут быть реализованы за счет утечки ПДн по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах ИСПДн, технические каналы перехвата информации при ее передаче по каналам связи, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа с использованием соответствующего программного обеспечения.

2. ОПИСАНИЕ ИСПДН

2.1. Общие характеристики ИСПДн приведены в Таблице 1

№ п/н	Характеристика	Значение характеристики
1	Состав ИСПДн	МАИС «ЗАГС»
2	Назначение	Предоставление государственных услуг, обратившимся гражданам. Передача данных в государственные, муниципальные и контролирующие органы
3	Категория обрабатываемых в ИСПДн персональных данных	ИСПДн «ЗАГС» является информационной системой, обрабатывающей специальные категории персональных данных, т.е. в ней обрабатываются персональные данные, касающиеся, национальной принадлежности, состояния здоровья, субъектов персональных данных
4	Объем обрабатываемых ПДн (количество субъектов персональных данных, ПДн которых обрабатываются в ИСПДн)	Объем обрабатываемых в ИСПДн «ЗАГС» персональных данных менее 100000 субъектов персональных данных
5	Субъекты персональных данных	ИСПДн «ЗАГС» является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора персональных данных.
6	Структура ИСПДн	Локальная информационная система (используются комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа).
7	Подключение ИСПДн к сетям связи общего пользования и (или) сетям международного обмена	Имеет подключение к сетям международного информационного обмена.
8	Режим обработки персональных данных	Многопользовательский
9	Разграничение доступа	ИСПДн с разграничением прав доступа.
10	Местонахождение технических средств ИСПДн	Все средства находятся в пределах Российской Федерации.

3. ОПРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИСПДН

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн.

Актуальность угрозы определяется следующими параметрами:

– уровень исходной защищенности ИСПДн;

– частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн. Характеристики ИСПДн «Бухгалтерия» приведены в таблице:

№	Параметр	Значение	Уровень защищенности
1	Территориальное размещение	локальная ИСПДн, развернутая в пределах одного здания	Высокий
2	Наличие соединений с сетями общего	ИСПДн, имеющая одноточечный выход в сеть	Средний

	пользования	общего пользования;	
3	Встроенные (легальные) операции с записями баз персональных данных	модификация, передача	Низкий
4	Разграничение доступа к персональным данным	ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	Средний
5	Наличие соединений с другими базами ПДн иных ИСПДн	ИСПДн, в которой используются несколько баз ПДн, принадлежащая организации – владельцу данной ИСПДн	Средний
6	Уровень обобщения (обезличивания) ПДн	ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	Средний
7	Объем ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	ИСПДн, предоставляющая часть ПДн;	Средний

Соотношение характеристик ИСПДн, соответствующих разным уровням защищенности:
- 14% характеристик ИСПДн соответствуют ***высокому*** уровню защищенности;
- 72% характеристик ИСПДн соответствуют ***среднему*** уровню защищенности;
- 14% характеристик ИСПДн соответствуют ***низкому*** уровню защищенности.

Уровень исходной защищенности ИСПДн – средний (Y_1=5).

По каждому виду угрозы, экспертным путем (опрос специалистов) определены:
- опасность (ущерб) в соответствии с правилами, приведенными в таблице 2.

Таблица 2

Опасность (ущерб) угрозы и её характеристики

Опасность (ущерб) угрозы		
Низкая	**Средняя**	**Высокая**
Реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных	Реализация угрозы может привести к негативным последствиям для субъектов персональных данных	Реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных

- вероятность реализации угрозы ($Y_{2)}$ в соответствии с правилами, приведенными в таблице 3.

Таблица 3

Вероятность угрозы и её характеристики

Вероятность	**Y2**
Маловероятно	0
Низкая	2
Средняя	5
Высокая	10

С учетом полученных числовых коэффициентов Y_1 и Y_2 по каждому виду угрозы безопасности ПДн рассчитывается числовой коэффициент реализуемости угрозы Y по формуле:

$$Y = (Y_1 + Y_2)/20$$

Соответствие значения числового коэффициента реализуемости угрозы Y и его возможной реализации приведено в таблице 4.

Таблица 4

Значения реализуемости

Значение числового коэффициента реализуемости угрозы Y	**Возможность реализации угрозы**
YЄ [0 ; 0.3]	Низкая
YЄ (0.3 ; 0.6]	Средняя
YЄ (0.6 ; 0.8]	Высокая
YЄ (0.8 ; 1]	Очень высокая

Актуальность угрозы безопасности ПДн определяется на основании значения коэффициента реализуемости угрозы (Y) и показателя опасности (ущерба) угрозы по каждому ее виду. Вывод об актуальности угрозы происходит в соответствии с правилами, представленными в таблице 5.

Таблица 5

Актуальность реализации угрозы

Возможность реализации угрозы	**Опасность угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная

Очень высокая	актуальная	актуальная	актуальная

Угрозы и их характеристики представлены в таблице 6.

Таблица угроз и их характеристик приведена ниже.

Наименование угрозы	Вероятность (Y2)	Реализуемость (Y)	Опасность	Актуальность
УГРОЗЫ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ				
Угрозы утечки акустической (речевой) информации	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы утечки видовой информации	низкая вероятность (2)	низкая (0.35)	низкая	неактуальная
Угрозы утечки информации по каналу ПЭМИН	маловероятно (0)	низкая (0.25)	низкая	неактуальная
УГРОЗЫ НСД К ПДн, ОБРАБАТЫВАЕМЫМ НА АВТОМАТИЗИРОВАННОМ РАБОЧЕМ МЕСТЕ				
Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	средняя вероятность (5)	средняя (0.5)	средняя	актуальная
Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование и т.п.) операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ	средняя вероятность (5)	средняя (0.5)	средняя	актуальная
СЕТЕВЫЕ УГРОЗЫ				
Угрозы "Анализа сетевого трафика" с перехватом передаваемой по сети информации	низкая вероятность (2)	низкая (0.35)	низкая	неактуальная
Угрозы выявления паролей	низкая вероятность (2)	низкая (0.35)	средняя	неактуальная
Угрозы удаленного запуска приложений	маловероятно (0)	низкая (0.25)	средняя	неактуальная
Угрозы внедрения по сети вредоносных программ	средняя вероятность (5)	средняя (0.5)	средняя	актуальная
УГРОЗЫ ИЗ ВНЕШНИХ СЕТЕЙ				
Угрозы "Анализа сетевого трафика" с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы выявления паролей	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы получения НСД путем подмены доверенного объекта	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы типа "Отказ в обслуживании"	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы удаленного запуска приложений	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы внедрения по сети вредоносных программ	средняя вероятность (5)	средняя (0.5)	средняя	актуальная

4. МОДЕЛЬ ВЕРОЯТНОГО НАРУШИТЕЛЯ

По наличию права постоянного или разового доступа в ИСПДн нарушители подразделяются на два типа:

- нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена – внешние нарушители;
- нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн – внутренние нарушители.

Внешними нарушителями могут быть:

- криминальные структуры;
- недобросовестные партнеры;
- внешние субъекты (физические лица).

Внешний нарушитель имеет следующие возможности:

- осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
- осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;
- осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
- осуществлять несанкционированные доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами контролируемой зоны.

Категории нарушителей

№	Описание	Нарушитель может	Возможный нарушитель
1	Лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн.	- иметь доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн; - располагать фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах; - располагать именами и вести выявление паролей зарегистрированных пользователей; - изменять конфигурацию технических средств ИСПДн, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн.	Сотрудники, не участвующие в обработке ПДн
2	Зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места.	- обладает всеми возможностями лиц первой категории; - знает по меньшей мере одно легальное имя доступа; - обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн; - располагает конфиденциальными данными, к которым имеет доступ.	Сотрудники, обрабатывающие ПДн
3	Зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам	- обладает всеми возможностями лиц первой и второй категорий; - располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системам, через которую он осуществляет доступ, и составе технических средств ИСПДн; - имеет возможность прямого (физического) доступа к фрагментам технических средств ИСПДн.	Отсутствует
4	Зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн.	- обладает всеми возможностями лиц предыдущих категорий; - обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИСПДн; - обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИСПДн; - имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИСПДн; – имеет доступ ко всем техническим средствам сегмента (фрагмента) ИСПДн; – обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) ИСПДн.	Отсутствует
5	Зарегистрированные пользователи с полномочиями системного администратора ИСПДн	– обладает всеми возможностями лиц предыдущих категорий; – обладает полной информацией о системном и прикладном программном обеспечении ИСПДн; – обладает полной информацией о технических средствах и конфигурации ИСПДн; – имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн; – обладает правами конфигурирования и административной настройки технических средств ИСПДн.	Системный администратор ИСПДн
6	Зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн	– обладает всеми возможностями лиц предыдущих категорий; – обладает полной информацией об ИСПДн; – имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн; – не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).	Администратор безопасности ИСПДн
7	Программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте	– обладает информацией об алгоритмах и программах обработки информации на ИСПДн; – обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;	Отсутствует

		– может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.	
8	Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн	– обладает возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения; – может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты информации в ИСПДн.	Отсутствует

5. ВЫВОДЫ

5.1 В результате анализа возможных угроз безопасности персональных данных выявлено 3 актуальные угрозы безопасности:

№ п/п	Угроза	Вероятность	Опасность
1	Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	средняя вероятность (5)	средняя
2	Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование и т.п.) операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ	средняя вероятность (5)	средняя
3	Угрозы внедрения по сети вредоносных программ	средняя вероятность (5)	средняя

5.2 Выявленные актуальные угрозы безопасности ПДн в ИСПДн при их реализации могут привести к незначительным последствиям для субъектов ПДн. Необходимо провести мероприятия по устранению указанных угроз или снижению их уровня.

Приложение № 29
Утверждена
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ИНСТРУКЦИЯ
АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ (ИСПДН) «ЗАГС»

г. Козловка
2024 г.

1. Общие положения

1.1. Администратор ИСПДн «ЗАГС» (далее Администратор) назначается распоряжением Администрации Козловского муниципального округа Чувашской Республики (далее Администрация).
1.2. Администратор подчиняется Главе Козловского муниципального округа Чувашской Республики.
1.3. Администратор в своей работе руководствуется настоящей инструкцией, Политикой информационной безопасности, а также другими руководящими и нормативными документами ФСТЭК России и регламентирующими документами Общества.
1.4. Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, при обработке персональных данных.
1.5. Методическое руководство работой Администратора осуществляется ответственным за обеспечение защиты персональных данных.

2. Должностные обязанности

Администратор обязан:
2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.
2.2. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:
программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное программное обеспечение);
аппаратных средств;
аппаратных и программных средств защиты.
2.3. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.
2.4. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.
2.5. Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.
2.6. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.
2.7. Проводить периодический контроль принятых мер по защиты, в пределах возложенных на него функций.
2.8. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля Оператором ИСПДн.
2.9. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.
2.10. Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.
2.11. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.
2.12. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие специальные исследования и специальную проверку.
2.13. Присутствовать при выполнении технического обслуживания элементов ИСПДн, сторонними физическими людьми и организациями.
2.14. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

3. Права

Администратор имеет право:
3.1. Знакомиться с проектами распоряжений и постановлений Администрации Козловского муниципального округа Чувашской Республики касающихся его деятельности.
3.2. Вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с предусмотренными настоящей инструкцией обязанностями.
3.3. В пределах своей компетенции сообщать своему непосредственному руководителю о всех выявленных в процессе осуществления должностных обязанностей недостатках в деятельности организации (его структурных подразделениях) и вносить предложения по их устранению.
3.4. Запрашивать лично или по поручению своего непосредственного руководителя от специалистов подразделений информацию и документы, необходимые для выполнения его должностных обязанностей.

3.5. Привлекать специалистов всех (отдельных) структурных подразделений к решению задач, возложенных на него (если это предусмотрено положениями о структурных подразделениях, если нет — то с разрешения их руководителей).
3.6. Требовать от своего непосредственного руководителя оказания содействия в исполнении им своих должностных обязанностей и прав.

4. Ответственность

Администратор несет ответственность:
4.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией — в пределах, определенных действующим трудовым законодательством Российской Федерации.
4.2. За правонарушения, совершенные в процессе осуществления своей деятельности — в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.
4.3. За причинение материального ущерба — в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.
4.4. За разглашение конфиденциальной информации, содержащей персональные данные – в пределах, определенных действующим административным, уголовным, трудовым и гражданским законодательством РФ.
4.4.1. Администратор ИСПДн, получающий доступ к конфиденциальной информации, содержащей персональные данные, несет персональную ответственность за сохранность носителя и конфиденциальность информации.

С инструкцией ознакомлен (а) и обязуюсь хранить на рабочем месте

_____ _____
(фамилия, инициалы) (подпись)
«____» _____20__ г.

Один экземпляр инструкции на руки получил

_____ _____
(фамилия, инициалы) (подпись)
«____» _____20__ г.

Инструкция разработана:

Начальник отдела правового обеспечения
и цифрового развития администрации
Козловского муниципального округа
Чувашской Республики _____ / _____

Приложение № 30
Утвержден
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ПОРЯДОК
УНИЧТОЖЕНИЯ ПДН, ОБРАБОТКА КОТОРЫХ ОСУЩЕСТВЛЯЕТСЯ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

АДМИНИСТРАЦИИ КОЗЛОВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА ЧУВАШСКОЙ РЕСПУБЛИКИ

г. Козловка
2024г.

Основные термины и определения

1.1. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
1.2. 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.
1.3. Основные технические средства и системы – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи персональных данных.
1.4. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.
1.5. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

1.6. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
1.7. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
1.8. 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.

Общие положения

2.1. Настоящий Порядок уничтожения ПДн, обработка которых осуществляется без использования средств автоматизации (далее – Порядок), разработан в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативными правовыми актами (методическими документами) федеральных органов исполнительной власти по вопросам безопасности ПДн.
2.2. Настоящий Порядок определяет основные принципы уничтожения ПДн обработка которых осуществляется без использования средств автоматизации.
2.3. Порядок обязателен для исполнения всеми работниками Администрации Козловского муниципального округа Чувашской Республики (далее – Администрации), непосредственно участвующими в обработке ПДн без использования средств автоматизации.

Обеспечение безопасности персональных данных

3.1. ПДн при их неавтоматизированной обработке должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн, в специальных разделах или на полях форм.
3.2. Не допускается хранение ПДн различных категорий на одном материальном носителе.
3.3. Не допускается фиксация на одном бумажном носителе ПДн, цели обработки которых заведомо не совместимы.
3.4. Должно обеспечиваться раздельное хранение материальных носителей, содержащих ПДн, обработка которых осуществляется в различных целях.
3.5. При несовместимости целей неавтоматизированной обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности:
- при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн, осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, используется (распространяется) копия ПДн;
- при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

3.6. Работники Администрации, осуществляющие неавтоматизированную обработку ПДн, имеют допуск к обработке ПДн в соответствии с распоряжением Главы Козловского муниципального округа Чувашской Республики «Об утверждении лиц, имеющих доступ к персональным данным».
3.7. Необходимо принимать организационные (охрана помещений) и технические меры, исключающие возможность несанкционированного доступа к материальным носителям ПДн.
3.8. Администрация не передает материальные носители персональных данных любым лицам, без письменного согласия субъектов ПДн, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта ПДн, а также в иных случаях, предусмотренных законодательством Российской Федерации.
3.9. При передаче материальных носителей, содержащих ПДн, третьей стороне должны быть приняты меры, исключающие возможность несанкционированного доступа к ПДн.
3.10. При передаче материальных носителей, содержащих ПДн, третьей стороне должно быть подготовлено сопроводительное письмо, в котором зафиксирован состав передаваемых материальных носителей, с указанием количества страниц для бумажных носителей, с указанием степени конфиденциальности (если необходимо).
3.11. О факте передачи/приема материальных носителей, содержащих ПДн, делаются соответствующие записи в журналах учета исходящей/входящей корреспонденции.
3.12. При приеме материальных носителей, содержащих ПДн, должны быть приняты меры, обеспечивающие их сохранность. При приеме бумажных носителей работа с такими носителями должна быть организована, в соответствии с принципом конфиденциального делопроизводства, действующего в Администрации.

Хранение персональных данных

4.1. При хранении материальных носителей ПДн должны соблюдаться условия, обеспечивающие сохранность ПДн, исключающие несанкционированный к ним доступ.
4.2. Материальные носители ПДн должны храниться в пределах контролируемой зоны.
4.3. Территория контролируемой зоны определяется распоряжением Главы Козловского муниципального округа Чувашской Республики.
4.4. Запрещен вынос или копирование носителей ПДн.
4.5. В нерабочее время и время отсутствия необходимости использования ПДн материальные носители ПДн должны храниться в хранилищах материальных носителей ПДн.
4.6. Перечень мест хранения носителей ПДн утверждается распоряжением Главы Козловского муниципального округа Чувашской Республики.

Уничтожение персональных данных

5.1. Уничтожение ПДн – действия, в результате которых становится невозможным восстановить содержание ПДн и (или) в результате которых уничтожаются материальные носители ПДн.
5.2. Уничтожение носителей ПДн осуществляется в течение 30 дней с момента отзыва субъектом ПДн согласия на обработку ПДн (если более короткий срок не предусмотрен соответствующим договором, стороной которого является Администрация) или истечения сроков обработки ПДн, в том числе хранения в архивах.

5.3. Уничтожением бумажных носителей ПДн занимается комиссия по обеспечению безопасности ПДн, создаваемая распоряжением Главы Козловского муниципального округа Чувашской Республики.
5.4. Бумажные носители ПДн (документы, их копии, выписки), уничтожаются путём измельчения на мелкие части, исключающие возможность последующего восстановления информации, или сжигаются.
5.5. По окончании уничтожения бумажных носителей ПДн комиссией составляется «Акт уничтожении персональных данных», форма которого установлена в Приложении 7 к Положению об обработке персональных данных Администрации Козловского муниципального округа Чувашской Республики.
5.6. Комиссия составляет и подписывает в двух экземплярах соответствующий «Акт уничтожении персональных данных». В течение трех дней после составления акт направляется на утверждение Главе Козловского муниципального округа Чувашской Республики. После утверждения один экземпляр акта остается у ответственного за организацию обработки ПДн, второй экземпляр передается в архив на хранение.

Ответственность

6.1. Ответственность за надлежащее и своевременное выполнение функций, предусмотренных настоящим порядком, несет ответственный за организацию обработки ПДн в Администрации.
6.2. На ответственного за организацию обработки ПДн в Администрации возлагается персональная ответственность за:
- создание надлежащих условий для использования документов;
- сохранность документов.

Срок действия и порядок внесения изменений

7.1. Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно, до замены его новым Положением.
Изменения и дополнения в настоящее Положение вносятся распоряжением Главы Козловского муниципального округа Чувашской Республики.

Приложение № 31
Утвержден
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

РЕГЛАМЕНТ
РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

АДМИНИСТРАЦИИ КОЗЛОВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА ЧУВАШСКОЙ РЕСПУБЛИКИ

г. Козловка
2024г.

1. Термины и определения

1.1. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
1.2. Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Инцидентами информационной безопасности являются:
- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по информационной безопасности;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

1.3. 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.
1.4. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
1.5. Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящий Регламент реагирования на инциденты информационной безопасности в информационных системах персональных данных Администрации Козловского муниципального округа Чувашской Республики (далее – регламент), разработан в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативно-методическими документами федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).
2.2. Настоящий Регламент определяет:

– порядок регистрации событий безопасности;
– порядок выявления инцидентов информационной безопасности и реагированию на них;
– порядок проведения анализа инцидентов информационной безопасности, в том числе определение источников и причин возникновения инцидентов.

2.3. Регламент обязателен для исполнения всеми работниками (далее –Администрация), непосредственно осуществляющими защиту ПДн в ИСПДн.

3. Инциденты информационной безопасности

3.1. К инцидентам ИБ относятся:
– несоблюдение требований по защите ПДн:
– использование ЭВМ в целях, не связанных с выполнением трудовых (служебных, должностных, функциональных) обязанностей;
– утрата носителя ПДн;
– утрата ключевых документов, ключей от помещений и хранилищ, личных печатей, удостоверений, пропусков.
– попытки НСД к ПДн:
– подбор чужого идентификатора и пароля, последующий доступ с использованием чужого пароля;
– изменение настроек, состава, паролей технических средств ИСПДн;
– изменение (увеличение) полномочий доступа;
– нарушение целостности установленных защитных пломб;
– копирование ПДн на неучтенные съемные носители ПДн;
– заражение рабочего места и/или сервера ИСПДн вредоносной программой;
– хищение носителей ПДн;
– хищение технических средств ИСПДн;
– умышленное нарушение работоспособности технических средств ИСПДн;
– хищение криптосредств, ключевых документов, ключей от помещений и хранилищ, личных печатей, удостоверений, пропусков;
– несанкционированное проникновение в помещения ИСПДн;
– очистка электронных журналов мониторинга.
– сбои в работе технических средств ИСПДн Общества.

3.2. К инцидентам ИБ не относятся:
– неудачные попытки вторжений, которые были обнаружены и нейтрализованы с использованием СЗИ;
– неудачные попытки заражения рабочих мест и/или серверов ИСПДн вредоносной программой, которые были обнаружены и нейтрализованы с использованием СЗИ

4. Порядок регистрации событий безопасности

4.1. Регистрация событий безопасности в ИСПДн осуществляется в следующей последовательности:
1) Определение событий безопасности, подлежащих регистрации, и сроков их хранения.
2) Определение состава и содержания информации о событиях безопасности, подлежащих регистрации.
3) Сбор, запись и хранение информации о событиях безопасности.
4) Защита информации о событиях безопасности.

4.2. События безопасности, подлежащие регистрации в ИСПДн, должны определяться с учетом способов реализации угроз безопасности ПДн для ИСПДн. К событиям безопасности, подлежащим регистрации в ИСПДн, должны быть отнесены любые проявления состояния ИСПДн и ее системы защиты, указывающие на возможность нарушения конфиденциальности, целостности или доступности ПДн, доступности компонентов ИСПДн, нарушения процедур, установленных организационно-распорядительными документами по защите ПДн, а также на нарушение штатного функционирования средств защиты информации (далее – СЗИ).

4.3. События безопасности, подлежащие регистрации в ИСПДн, и сроки хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов информационной безопасности, возникших в ИСПДн.

4.4. В ИСПДн подлежат регистрации следующие события:
– вход (выход), а также попытки входа субъектов доступа в ИСПДн и загрузки (остановка) операционной системы;
– подключение съемных машинных носителей ПДн и вывод ПДн на носители;
– запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой ПДн;
– обновление или ошибки при обновлении программных средств ИСПДн и СЗИ;
– попытки доступа программных средств к определяемым защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;
– попытки удаленного доступа.

4.5. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъекта доступа (пользователя и (или) процесса), связанного с данным событием безопасности.

4.6. При регистрации входа (выхода) субъектов доступа в ИСПДн и загрузки (остановка) операционной системы состав и содержание информации должны, как минимум, включать дату и время входа (выхода) в систему (из системы) или загрузки (остановки) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

4.7. При регистрации подключения съемных машинных носителей ПДн и вывода ПДн на съемные носители состав и содержание регистрационных записей должны, как минимум, включать дату и время подключения съемных машинных носителей ПДн и вывода ПДн на съемные носители, логическое имя (номер) подключаемого съемного машинного носителя ПДн, идентификатор субъекта доступа, осуществляющего вывод ПДн на съемный носитель ПДн.

4.8. При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой ПДн состав и содержание регистрационных записей должны, как минимум, включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

4.9. При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны, как минимум, включать дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

4.10. При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации должны, как минимум, включать дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер).

4.11. При регистрации попыток удаленного доступа к ИСПДн состав и содержание информации должны, как минимум, включать дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к ИСПДн.

4.12. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения должен предусматривать:

- возможность выбора Ответственным за обеспечение безопасности ПДн в ИСПДн и (или) Администратором ИСПДн событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности, определенных в пункте 4.4 настоящего Регламента;
- генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с составом и содержанием информации, определенными в соответствии с пунктами 4.6 – 4.11 настоящего Регламента;
- хранение информации о событиях безопасности в течение времени, установленного в пункте 4.3 настоящего Регламента.

4.13. Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации в соответствии с составом и содержанием информации о событиях безопасности, подлежащих регистрации, в соответствии с пунктами 4.7 – 4.11 настоящего Регламента, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

4.14. Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

4.15. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам:

- ответственному за обеспечение безопасности ПДн в ИСПДн;
- администратору ИСПДн.

5. Порядок выявления инцидентов информационной безопасности и реагирования на них

5.1. За выявление инцидентов информационной безопасности и реагирование на них отвечают:

- ответственный за обеспечение безопасности ПДн в ИСПДн;
- администратор ИСПДн.

5.2. Работники Администрации, должны сообщать ответственным за выявление инцидентов информационной безопасности о любых инцидентах, в которые входят:

- факты попыток и успешной реализации несанкционированного доступа в ИСПДн, в помещения, в которых осуществляется обработка ПДн, и к хранилищам ПДн;
- факты сбоя или некорректной работы систем обработки информации;
- факты сбоя или некорректной работы СЗИ;
- факты разглашения ПДн;
- факты разглашения информации о методах и способах защиты и обработки ПДн.

5.3. Все нештатные ситуации, факты вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки ПДн в ИСПДн должны быть занесены ответственными за выявление инцидентов информационной безопасности в «ЖУРНАЛ учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ПЭВМ»», форма которого утверждена Положением о обработке персональных данных или в электронные журналы операционной системы и СЗИ.

5.4. Анализ инцидентов информационной безопасности, в том числе определение источников и причин возникновения инцидентов, осуществляется согласно порядку проведения разбирательств по фактам возникновения инцидентов информационной безопасности в ИСПДн.

5.5. Меры по устранению последствий инцидентов информационной безопасности, планированию и принятию мер по предотвращению повторного возникновения инцидентов, возлагаются на ответственных за выявление инцидентов информационной безопасности.

6. Основные этапы процесса реагирования на инциденты

6.1. Ответственные лица, занимающиеся реагированием на инциденты должны обеспечить защиту ИСПДн и проинформировать пользователей, о важности мер по обеспечению информационной безопасности.

6.2. Лица, занимающиеся реагированием на инциденты, должны определить, является ли обнаруженное ими с помощью различных систем обеспечения информационной безопасности событие инцидентом или нет. Для этого могут использоваться публичные отчеты, потоки данных об угрозах, средства статического и динамического анализа образцов программного обеспечения и другие источники информации. Статический анализ выполняется без непосредственного запуска исследуемого образца и позволяет выявить различные индикаторы, например, строки, содержащие URL-адреса или адреса электронной почты. Динамический анализ подразумевает выполнение исследуемой программы в защищенной среде (Песочнице) или на изолированной машине с целью выявления поведения образца и сбора артефактов его работы.

6.3. Лица, занимающиеся реагированием на инциденты, должны идентифицировать скомпрометированные компьютеры и настроить правила безопасности таким образом, чтобы заражение не распространилось дальше по сети. Кроме того, на этом этапе необходимо перенастроить сеть таким образом, чтобы ИСПДн могли продолжать работать без зараженных машин.

6.4. Далее лица, занимающиеся реагированием на инциденты, удаляют вредоносное программное обеспечение, а также все

артефакты, которые оно могло оставить на зараженных компьютерах в ИСПДн.

6.5. Ранее скомпрометированные компьютеры вводятся обратно в сеть. При этом лица, занимающиеся реагированием на инциденты, некоторое время продолжают наблюдать за состоянием этих машин и ИСПДн в целом, чтобы убедиться в полном устранении угрозы.

6.6. Лица, занимающиеся реагированием на инциденты, анализируют произошедший инцидент, вносят необходимые изменения в конфигурацию программного обеспечения и оборудования, обеспечивающего информационной безопасности, и формируют рекомендации для того, чтобы в будущем предотвратить подобные инциденты. При невозможности полного предотвращения будущей атаки составленные рекомендации позволят ускорить реагирование на подобные инциденты.

7. Порядок проведения разбирательств по фактам возникновения инцидентов информационной безопасности

7.1. Для проведения разбирательств по фактам возникновения инцидентов информационной безопасности создаётся комиссия, состоящая не менее чем из трех человек с обязательным включением в её состав:

- ответственного за обеспечение безопасности ПДн в ИСПДн;
- администратора ИСПДн.

7.2. Председатель комиссии организует работу комиссии, решает вопросы взаимодействия комиссии с руководителями и работниками структурных подразделений организации, готовит и ведёт заседания комиссии, подписывает протоколы заседаний. По окончании работы комиссии готовится заключение по результатам проведённого разбирательства, которое передается на рассмотрение Главе Козловского муниципального округа.

7.3. При проведении разбирательства устанавливаются:

- наличие самого факта совершения инцидента информационной безопасности, служащего основанием для вынесения соответствующего решения;
- время, место и обстоятельства возникновения инцидента, а также оценка его последствий;
- конкретный работник, совершивший инцидент информационной безопасности или повлекший своими действиями возникновения инцидента;
- наличие и степень вины работника, совершившего инцидент информационной безопасности или повлекшего своими действиями возникновение инцидента;
- цели и мотивы, способствовавшие совершению инцидента информационной безопасности.

7.4. В целях проведения разбирательства все работники обязаны по первому требованию членов комиссии предъявить для проверки все числящиеся за ними материалы и документы, дать устные или письменные объяснения об известных им фактах по существу заданных им вопросов.

7.5. Работник, совершивший инцидент информационной безопасности или повлекший своими действиями возникновения инцидента, обязан по требованию комиссии представить объяснения в письменной форме не позднее трех рабочих дней с момента получения соответствующего требования. Комиссия вправе поставить перед работником перечень вопросов, на которые работник обязан ответить. В случае отказа работника от письменных объяснений, комиссией составляется акт.

7.6. Работник имеет право, по согласованию с председателем комиссии, знакомиться с материалами разбирательства, касающимися лично его, и давать по поводу них свои комментарии, предоставлять дополнительную информацию и документы. По окончании разбирательства работнику для ознакомления предоставляется итоговый акт с выводами комиссии.

7.7. В случае давления на работника со стороны других лиц (не из состава комиссии) в виде просьб, угроз, шантажа и др., по вопросам, связанным с проведением разбирательства, работник обязан сообщить об этом председателю комиссии.

7.8. До окончания работы комиссии и вынесения решения членам комиссии запрещается разглашать сведения о ходе проведения разбирательства и ставшие известные им обстоятельства.

7.9. В процессе проведения разбирательства комиссией выясняются:

- перечень разглашенных сведений;
- причины разглашения сведений;
- лица, виновные в разглашении сведений;
- размер (экспертную оценку) причиненного ущерба;
- недостатки и нарушения, допущенные работниками при работе с ПДн;

7.10. иные обстоятельства, необходимые для определения причин разглашения ПДн, степени виновности отдельных лиц, возможности применения к ним мер воздействия.

7.11. По завершении разбирательства комиссией составляется заключение. В заключении указываются:

- основание для проведения в разбирательства;
- состав комиссии и время проведения разбирательства;
- сведения о времени, месте и обстоятельствах возникновения инцидента информационной безопасности;
- сведения о работнике, совершившем инцидент информационной безопасности или повлекшем своими действиями возникновения инцидента (должность, фамилия, имя, отчество, год рождения, время работы в Администрации, а также в занимаемая должность);
- цели и мотивы работника, способствовавшие совершению инцидента информационной безопасности;
- причины и условия возникновения инцидента информационной безопасности;
- данные о характере и размерах причиненного в результате инцидента ущерба;
- предложения о мере ответственности работника, совершившего инцидент информационной безопасности или повлекшего своими действиями возникновения инцидента.

7.12. На основании заключения выносится решение о применении мер ответственности к работнику, совершившему инцидент или повлекшему своими действиями возникновению инцидента, также о возмещении ущерба виновным работником (или его законным представителем), которое доводится до указанного работника в письменной форме под расписку.

7.13. Все материалы разбирательства относятся к информации ограниченного доступа и хранятся в течение 5 лет. Копии заключения и распоряжения по результатам разбирательства приобщаются к личному делу работника, в отношении которого оно проводилось.

8. Ответственность

8.1. Все работники, осуществляющие защиту ПДн, обязаны ознакомиться с данным Регламентом под подпись.

8.2. Работники несут персональную ответственность за выполнение требований настоящего Регламента.

9. Срок действия и порядок внесения изменений

9.1. Настоящий Регламент вступает в силу с момента его утверждения и действует бессрочно.

9.2. Настоящий Регламент подлежит пересмотру не реже одного раза в три года.
Изменения и дополнения в настоящий Регламент вносятся распоряжением Главы Козловского муниципального округа Чувашской Республики.

Приложение № 32
Утверждена
распоряжением Администрации
Козловского муниципального округа
Чувашской Республики
от 18.12.2024 г. № 454

ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ РЕЗЕРВИРОВАНИЯ И ВОССТАНОВЛЕНИЯ РАБОТОСПОСОБНОСТИ ТЕХНИЧЕСКИХ СРЕДСТВ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, БАЗ ДАННЫХ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

АДМИНИСТРАЦИИ КОЗЛОВСКОГОМУНИЦИПАЛЬНОГО ОКРУГА ЧУВАШСКОЙ РЕСПУБЛИКИ

г. Козловка
2024 г.

1. Термины и определения

1.1. Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.
1.2. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
1.3. 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.
1.4. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.
1.5. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
1.6. Пользователь информационной системы персональных данных – работник, осуществляющий обработку персональных данных в информационной системе персональных данных.
1.7. Средство антивирусной защиты – программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации.
1.8. Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенные или используемые для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных (далее – Инструкция) устанавливает основные требования к организации резервного копирования (восстановления) программ и данных, хранящихся в базах данных информационных систем персональных данных (далее – ИСПДн) Администрации Козловского муниципального округа Чувашской Республики (далее – Учреждение), а также к резервированию аппаратных средств.
2.2. Настоящая Инструкция разработана с целью:
- определения категории информации, подлежащей обязательному резервному копированию;
- определения процедуры резервирования данных для последующего восстановления работоспособности ИСПДн при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);
- определения порядка восстановления информации в случае возникновения такой необходимости;
- упорядочения работы и определения ответственности должностных лиц, связанной с резервным копированием и восстановлением информации.

2.3. Действие настоящей Инструкции распространяется на всех пользователей ИСПДн Учреждения, а также на основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:
- системы жизнеобеспечения технических средств;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;

2.4. Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности ИСПДн в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.
2.5. Резервному копированию подлежит информация следующих основных категорий:
- информация, обрабатываемая пользователями в ИСПДн, а также информация, необходимая для восстановления работоспособности ИСПДн, в т.ч. систем управления базами данных (далее – СУБД) общего пользования и справочно-информационных систем общего использования;
- рабочие копии установочных компонентов программного обеспечения общего назначения и специализированного программного обеспечения серверов и рабочих станций;

– информация, необходимая для восстановления систем управления базами данных ИСПДн, локальной вычислительной сети, системы электронного документооборота;

– регистрационная информация систем защиты информации;

– другая информация ИСПДн, по мнению пользователей, администраторов ИСПДн и ответственного за обеспечение безопасности персональных данных (далее – ПДн) в ИСПДн, являющаяся критичной для работоспособности ИСПДн.

2.6. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности персональных данных, и не исключает обязательного выполнения их требований.

3. Общие требования к резервному копированию

3.1. В Инструкции резервного копирования описываются действия при выполнении следующих мероприятий:

– резервное копирование с указанием конкретных резервируемых данных и аппаратных средств (в случае необходимости);

– контроль резервного копирования;

– хранение резервных копий;

– полное или частичное восстановление данных.

4. Ответственность за состояние резервного копирования

4.1. Ответственность за контроль над своевременным осуществлением резервного копирования и соблюдением соответствующей Инструкции, а также за выполнением требований по хранению резервных копий и предотвращению несанкционированного доступа к ним возлагается на ответственного за обеспечение безопасности ПДн в ИСПДн и администраторов ИСПДн.

4.2. В случае обнаружения попыток несанкционированного доступа к носителям резервной информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается ответственному за обеспечение безопасности ПДн в ИСПДн в течение рабочего дня после обнаружения указанного события.

5. Периодичность резервного копирования

5.1. Резервное копирование специализированного программного обеспечения производится при его получении (если это предусмотрено инструкцией по его применению и не противоречит условиям его распространения), а также при его обновлении и получении исправленных и обновленных версий.

5.2. Информация, содержащаяся в постоянно изменяемых базах данных, сохраняется в соответствии со следующим графиком:

– ежедневно проводится копирование измененной и дополненной информации (носители с ежедневной информацией должны храниться в течение недели);

– еженедельно проводится резервное копирование всей базы данных (носители с еженедельными копиями хранятся в течение месяца);

– ежемесячно производится резервное копирование на специально выделенный носитель длительного хранения, информация на котором хранится постоянно.

5.3. Не реже одного раза в год на носители длительного хранения записывается информация, не относящаяся к постоянно изменяемым базам данных (приказы, распоряжения, открытые издания и т.д.)

5.4. Восстановление информации из резервных копий

6.1. В случае необходимости, восстановление данных из резервных копий производится ответственными работниками.

6.2. Восстановление данных из резервных копий происходит в случае ее исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.

6.3. Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.

6.4. Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

6.5. Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей. При этом используется последняя копия информации.

6.6. При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.

6. Срок действия и порядок внесения изменений

7.1. Настоящая Инструкция вступает в силу с момента ее утверждения и действует бессрочно.

7.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

Изменения и дополнения в настоящую Инструкцию вносятся распоряжением Главы Козловского муниципального округа Чувашской Республики.

Инструкция разработана:

Начальник отдела правового обеспечения
и цифрового развития администрации
Козловского муниципального округа
Чувашской Республики _____/ _____