АДМИНИСТРАЦИЯ ХАРЬКОВСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ МУНИЦИПАЛЬНОГО РАЙОНА «РОВЕНЬСКИЙ РАЙОН»
БЕЛГОРОДСКОЙ ОБЛАСТИ
село Харьковское

Р А С П О Р Я Ж Е Н И Е

01 декабря 2022 года № 85

О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах администрации Харьковского сельского поселения муниципального района «Ровеньский район» Белгородской области

В соответствии с требованиями Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации 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»:

1.Возложить обязанности по защите информации:

1.1. Назначить лицом, ответственным за защиту информации, за обеспечение безопасности персональных данных в информационных системах администрации Харьковского сельского поселения заместителя главы администрации Садченко Светлану Викторовну.

1.2. Назначить ответственным за эксплуатацию ИС заместителя главы администрации Садченко Светлану Викторовну.

1.3. Утвердить перечень должностей, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей согласно приложению 1 к настоящему распоряжению.

1.4. Утвердить перечень должностей, ведущих обработку персональных данных без использования средств автоматизации согласно приложению 2 к настоящему распоряжению.

5.5. Утвердить перечень лиц, ответственных за обезличивание персональных данных согласно приложению 3 к настоящему распоряжению.

2. Создать комиссию по защите информации:

2.2. Утвердить состав комиссии по защите информации согласно приложению 4 к настоящему распоряжению.

2.2. Утвердить положение о комиссии по защите информации согласно приложению 5 к настоящему распоряжению.

3. Утвердить типовые формы документов по защите информации:

3.1. Согласие на обработку персональных данных согласно приложению 6 к настоящему распоряжению.

3.2. Разъяснение субъекту персональных данных согласно приложению 7 к настоящему распоряжению.

3.3. Соглашение о неразглашении информации, содержащей персональные данные, согласно приложению 8 к настоящему распоряжению.

3.4.Журналы по защите информации согласно приложению 9 к настоящему распоряжению.

3.5. Протокол заседания комиссии по защите информации согласно приложению 10 к настоящему распоряжению.

3.6. Акт определения уровня защищенности ПДн при их обработке в ИСПДн и класса защищенности ИС согласно приложению 11 к настоящему распоряжению.

3.7. Акт оценки возможного вреда субъектам персональных данных и принятия мер по его предотвращению в администрации Харьковского сельского поселения согласно приложению 12 к настоящему распоряжению.

3.8. Акт об уничтожении персональных данных, согласно приложению 13 к настоящему распоряжению.

4. Утвердить перечень обрабатываемых персональных данных согласно приложению 14 к настоящему распоряжению.

5. Утвердить инструкции и правила по защите информации:

- Положение об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения, согласно приложению 15 к настоящему распоряжению

– Правила работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей, согласно приложению 16 к настоящему распоряжению;

– Инструкцию ответственного за организацию обработки персональных данных согласно приложению 17 к настоящему распоряжению

– Инструкцию ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных согласно приложению 18 к настоящему распоряжению;

– Инструкцию по учету лиц, допущенных к работе с персональными данными в информационных системах персональных данных согласно приложению 19 к настоящему распоряжению;

– Инструкцию по проведению инструктажа лиц, допущенных к работе с информационной системой персональных данных, согласно приложению 20 к настоящему распоряжению;

– Инструкцию пользователя информационной системой персональных данных, согласно приложению 21 к настоящему распоряжению;

– Инструкцию по учету и хранению съемных носителей, согласно приложению 22 к настоящему распоряжению;

– Инструкцию пользователя при возникновении нештатной ситуации, согласно приложению 23к настоящему распоряжению;

– Инструкцию по обработке персональных данных без использования средств автоматизации согласно приложению 24 к настоящему распоряжению;

– Инструкцию по работе с инцидентами информационной безопасности согласно приложению 25 к настоящему распоряжению;

– Инструкцию ответственного за эксплуатацию информационных систем персональных данных согласно приложению 26 к настоящему распоряжению;

– Инструкцию по организации антивирусной защиты в информационных системах персональных данных, согласно приложению 27 к настоящему распоряжению;

– Правила работы с обезличенными данными согласно приложению 28 к настоящему распоряжению;

6. Рекомендовать подведомственному администрации Харьковского сельского поселения МКУ «Харьковская АХС» к принятию аналогичного акта о назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах МКУ «Харьковская АХС».

7. Контроль за исполнением настоящего распоряжения оставляю за собой.

8. Контроль за исполнением настоящего распоряжения оставляю за собой.

Глава администрации
Харьковского сельского поселения **Ю.И.Снеговской**

С данным распоряжением ознакомлен(а):

_____ / _____ *(подпись/Ф.И.О.)*

_____ / _____ *(подпись/Ф.И.О.)*

_____ / _____ *(подпись/Ф.И.О.)*

Приложение 1
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

Перечень должностей, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей

Должность	Ф.И.О.
Глава администрации Харьковского сельского поселения	Снеговской Юрий Иванович
Заместитель главы администрации Харьковского сельского поселения	Садченко Светлана Викторовна
Экономист-финансист администрации Харьковского сельского поселения	Схоменко Людмила Александровна

Приложение 2
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

Перечень должностей, ведущих обработку персональных данных без использования средств автоматизации

Должность	Ф.И.О.
Глава администрации Харьковского сельского поселения	Снеговской Юрий Иванович
Заместитель главы администрации Харьковского сельского поселения	Садченко Светлана Викторовна
Экономист-финансист администрации Харьковского сельского поселения	Схоменко Людмила Александровна

Приложение 3
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

Перечень лиц, ответственных за обезличивание персональных данных

Должность	Ф.И.О.
Глава администрации Харьковского сельского поселения	Снеговской Юрий Иванович
Заместитель главы администрации Харьковского сельского поселения	Садченко Светлана Викторовна
Экономист-финансист администрации Харьковского сельского поселения	Схоменко Людмила Александровна

Приложение 4
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

Состав комиссии по защите информации

Председатель комиссии	Снеговской Ю.И. - глава администрации
Члены комиссии	Садченко С.В. - заместитель главы администрации
	Схоменко Л.А. - экономист-финансист администрации

Приложение 5
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

ПОЛОЖЕНИЕ
о комиссии по защите информации

1. Общие положения

1.1. Настоящее Положение определяет основные задачи, порядок формирования, полномочия и ответственность комиссии.

2. Основные задачи комиссии

2.1. Основными задачами комиссии являются:

2.1.1. Сбор и анализ исходных данных по информационным системам персональных данных администрации Харьковского сельского поселения.

2.1.2. Определение значений параметров для проведения классификации информационных систем в соответствии с Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2.1.3. Определение значений параметров для установления уровня защищенности персональных данных в соответствии с постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2.1.4. Определение класса защищенности информационных систем персональных данных администрации Харьковского сельского поселения на основании собранных данных.

2.1.5. Определение уровня защищенности персональных данных при их обработке в информационных системах персональных данных.

3. Порядок формирования комиссии

3.1. Комиссия формируется из числа штатных сотрудников администрации Харьковского сельского поселения, участвующих в процессе обработки персональных данных.

3.2. В состав Комиссии входит не менее трех человек – членов Комиссии, в их числе – председатель Комиссии.

3.3. Члены комиссии назначаются распоряжением главы администрации Харьковского сельского поселения.

3.4. В случае изменения состава Комиссии, в распоряжение вносятся соответствующие изменения.

4. Полномочия комиссии

4.1. Для осуществления задач, указанных в разделе 2 настоящего Положения, Комиссия имеет право:

4.1.1. Получать необходимые сведения у всех работников администрации Харьковского сельского поселения, участвующих в обработке персональных данных.

4.1.2. Просматривать электронные базы данных и бумажные носители, содержащие персональные данные, с целью выявления состава обрабатываемых персональных данных.

4.1.3. Отслеживать технологический процесс обработки персональных данных.

4.1.4. Выявлять или получать готовые сведения о структуре локальной вычислительной сети администрации Харьковского сельского поселения.

4.1.5. Определять или получать готовые сведения о наличии и способах доступа к сетям общего пользования.

4.1.6. Определять или получать готовые сведения о технических и программных средствах обработки персональных данных.

4.1.7. Определять или получать готовые сведения об условиях, местах и способах передачи персональных данных в сторонние организации.

5. Отчетность комиссии

5.1. Комиссия при выполнении своих задач должна составить протокол заседания комиссии.

5.2. В результате своей деятельности Комиссия должна составить Акт(ы) определения уровня защищенности персональных данных и класса защищенности информационных систем персональных данных.

Приложение 6
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения

с. Харьковское «_____» _____20____г.

Я,_____
Ф.И.О. субъекта персональных данных

место регистрации_____

телефон:_____адрес электронной почты: _____ руководствуясь статьей 10.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», заявляю о согласии на распространение администрацией Харьковского сельского поселения» (далее – Оператор) (ОГРН 1023102155130, ИНН 3117001121, КПП 3117010001, ОКВЭД 84.11.31, ОКПО 04115102, ОКГУ 3300500, место нахождения: 309757, Белгородская область, Ровеньский район, с. Харьковское, ул. Центральная, д.31/2) моих персональных данных с целью:

- ✓ обеспечение соблюдения законов и иных нормативных правовых актов Российской Федерации, а также локальных нормативных актов Оператора;
- ✓ видео- и фотосъемки и размещение материалов на официальных сайтах в следующем порядке:

Категория персональных данных	Перечень персональных данных	Разрешаю к распространению (да/нет)	Разрешаю к распространению неограниченному кругу лиц (да/нет)	Условия и запреты[1]	Дополнительные условия
Общие персональные данные	Фамилия	да	да	не устанавливаю	
	Имя	да	да	не устанавливаю	
	Отчество	да	да	не устанавливаю	
	Год рождения	да	нет	не устанавливаю	
	Адрес	да	нет	не устанавливаю	
	Дата рождения	да	нет	не устанавливаю	
	Образование	да	нет	не устанавливаю	
	Место жительства	да	нет	не устанавливаю	
	Семейное поло-	да	нет	не	

	жение			устанавливаю	
	Данные о повышении квалификации	да	да	не устанавливаю	
	Данные о профессиональной переподготовке	да	да	не устанавливаю	
	Профессия (специальность) квалификация	да	да	не устанавливаю	
	Сведения о трудовой деятельности (занимаемых ранее должностях и стаже работы)	да	да	не устанавливаю	
	Сведения о наградах и поощрениях	да	да	не устанавливаю	
	Доходы	да	нет	не устанавливаю	только руководителю, юрисконсульту, сотрудникам МКУ «ЦБУ Ровеньского района»
Специальные категории персональных данных	состояние здоровья	да	нет	не устанавливаю	только руководителю, юрисконсульту, сотрудникам отдела кадров, специалисту по охране труда
	сведения о судимости	да	нет	не устанавливаю	только руководителю, юрисконсульту, сотрудникам отдела кадров
Биометрические персональные данные	фото- и (или) видеоизображения			не устанавливаю	

Сведения об информационных ресурсах Оператора, посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных:

Информационный ресурс	Действия с персональными данными
https://xarkovskoe-r31.gosweb.gosuslugi.ru	Предоставление сведений неограниченному кругу лиц
https://vk.com/public216944463	Предоставление сведений неограниченному кругу лиц

https://ok.ru/group/61171937706175	Предоставление сведений неограниченному кругу лиц

Настоящее согласие дано мной добровольно и действует с «__» _____ 20 __ года.

Настоящее согласие дано мной на срок _____.

Оставляю за собой право потребовать прекратить распространять мои персональные данные. В случае получения требования Оператор обязан немедленно прекратить распространять мои персональные данные, а также сообщить перечень третьих лиц, которым персональные данные были переданы. Подтверждаю, что мои права и обязанности в области защиты персональных данных мне разъяснены.

_____ /_____
(подпись) (расшифровка подписи

---

[1] Условия и запреты на обработку вышеуказанных персональных данных (ч. 9 ст. 10.1 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных") :

1. не устанавливаю
2. устанавливаю запрет на передачу (кроме предоставления доступа) этих данных оператором неограниченному кругу лиц
3. устанавливаю запрет на обработку (кроме получения доступа) этих данных неограниченным кругом лиц

4.устанавливаю условия обработки (кроме получения доступа) этих данных неограниченным кругом лиц

Приложение 7
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

Разъяснение
субъекту персональных данных юридических последствий
отказа предоставить свои персональные данные

Мне,_____,
фамилия, имя, отчество полностью

_____,
адрес регистрации субъекта персональных данных

_____
вид документа, удостоверяющего личность, серия, номер, когда и кем выдан

_____,

в соответствии с частью 2 статьи 18 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
разъяснены юридические последствия отказа предоставить свои персональные данные в администрацию Харьковского сельского поселения.

В соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152 ФЗ «О персональных данных», определен перечень персональных данных, которые субъект персональных данных обязан предоставить в администрацию Харьковского сельского поселения в связи с поступлением на работу.

Без представления субъектом персональных данных обязательных для заключения трудового договора сведений, трудовой договор не может быть заключен.

_____	_____	_____
дата	подпись	расшифровка

Приложение 8
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

Соглашение
о неразглашении информации, содержащей персональные данные

Я, _____,
(Фамилия Имя Отчество)

работая в должности _____
понимаю, что на период исполнения мною должностных обязанностей по трудовому договору, заключенному между мною и администрацией Харьковского сельского поселения и непосредственно осуществляя обработку персональных данных (далее – ПДн), ознакомлен(а) с требованиями по соблюдению конфиденциальности обрабатываемых мною ПДн субъектов ПДн и обязуюсь прекратить обработку ПДн, ставших мне известными в связи с исполнением должностных обязанностей в случае расторжения со мной трудового договора или перехода на должность, не предусматривающую доступ к ПДн.

В соответствии со статьей 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон) я уведомлен(а) о том, что операторы и иные лица, получившие доступ к ПДн субъектов ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено Федеральным законом.

Настоящим добровольно принимаю на себя обязательства:

– не разглашать третьим лицам персональные данные, которые мне доверены (будут доверены) или станут известными в связи с исполнением должностных обязанностей

– не передавать (в любом виде) и не разглашать третьим лицам, не имеющим на это право в силу выполняемых ими должностных обязанностей, информацию, содержащую ПДн (за исключением собственных данных), которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей;

– не использовать информацию, содержащую ПДн, с целью получения выгоды;

– выполнять требования закона и иных нормативных правовых актов Российской Федерации, а также внутренних документов администрации, регламентирующих вопросы защиты интересов субъектов ПДн, порядка обработки и защиты ПДн;

– в случае попытки третьих лиц, не имеющих на это право, получить от меня информацию, содержащую ПДн, немедленно сообщать об этом факте своему непосредственному руководителю;

– в течение 1 (одного) года после прекращения моих прав на допуск к информации, содержащей ПДн (переход на должность, не предусматривающую доступ к ПДн или прекращения трудового договора), не разглашать, не раскрывать публично и не передавать третьим лицам известную мне информацию, содержащую ПДн. Носители информации, содержащие ПДн (документы, диски, машинные накопители и так далее), которые находились в моем распоряжении во время работы в администрации, передать своему непосредственному руководителю или другому работнику по указанию главы администрации.

Ответственность, предусмотренная законодательством Российской Федерации, мне разъяснена.

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

«___» _____ 20__ г. _____ /_____ /

(подпись) **(фамилия, инициалы)**

Приложение 9
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

ЖУРНАЛ
учета машинных носителей персональных данных (съемные носители)

№ п/п	Регистрационный номер	Тип и ёмкость	Получил (Ф.И.О, дата, подпись)	Сдал (Ф.И.О, дата, подпись)	Место хранения	Ответственное должностное лицо (Ф.И.О)

ЖУРНАЛ
учета лиц, допущенных к работе с персональными данными в информационных системах

№ п/п	Сведения о допуске к персональным данным				Сведения о прекращении допуска к персональным данным	
	Наименование информационной системы персональных данных/ способ обработки ПДн	ФИО, должность получившего допуск	Дата и номер приказа о допуске	Дата и подпись допускаемого лица	Дата и номер приказа о прекращении допуска	Номер приказа об увольнении или дата и подпись лица об ознакомлении с документом, прекращающим допуск к ПДн

ЖУРНАЛ
учета согласий субъектов персональных данных

№ п/п	Дата и номер согласия	Ф.И.О. субъекта персональных данных

ЖУРНАЛ
прохождения первичного инструктажа работниками допущенных к работе с персональными данными в информационных системах

№ п/п	Фамилия, имя, отчество инструктируемого	Дата прохождения инструктажа	Подпись работника	Фамилия инструктирующего или организующего обучение	Подпись должностного лица

ЖУРНАЛ
учета ЭП

№ п/п	Номера экземпляров ключевых документов	Номера криптографических ключей	Наименование СКЗИ	Отметка о получении		Отметка о выдаче		
				От кого получены (УУЦ)	Дата	ФИО пользователя	Дата	Подпись

ЖУРНАЛ
учета обращений субъектов персональных данных по вопросам обработки персональных данных

№ № п/п	Дата обращения	ФИО обратившегося	Цель обращения	Отметка о предоставлении информации или отказе в ее предоставлении / дата предоставления или отказа в предоставлении информации	Подпись ответственного	Примечание

ЖУРНАЛ
учета выявленных инцидентов информационной безопасности

№ № п/п	Дата и время	Описание инцидента	Ответственный за реагирование на инцидент	Отметка об устранении инцидента	Дата устранения инцидента	Подпись ответственного лица	Примечание

ЖУРНАЛ
регистрации нарушения и восстановления работоспособности оборудования или ИСПДн

№ п/п	Наименование ИСПДн, описание нарушения работоспособности оборудования или ИСПДн	Дата и время обнаружения начала нарушения работоспособности	Выявленная причина нарушения работоспособности	Дата и время восстановления работоспособности		Наименование инфицированных файлов, источника поступления (носитель, организация)	Сотрудник, проводивший восстановление работоспособности оборудования или ИСПДн	
							Ф.И.О.	Подпись

ЖУРНАЛ
учета передачи персональных данных

№ п/п	Сведения о запрашивающем лице	Состав запрашиваемых персональных данных	Цель получения персональных данных	Отметка о передаче или отказе в передаче персональных данных	Дата передачи/ отказа в передаче персональных данных	Подпись запрашивающего лица

ЖУРНАЛ
уничтожения носителей персональных данных

№ № п/п	Наименование ИСПДн, в которой уничтожаются персональные данные	Ф.И.О. субъекта, персональные данные которого подлежат уничтожению	Обоснование уничтожения	Наименование файла, и его месторасположение	Дата уничтожения	Ф.И.О. и подпись Исполнителя	Ф.И.О. и подпись ответственного за обработку персональных данных

Приложение 10
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

ПРОТОКОЛ № 1
заседания комиссии по защите информации

Дата и время проведения _____
Место проведения _____

Комиссия в составе:
Председатель комиссии _____ Снеговской Ю.И.
Члены комиссии _____ Садченко С.В.
_____ Схоменко Л.А.

Повестка дня

Определение информационных систем персональных данных (далее - ИСПДн), принадлежащих администрации Харьковского сельского поселения.

1. Слушали: _____
доложил(а) исходные данные об ИСПДн администрации Харьковского сельского поселения.

Выступил(а): _____ предложил(а) утвердить акт определения уровня защищенности персональных данных и класса защищённости ИСПДн администрации Харьковского сельского поселения.

Постановили:
Утвердить акт определения уровня защищенности персональных данных и класса защищённости ИС администрации Харьковского сельского поселения.

2. Слушали: _____ доложил(а) исходные данные об ИСПДн администрации Харьковского сельского поселения.

Выступил(а): _____ предложил(а) утвердить акт определения уровня защищенности персональных данных и класса защищённости ИСПДн администрации Харьковского сельского поселения.

Постановили:
Утвердить акт определения уровня защищенности персональных данных и класса защищённости ИС администрации Харьковского сельского поселения.

Председатель комиссии _____ Снеговской Ю.И.
Члены комиссии _____ Садченко С.В.
_____ Схоменко Л.А.

Приложение 11
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

АКТ
определения уровня защищенности ПДн при их обработке в ИСПДн администрации Харьковского сельского поселения и класса защищенности ИС администрации Харьковского сельского поселения

Комиссия в составе:

Председатель комиссии	_____	Снеговской Ю.И.
Члены комиссии	_____	Садченко С.В.
	_____	Схоменко Л.А.

Рассмотрев исходные данные об информационной системе персональных данных (далее - ИСПДн), комиссия определила:

– Категории персональных данных обрабатываемых в ИСПДн: в информационной системе обрабатываются общие категории персональных данных;

– Категории субъектов: персональные данные субъектов персональных данных, не являющихся сотрудниками оператора;

– Объем обрабатываемых персональных данных: менее 1 000;

– Тип актуальных угроз: для информационной системы актуальны угрозы 3-го типа;

– Уровень значимости информации: информация имеет низкий уровень значимости УЗ 3;

– Масштаб информационной системы: информационная система имеет объектовый масштаб.

Комиссия решила, в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а так же в соответствии с приказом ФСТЭК Российской Федерации от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и на основании анализа исходных данных, необходимо обеспечить третий уровень защищенности (УЗ 3) персональных данных и установить третий класс защищенности информационной системы (К3).

Результат оценки вреда:

Для информационной системы актуальны угрозы 3-го типа.

Уровень значимости информации определен степенью возможного ущерба для обладателя информации от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности

(неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации, руководствуясь следующей формулой:

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)], где степень возможного ущерба определяется обладателем информации.

Комиссия утвердила следующее:

УЗ = [(конфиденциальность, низкая степень ущерба) (целостность, низкая степень ущерба) (доступность, низкая степень ущерба)] – таким образом, комиссия установила низкий уровень значимости (УЗ 3) (возможны незначительные негативные последствия).

Председатель комиссии	_____	Снеговской Ю.И.
Члены комиссии	_____	Садченко С.В.
	_____	Схоменко Л.А.

«__»_____20__ г.

Приложение 12
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

АКТ
оценки возможного вреда субъектам персональных данных и принятия мер по его предотвращению в администрации Харьковского сельского поселения

Комиссия в составе:

Председатель комиссии _____ Снеговской Ю.И.
Члены комиссии _____ Садченко С.В.
_____ Схоменко Л.А.

Произвела оценку возможного вреда субъектам персональных данных и принятия мер по его предотвращению в администрации Харьковского сельского поселения(далее – администрация). По результатам оценки установлено:

№ п/п	**Требования Федерального закона «О персональных данных», которые могутбыть нарушены**	**Возможные нарушение безопасности информации**		**Уровень возможного вреда субъекту персональных данных**	**Принимаемые администрацией меры по исключению нанесения возможного вреда**
1.	Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей	Целостность		Низкий	Цели обработки персональных данных закреплены в Правилах обработки персональных данных в администрации и в договорах, регламентирующих правоотношения администрации с третьими лицами.
		Доступность			
		Конфеденциальность	+		
2.	Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой	Целостность		Низкий	Соответствующие нормы закреплены в Политике администрации в отношении обработки персональных данных и Правилах обработки персональных данных в администра-
		Доступность			
		Конфеденциальность	+		

					ции
3.	Обработке подлежат только персональные данные, которые отвечают целям их обработки	Целостность		Низкий	Соответствующие нормы закреплены в Правилах обработки персональных данных в администрации.
		Доступность			
		Конфеденциальность			
4	Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки	Целостность		Низкий	Содержание и объем обрабатываемых персональных определены в Правилах обработки персональных данных в администрации.
		Доступность	+		
		Конфеденциальность			
5.	При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных	Целостность	+	Низкий	Соответствующие нормы закреплены в Правилах обработки персональных данных в администрации.
		Доступность			
		Конфеденциальность			
6.	Хранение персональных данных должно осуществляться 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,выгодоприобретателем или поручителем по которому является субъект персональных данных	Целостность		Низкий	Соответствующие нормы закреплены в Правилах обработки персональных данных в администрации
		Доступность			
		Конфеденциальность	+		
7.	Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требова-	Целостность	+	Низкий	Необходимые требования закреплены в договорах, регламентирующих правоотношения администрации с третьими лицами.
		Доступность	+		
		Конфеденциальность	+		

	ния к защите обрабатываемых персональных данных в соответствии со статьей 19 настоящего Федерального закона				
8.	Операторы и иные 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 федеральным законом	Целостность		Низкий	Соответствующие нормы закреплены в организационно-распорядительных документах администрации, регламентирующих обработку и защиту персональных данных и в договорах, регламентирующих правоотношения
		Доступность			
		Конфеденциальность	+		
9.	В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных	Целостность	+	Низкий	Соответствующие нормы закреплены в Правилах обработки персональных данных в администрации. Размещение информации в общедоступных источниках осуществляется на основании письменного согласия субъекта персональных данных
		Доступность	+		
		Конфеденциальность			
10	Персональные данные могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона	Целостность	+	Низкий	Соответствующие нормы закреплены в договорах, регламентирующих правоотношения администрации с третьими лицами.
		Доступность	+		
		Конфеденциальность			
11.	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 частью 2 настоящей статьи	Целостность	+	Низкий	Соответствующие нормы закреплены в договорах, регламентирующих правоотношения администрации с третьими лицами.
		Доступность	+		
		Конфеденциальность			
12.	Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональ-	Целостность	+	Низкий	Обработка биометрических персональных данных в администрации не осуществляется
		Доступность			
		Конфеденци-			

	ные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи	альность			
13.	Оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных	Целостность Доступность Конфеденциальность	+ + +	Низкий	Соответствующие нормы закреплены в организационно-распорядительных документах администрации, регламентирующих обработку и защиту персональных данных и в договорах, регламентирующих правоотношения администрации с третьими лицами.
14.	Субъект персональных данных вправе требовать от оператора 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	Целостность Доступность Конфеденциальность	+ +	Низкий	Соответствующие нормы закреплены в Правилах рассмотрения запросов субъектов персональных данных или их представителей в администрации и других организационно-распорядительных документах администрации, регламентирующих обработку и защиту персональных данных
15.	Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных	Целостность Доступность Конфеденциальность	 + +	Низкий	Соответствующие нормы закреплены в Правилах рассмотрения запросов субъектов персональных данных или их представителей в администрации и других организационно-распорядительных документах администрации, регламентирующих обработку и защиту персональных данных.

По результатам оценки возможного вреда субъектам персональных данных и принятым мерам по его предотвращению в администрации, комиссией установлено, что принимаемые меры ограничивают причинение возможного вреда субъектам персональных данных.

Председатель комиссии _____ Снеговской Ю.И.

Члены комиссии _____ Садченко С.В.

_____ Схоменко Л.А.

Приложение 13
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

_____(Наименование оператора персональных данных)

Утверждаю
_____ (должность)
_____ / _____
"__" _____ 20__ года

Акт об уничтожении персональных данных №__

г. _____
"__" _____ 20__ года

Комиссия в составе председателя, _____ (должность, ФИО), и членов, _____ (должности, ФИО), наделенная полномочиями _____ (наименование документа) _____ (должность, ФИО) №__ от "__" _____ 20__ года, составила настоящий акт о нижеследующем.

"__" _____ 20__ года в соответствии с положениями Федерального закона от 27.07.2006 №152-ФЗ "О персональных данных" комиссией было произведено уничтожение персональных данных _____ (категория лиц). Данные находились на бумажных носителях, хранящихся в _____ (наименование оператора персональных данных).

№ п/п	Наименование носителя	Пояснения

Уничтожение информации произведено _____ (способ уничтожения), гарантирующим полное уничтожение персональных данных.

Основания для уничтожения персональных данных: _____.

Подписи

Председатель комиссии: _____ / _____

Члены комиссии:

_____ / _____
_____ / _____

Приложение 14
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

Перечень
персональных данных, обрабатываемых в администрации Харьковского сельского поселения муниципального района «Ровеньский район» Белгородской области в связи с реализацией служебных (трудовых) отношений, а также в связи с осуществлением муниципальных функций и оказанием муниципальных услуг

1. Персональные данные, обрабатываемые в связи с реализацией служебных (трудовых) отношений:

фамилия, имя, отчество (в том числе информация о смене фамилии, имени, отчества);

дата и место рождения;

гражданство;

данные российского паспорта (серия, номер, когда и кем выдан);

сведения о пребывании за границей (когда, где, с какой целью);

место жительства и дата регистрации по месту жительства, место фактического проживания;

номера контактных телефонов;

семейное положение (информация о вступлении в брак, в случае развода - данные о разводе);

сведения о близких родственниках (отец, мать, усыновители, усыновленные, братья и сестры, дети, а также жена (муж), в том числе бывшие):

- степень родства, фамилия, имя, отчество (в том числе информация о смене фамилии, имени, отчества);
- дата и место рождения;
- место работы (учебы), должность;
- адрес регистрации и фактического проживания (в случае проживания за границей - с какого времени проживают);
- сведения об оформлении документов для выезда на постоянное место жительства в другое государство (в том числе в связи с работой либо обучением);
- сведения о судимости;

сведения о полученном образовании;

сведения о судимости;

сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу;

сведения об уровне специальных знаний (работа на компьютере, знание иностранного языка и языков народов Российской Федерации);

сведения о трудовой деятельности, общем трудовом стаже и стаже государственной гражданской службы Российской Федерации, муниципальной службы;

сведения о состоянии здоровья (заключение медицинского учреждения установленной формы об отсутствии заболевания, препятствующего поступлению на муниципальную службу и ее прохождению);

сведения о замещаемой должности;

сведения о наличии допуска к государственной тайне, оформленного за период

работы, службы, учебы;

сведения о классных чинах, воинских и специальных званиях;

сведения о профессиональной переподготовке, повышении квалификации, дополнительном образовании;

сведения о награждении государственными и ведомственными наградами, иными наградами и знаками отличия;

сведения об отпусках и командировках;

сведения о прохождении аттестации и сдаче квалификационного экзамена;

сведения об участии в конкурсных процедурах, включении в кадровый резерв;

информация о проведении служебных проверок, наложении дисциплинарных взысканий;

сведения о поощрении;

сведения о доходах (расходах), имуществе и обязательствах имущественного характера, в том числе супруга (супруги) и несовершеннолетних детей;

сведения о временной нетрудоспособности;

реквизиты идентификационного номера налогоплательщика (ИНН);

реквизиты страхового номера индивидуального лицевого счета в Пенсионном фонде Российской Федерации (СНИЛС);

реквизиты полиса обязательного медицинского страхования;

сведения о социальных льготах;

информация о доходах, выплатах и удержаниях;

номера банковских счетов;

номер служебного телефона;

фото;

адрес электронной почты;

сведения об адресах сайтов или страниц сайтов, на которых субъект персональных данных разместил общедоступную информацию, а также данные, позволяющие его идентифицировать.

2. Персональные данные физических лиц, обрабатываемые в связи с рассмотрением обращений:

фамилия, имя, отчество;

адрес местожительства (места пребывания);

иные персональные данные, содержащиеся в обращениях.

3. Персональные данные, обрабатываемые в целях заключения договоров и ведения расчетов с физическими лицами:

фамилия, имя, отчество;

паспортные данные (серия, номер, когда и кем выдан);

адрес местожительства (места пребывания);

реквизиты идентификационного номера налогоплательщика (ИНН);

реквизиты страхового номера индивидуального лицевого счета в Пенсионном фонде Российской Федерации (СНИЛС);

информация о выплатах;

номера банковских счетов.

4. Персональные данные, обрабатываемые в целях аккредитации журналистов при администрации поселения:

фамилия, имя, отчество;

место работы, должность;

контактные телефоны;

адрес электронной почты;

фото.

5. Персональные данные, обрабатываемые при сборе документов, необходимых для установления (назначения) и выплаты пенсии за выслугу лет лицам, замещавшим должности муниципальной службы в администрации поселения, назначения и выплаты доплаты к пенсии лицам, замещавшим должность главы администрации Харьковского сельского поселения:

фамилия, имя, отчество;

место жительства и дата регистрации по месту жительства, место фактического проживания;

реквизиты страхового номера индивидуального лицевого счета в Пенсионном фонде Российской Федерации (СНИЛС);

реквизиты идентификационного номера налогоплательщика (ИНН);

данные российского паспорта (серия, номер, когда и кем выдан);

номера контактных телефонов;

сведения о месячном денежном содержании, учитываемом по должности муниципальной службы, муниципальной должности;

сведения о периодах службы (работы) в должностях, учитываемых при назначении пенсии за выслугу лет, доплаты к пенсии;

сведения о размере получаемой пенсии, о получении (неполучении) доплат, иных постоянных социальных выплат;

данные военного билета;

данные трудовой книжки.

6. Правовое основание обработки персональных данных и сроки их хранения

Группа персональных данных	Основание для обработки персональных данных
1. Обработка персональных данных в ИСПДн администрации Харьковского сельского поселения	
Сведения о гражданах	Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»
2. Обработка персональных данных в ИСПДн администрации Харьковского сельского поселения	
Сведения о работнике	Статьи 85-90 Трудового Кодекса РФ, Налоговый Кодекс РФ.
Сведения о родственниках работника	

Приложение 15
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

Положение об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

1. Общие положения

1.1. Положение об организации режима обеспечения безопасности помещений администрации Харьковского сельского поселения (далее – Оператор), в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (далее – Положение) разработано в соответствии с Постановлением правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

1.2. Защита от проникновения посторонних лиц в помещения Оператора обеспечивается организацией порядка доступа, а также соответствующей инженерно-технической защитой помещений, а именно охранной сигнализацией и системой контроля и управления доступом.

2. Границы контролируемой зоны

2.1. Контролируемая зона – часть здания по адресу: Белгородская обл., Ровеньский р-н, с.Харьковское, ул. Центральная, 35, в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска.

3. Порядок доступа в помещения

3.1. Перечень лиц, доступ которых в помещения находящиеся в пределах границы контролируемой зоны, необходим для выполнения ими служебных (трудовых обязанностей) приведен в приложении 1 к настоящему приказу.

3.2. Неконтролируемое пребывание лиц в помещениях, находящихся в пределах границы контролируемой зоны, указанных в п. 3.1 настоящего Положения разрешено в период рабочего времени в присутствии лиц, имеющих право пребывания в данных помещениях, либо вне периода рабочего времени с письменного

разрешения ответственного за организацию обработки персональных данных или ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных.

3.3. Лица, не указанные в п. 3.1 настоящего Положения, допускаются в помещения в присутствии лиц, имеющих право пребывания в данных помещениях.

Приложение 1
к Положению об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения

Перечень
должностей служащих в администрации Харьковского сельского поселения, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным и имеющих право пребывания в помещениях контролируемой зоны для выполнения ими служебных (трудовых обязанностей)

1. Глава администрации Харьковского сельского поселения;
2. Заместитель главы администрации Харьковского сельского поселения;
3. Экономист-финансист администрации Харьковского сельского поселения.

Приложение 16
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

Правила работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей

Допуск для работы на автоматизированных рабочих местах (далее – АРМ) состоящих в составе информационной системы персональных данных (далее – ИСПДн) осуществляется на основании утвержденного перечня лиц, доступ которых к персональным данным, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей (далее – Пользователи ИСПДн).

Пользователь ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для хранения и записи информации, содержащей персональные данные (далее – ПДн), разрешается использовать только машинные носители информации, учтенные в журнале учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации.

Пользователь несет ответственность за правильность включения и выключения АРМ, входа и выхода в систему и за все свои действия при работе в ИСПДн.

Вход пользователя в систему осуществляется по выдаваемому ему электронному идентификатору и по персональному паролю.

При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов и иных вредоносных программ с использованием штатных антивирусных средств, установленных на АРМ. В случае обнаружения вирусов либо вредоносных программ пользователь ИСПДн обязан немедленно прекратить их использование и действовать в соответствии с требованиями инструкции по организации антивирусной защиты.

Каждый работник, участвующий в рамках своих служебных обязанностей в процессах обработки персональных данных в ИСПДн и имеющий доступ к АРМ, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

– Строго соблюдать установленные соответствующими инструкциями правила обеспечения безопасности информации в ИСПДн;

– Знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;

– Хранить в тайне свой пароль (пароли). Выполнять требования инструкции по организации парольной защиты в полном объеме;

– Хранить индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);

– Выполнять требования инструкции по организации антивирусной защиты в полном объеме;

– Немедленно известить ответственного за обеспечение безопасности персональных данных в случае утери электронного идентификатора или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

– Несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ;

– Отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования компонентов АРМ, а также перебоев в системе электроснабжения;

– Некорректного функционирования установленных на АРМ технических средств защиты;

– Непредусмотренных отводов кабелей и подключенных устройств.

Пользователю АРМ категорически запрещается:

– Использовать компоненты программного и аппаратного обеспечения АРМ в личных целях;

– Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения АРМ;

– Записывать и хранить конфиденциальную информацию (содержащую персональные данные) на неучтенных машинных носителях информации (гибких магнитных дисках, флэш-накопителях и т.п.);

– Оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

– Оставлять без личного присмотра на рабочем месте или в ином месте свой электронный идентификатор, машинные носители и распечатки, содержащие персональные данные;

– Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты;

– Размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации, содержащей персональные данные.

Приложение 17
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных

1. Общие положения

Настоящая инструкция определяет права, обязанности и ответственность лица, ответственного за организацию обработки персональных данных.

Ответственный за организацию обработки персональных данных в своей деятельности руководствуется:

– Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119;

– Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687;

– Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2. Обязанности

Ответственный за организацию обработки персональных данных обязан:

– Доводить до сведения работников положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к обеспечению безопасности персональных данных;

– Осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, а именно организовывать проведение периодических (не менее одного раза в год) проверок соответствия обработки персональных данных. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывать непосредственному руководителю в письменном виде;

– Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и/или осуществлять контроль за приемом и обработкой таких обращений и запросов.

3. Ответственность

За неисполнение (ненадлежащее исполнение) своих должностных обязанностей, предусмотренных настоящей инструкцией, ответственный за организацию обработки персональных данных несет персональную ответственность в соответствии с законодательством Российской Федерации.

4. Права

Ответственный за организацию обработки персональных данных имеет право:

– Требовать от работников письменных объяснений по фактам нарушения ими требований законодательства Российской Федерации, локальных актов о персональных данных и защите персональных данных;

– Вносить предложения непосредственному руководителю об отстранении работников от обработки персональных данных, применению к ним дисциплинарных взысканий, при обнаружении нарушения ими требований законодательства Российской Федерации, локальных актов по вопросам обработки персональных данных или требований к защите персональных данных.

Приложение 18
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных

1. Общие положения

Настоящая инструкция определяет права и обязанности лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – ИСПДн).

Лицо ответственное за обеспечение безопасности персональных данных в ИСПДн (далее – администратор информационной безопасности) это лицо, отвечающее за обеспечение заданных характеристик информации, содержащей персональные данные (конфиденциальности, целостности и доступности) в процессе их обработки в ИСПДн.

Администратор информационной безопасности в ИСПДн осуществляет контроль за выполнением требований нормативно-правовых и организационно-распорядительных документов по организации обработки и обеспечению безопасности персональных данных при их обработке в ИСПДн с использованием автоматизированных рабочих мест.

2. Обязанности администратора информационной безопасности

Администратор информационной безопасности обязан:

– Знать требования нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности персональных данных при их обработке в ИСПДн;

– Знать перечень обрабатываемых персональных данных, состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных.

– Уметь пользоваться средствами защиты информации и осуществлять их непосредственное администрирование;

– Еженедельно осуществлять резервное копирование информации, содержащей персональные данные (при необходимости);

– Обязан осуществлять периодический контроль за выполнением работниками эксплуатирующими ИСПДн (пользователями ИСПДн), мероприятий по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн;

– Участвовать в работе по проведению внутреннего контроля соответствия обработки персональных данных требованиям по защите информации;

– Обязан анализировать журнал системы защиты информации от несанкционированного доступа (НСД), проводить проверки электронного журнала обращений к информационным системам персональных данных;

– Обязан обеспечивать строгое выполнение требований по обеспечению защиты информации при организации технического обслуживания АРМ;

– Обязан вести журнал учета средств защиты информации, используемых в ИСПДн;

– Обязан присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию АРМ;

– Обязан проводить инструктаж пользователей ИСПДн по правилам работы с используемыми техническими средствами и средствами защиты информации в соответствии с технической документацией на используемые средства защиты;

– Обязан проводить мероприятия по организации антивирусной защиты;

– Осуществлять организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями, согласно инструкции по организации парольной защиты в информационных системах персональных данных;

– Обязан организовать ведение журнала учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации;

– Обязан немедленно сообщать ответственному за организацию обработки персональных данных, информацию об имевших место попытках несанкционированного доступа к информации и техническим средствам АРМ, а также принимать необходимые меры по устранению нарушений:

– Установить причины, по которым стал возможным НСД;

– Установить последствия, к которым привел НСД;

– Зафиксировать случай НСД в виде документа (акта, служебной записки и т.д.) с описанием причин НСД, предполагаемых или установленных нарушителей и последствий;

– Провести проверку настроек средств защиты информации и операционных систем на соответствие требованиям руководящих документов и разрешительной системы доступа пользователей к защищаемым информационным ресурсам и объектам доступа ИСПДн, при необходимости провести настройку;

– Провести инструктаж пользователей ИСПДн по выполнению требований по обеспечению защиты персональных данных.

3. Права администратора информационной безопасности.

Администратор информационной безопасности имеет право:

– Требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкции о порядке работы

пользователей в ИСПДн в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;

– Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн;

– Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности персональных данных к ответственному за организацию обработки персональных данных в ИСПДн и/или ответственному за эксплуатацию ИСПДн;

4. Ответственность администратора информационной безопасности

На администратора информационной безопасности возлагается персональная ответственность за качество проводимых им работ по обеспечению безопасности ПДн в ИСПДн;

Администратор информационной безопасности в ИСПДн несет ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение 19
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

Инструкция
по учету лиц, допущенных к работе с персональными данными в информационных системах персональных данных

1. Настоящая инструкция определяет порядок учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных администрации Харьковского сельского поселения (далее – ИСПДн).

2. Порядок допуска работника к работе с персональными данными:

— утверждение распоряжением о допуске к обработке персональных данных перечня должностей работников, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей (далее – Перечень);

— прохождение первичного инструктажа, включающего ознакомление со всеми нормативными документами, регламентирующими работу с персональными данными, согласно Инструкции по проведению инструктажа лиц, допущенных к работе с персональными данными с внесением соответствующей информации в Журнал учёта прохождения первичного инструктажа сотрудниками, допущенными к работе с персональными данными в ИСПДН;

— внесение записи в Журнал учёта прав доступа к ИСПДн.

3. Допуск работника к персональным данным прекращается:

— в случае обнаружения нарушений порядка обработки персональных данных до выяснения и устранения причин нарушений;

— в случае увольнения сотрудника с момента подписания приказа об увольнении;

— при изменении его служебных обязанностей с момента утверждения нового Перечня.

Приложение 20
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

Инструкция
по проведению инструктажа лиц, допущенных к работе с информационной системой персональных данных

1. Настоящая инструкция разработана с целью обеспечения безопасности персональных данных, обрабатываемых в информационных системах персональных данных администрации Харьковского сельского поселения (далее – ИСПДн).

2. При поступлении на работу сотрудника, которому для выполнения своих трудовых обязанностей необходим доступ к ИСПДн (далее – новый сотрудник), ответственный за организацию обработки персональных данных:

а) в соответствии с п.6 ч.1 ст.18.1 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» проводит ознакомление нового сотрудника с положениями законодательства Российской Федерации о персональных данных и локальными актами организации в отношении обработки персональных данных

б) знакомит нового сотрудника с ответственностью за неисполнение требований по обеспечению безопасности персональных данных в ИСПДн, предусмотренной действующим законодательством Российской Федерации;

в) отмечает в Журнале учета прохождения первичного инструктажа данные о проведении инструктажа.

3. Новый сотрудник может приступить к исполнению своих непосредственных трудовых обязанностей, связанных с обработкой персональных данных, только после успешного прохождения первичного инструктажа.

Приложение 21
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

ИНСТРУКЦИЯ
пользователя информационной системы, предназначенной для обработки информации, содержащей персональные

1. Общие положения

Настоящая инструкция разработана для обеспечения защиты персональных данных в администрации Харьковского сельского поселения (далее – ИСПДн).

Пользователями информационной системы, предназначенной для обработки информации, содержащей персональные данные (далее ИСПДн), являются сотрудники, допущенные к работе в ИСПДн, в соответствии с приказом об утверждении списка лиц, которым необходим доступ к ПДн для выполнения служебных (трудовых) обязанностей.

Наиболее вероятными каналами утечки информации для информационных систем персональных данных (ИСПДн) являются:

- несанкционированный доступ к информации, обрабатываемой в ИСПДн;
- хищение документов или технических средств с хранящейся в них информацией, а также отдельных носителей информации;
- просмотр информации с экранов дисплеев мониторов и других средств ее отображения с помощью оптических устройств;
- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности обмена, в том числе электромагнитного, через специально внедренные электронные и программные средства («закладки»).

Работа с персональными данными строится на следующих принципах:

- принцип персональной ответственности - в любой момент времени за каждый документ (не зависимо от типа носителя: бумажный, электронный) должен отвечать и распоряжаться конкретный работник;
- принцип контроля и учета - все операции с документами должны отражаться в соответствующих журналах (передача из рук в руки, снятие копии и т.п.).

2. Обязанности работников, имеющих доступ к ПДн

Работники, получившие доступ к персональным данным, обязаны хранить в тайне сведения ограниченного распространения, ставшие им известными во время работы или иным путем, и пресекать действия других лиц, кото-

рые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки персональных данных немедленно информировать руководителя структурного подразделения, руководителя отдела информационной безопасности.

Персональные данные не подлежат разглашению (распространению). Прекращение доступа к такой информации не освобождает работника от взятых им обязательств по неразглашению сведений ограниченного распространения.

В случае оставления занимаемой должности работник обязан вернуть все документы и материалы, относящиеся к деятельности подразделения, организации. В том числе: отчеты, инструкции, переписку, списки работников, компьютерные программы, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к деятельности ПетрГУ, полученные в течение срока работы.

Работники при работе с персональными данными обязаны:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;
- выполнять требования администратора безопасности, касающиеся защиты информации;
- знать и строго выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на персональных компьютерах;
- хранить в тайне свой аутентификатор (пароль доступа в автоматизированную систему, либо ключевой носитель), а также информацию о системе защиты, установленной в ИСПДн;
- контролировать обновление антивирусных баз и в случае необходимости сообщать о необходимости обновления администратору безопасности, ответственному за антивирусную защиту автоматизированной системы.

Немедленно ставить в известность руководителя подразделения, руководителя сектора информационной безопасности:

- при подозрении компрометации личных ключей и паролей;
- нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах ПЭВМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к защищенной ИСПДн;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;
- в случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции, выхода из строя или неустойчивого функционирования узлов ПЭВМ или периферийных устройств (принтера и т.п.), а также перебоев в системе

электроснабжения, некорректного функционирования установленных в автоматизированной системе технических средств защиты ставить в известность ответственного за техническое обслуживание и (или) ответственного за обслуживание программного обеспечения.

Ставить в известность сотрудников отдела технического обслуживания компьютерной техники или сотрудников отдела информационной безопасности при:

- необходимости обновления антивирусных баз;
- обновлении программного обеспечения;
- проведении регламентных работ, модернизации аппаратных средств или изменении конфигурации ИСПДн;
- необходимости вскрытия системных блоков персональных компьютеров входящих в состав ИСПДн;
- резервном копировании информации;
- и т.д.

Вынос ПЭВМ, на которой проводилась обработка персональных данных, за пределы территории здания с целью их ремонта, замены и т. п. без согласования с руководителем подразделения, запрещен.

ПЭВМ, используемые для работы с персональными данными, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана видеомонитора, не имеющими отношения к конкретно обрабатываемой информации работниками.

Запрещается:

- передавать, кому бы то ни было (в том числе родственникам) устно или письменно сведения ограниченного распространения;
- использовать сведения ограниченного распространения при подготовке открытых публикаций, докладов, научных работ и т.д.;
- выполнять работы с документами ограниченного распространения на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения руководителя;
- передавать или принимать без расписки документы ограниченного распространения;
- оставлять на рабочих столах, в столах и незакрытых сейфах документы ограниченного распространения, а также оставлять незапертыми и неопечатанными после окончания работы сейфы, помещения и хранилища с документами конфиденциального характера;
- использовать компоненты программного и аппаратного обеспечения ИСПДн подразделения в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства;

- осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить персональные данные на неучтенных съемных носителях информации;
- оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок - ставить в известность руководителя своего подразделения, ответственного за техническое и (или) программное обеспечение, сотрудников отдела информационной безопасности.

3. Ответственность

Пользователь несет ответственность за соблюдение требований настоящей инструкции, а также других нормативных документов в области защиты информации. За разглашение информации ограниченного распространения, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

За разглашение информации ограниченного распространения, нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

Приложение 22
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

Инструкция
пользователя информационной системы персональных данных при возникновении нештатных ситуаций

1. Общие положения

Данная инструкция призвана регламентировать порядок действий пользователя информационной системы персональных данных администрации Харьковского сельского поселения (далее — ИСПДн), при возникновении внештатных ситуаций.

Инструкция утверждается распоряжением главы Администрации. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн Администрации, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.

Задачей данной Инструкции является определение мер защиты от прерывания и определение действий восстановления в случае прерывания.

Действие настоящей Инструкции распространяется на всех сотрудников Администрации, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в два года.

2. Порядок действий при возникновении аварийной ситуации

В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн.

Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование сотрудником в «Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и про-

граммных средств информационной системы персональных данных» (Приложение 25 к Постановлению «Об утверждении перечня мер , направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами»).

В кратчайшие сроки, не превышающие одного рабочего дня, ответственный за обеспечение информационной безопасности, администратор баз данных или другой назначенный ответственным за реагирование сотрудник предпринимает меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. При необходимости привлекаются квалифицированные сотрудники сторонних организаций с целью восстановления работоспособности в кратчайшие сроки.

Уровни реагирования на инцидент

При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

Уровень 1 – **Незначительный инцидент**. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.

Уровень 2 – **Авария**. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками.

К авариям относятся следующие инциденты:

Отказ элементов ИСПДн и средств защиты из-за:

- повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей;
- сбоя системы кондиционирования;
- других физических повреждений элементов ИСПДн, критичных для функционирования всей ИСПДн.

Уровень 3 – **Катастрофа**. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа.

К катастрофам относятся следующие инциденты:

- пожар в здании;
- взрыв;
- просадка грунта с частичным обрушением здания;
- массовые беспорядки в непосредственной близости от Объекта.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций

3.1. Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Все критичные помещения Администрации (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Порядок предотвращения потерь информации и организации системы жизнеобеспечения ИСПДн описан в «Порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации».

3.2. Организационные меры

Ответственные за реагирование сотрудники ознакомляют всех сотрудников Администрации, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий 3х рабочих дней с момента выхода нового сотрудника на работу.

Должно быть проведено обучение сотрудников Администрации, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций.

Сотрудники, ответственные за обеспечение безопасности ИСПДн должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов ИСПДн.

Приложение 23
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

ИНСТРУКЦИЯ
по обработке персональных данных без использования средств автоматизации

1. Общие положения.

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому гражданину, обратившемуся в администрации Харьковского сельского поселения, или сотруднику (далее – субъекту персональных данных) администрации Харьковского сельского поселения.

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.

Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные настоящим Положением, должны применяться с учетом требований Постановления Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 г. № 687, а также требований нормативных правовых актов федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации.

2. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации.

3.

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники администрации Харьковского сельского поселения или лица, осуществляющие такую обработку по договору с администрацией Харьковского сельского поселения), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется администрацией Харьковского сельского поселения без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами администрации Харьковского сельского поселения.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

− типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес учреждения, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых учреждением способов обработки персональных данных;

− типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации,– при необходимости получения письменного согласия на обработку персональных данных;

− типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

При ведении журналов (журналов регистрации, журналов посещений), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в помещения администрации Харьковского сельского поселения или в иных аналогичных целях, должны соблюдаться следующие условия:

− необходимость ведения такого журнала должна быть предусмотрена актом администрации Харьковского сельского поселения , содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за

ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных;

− копирование содержащейся в таких журналах информации не допускается;

− персональные данные каждого субъекта персональных данных могут заноситься в такой журнал не более одного раза в каждом случае пропуска субъекта персональных данных.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, зачеркивание, стирание).

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя,– путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

3. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

Приложение 24
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

ИНСТРУКЦИЯ
по работе с инцидентами информационной безопасности

Ответственность за выявление инцидентов ИБ и реагирование на них в администрации Харьковского сельского поселения возлагается на администратора информационной безопасности.

Администратор информационной безопасности имеет полномочия инициировать проведение служебных проверок (ходатайствовать о наложении дисциплинарного взыскания перед главой администрации Харьковского сельского поселения) по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации.

Администратор информационной безопасности обязан вести журнал учёта инцидентов ИБ (событий, действий повлекших за собой риски безопасности защищаемой информации и создающих предпосылки к нарушению критериев безопасности информации). Сюда относятся нарушения пользователями положений организационно-распорядительных документов, установленных порядков и технологии работы в ИС, разглашение защищаемой информации и любые действия, направленные на это, не антропогенные инциденты (сбои ПО, стихийные бедствия).

В журнале в свободной форме описывается инцидент с указанием следующих данных:

- даты и времени;
- причин (умышленные и неумышленные действия, не антропогенные инциденты и т.п.) и описания инцидента и задействованных лиц;
- информации о последствиях;
- информации о возможных последствиях (экономические убытки (в связи с заменой СЗИ, повторной аттестации; временные и трудозатраты на устранение последствий, нарушение работы пользователей, ущерб субъектам ПДн и юридические последствия для администрации Харьковского сельского поселения и т.п.).

Журнал с данным отчётом об инциденте предоставляется на ознакомление ответственному за организацию обработки персональных данных для принятия мер по предотвращению рецидива (возникновения повторного инцидента).

В случае возникновения рецидива со стороны пользователя или администратора информационной безопасности, по ходатайству ответственного за организацию обработки персональных данных главой администрации Харьковского сельского поселения накладывается дисциплинарное взыскание.

Сокрытие нарушений и инцидентов ИБ, вызванных любыми должностными лицами администрации Харьковского сельского поселения, является гру-

бым нарушением трудовой дисциплины. Сокрытие нарушений и инцидентов ИБ, вызванных действиями администратора информационной безопасности и ответственным за организацию обработки персональных данных, является грубейшим нарушением дисциплины, и при выяснении данного факта должно строго наказываться.

Любой сотрудник должен согласовывать следующие действия с администратором информационной безопасности:

- замена прикладного оборудования (мышь, клавиатура, принтер, монитор);
- установка дополнительного ПО;
- изменение сетевых настроек рабочего места;
- замена, изменение любой аппаратной части рабочего места.

Ответственный за организацию обработки персональных данных не может требовать от администратора информационной безопасности действий, направленных на нарушение настоящего руководства и других организационно-распорядительных документов администрации Харьковского сельского поселения, требовать сокрытия инцидентов ИБ, вызванных любыми должностными лицами, требовать сообщения ему паролей на средства защиты информации и нарушения установленного разграничения прав по допуску к информационным ресурсам, установленным матрицей доступа к информационными ресурсам ИС.

Приложение 25
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

Инструкция
ответственного за эксплуатацию информационной системы персональных данных

1. Общие положения.

1.1. Ответственный за эксплуатацию информационной системы персональных данных (далее – ИСПДн) в муниципальном автономном учреждении «Комплексный центр социального обслуживания населения Ярковского района» (далее – Учреждение) назначается приказом руководителя.

1.2. Методическое руководство работой ответственного за эксплуатацию ИСПДн осуществляется ответственным за организацию обработки персональных данных в Учреждении.

1.3. Ответственный за эксплуатацию в своей работе руководствуется положениями, руководящими и нормативными документами ФСТЭК и ФСБ России по защите информации и организационно-распорядительными документами для данной ИСПДн, а также иными нормативными документами в части защиты информации.

1.4. Ответственный за эксплуатацию ИСПДн несет ответственность за свои действия, и действия сотрудников вверенного структурного подразделения в соответствии с действующим законодательством РФ.

2. Функции ответственного за эксплуатацию ИСПДн.

2.1. Осуществлениеконтроля за целевым использованием ИСПДн, всех периферийных устройств и технических средств, входящих в состав ИСПДн.

2.2. Контроль за отсутствием в период обработки защищаемой информации в помещении, где осуществляется обработка, посторонних лиц, не допущенных к обрабатываемой информации.

2.3. Контроль использования сотрудниками структурных подразделений, эксплуатирующими ИСПДн, средств защиты информации, установленных на АРМ, входящих в состав ИСПДн.

2.4. Контроль за правильностью использования и хранения сотрудниками структурных подразделений, эксплуатирующими ИСПДн, машинных носителей информации и документов, содержащих персональные данные.

2.5. Представление заявок на пользователей, допускаемых к защищаемым

ресурсам ИСПДн, с целью закрепления за ними носителей информации устройств блокировки, паролей и других средств разграничения доступа к информации, а также прав пользования средствами вычислительной техники.

2.6. Организация повышения уровня осведомленности подчиненных должностных лиц по вопросам информационной безопасности.

3. Обязанности ответственного за эксплуатацию ИСПДн.

3.1. Четко знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководств по защите информации и распоряжений, регламентирующих порядок действий по защите информации.3.2. Обеспечивать функционирование ИСПДн в пределах возложенных на него функций.

3.3. Обеспечивать контроль выполнения установленного комплекса мероприятий по обеспечению безопасности ПДн.

3.4. Контролировать целостность печатей (пломб) на устройствах ИСПДн.

3.5. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств ИСПДн и отправке их в ремонт.

3.6. Присутствовать при выполнении технического обслуживания ИСПДн при установке (модификации) программного обеспечения.

3.7. Информировать администратора информационной безопасности о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

3.8. Контролировать соответствие состава ИСПДн техническому паспорту на ИСПДн.

Приложение 26
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

Инструкция
по организации антивирусной защиты информационных систем персональных данных

Настоящая инструкция определяет порядок организации антивирусной защиты на информационных систем персональных данных (далее -ИСПДн).

1. Общие положения

1.1. Настоящая Инструкция предназначена для администратора ИСПДн, ответственного за защиту информации на объекте информатизации и пользователей, эксплуатирующих ИСПДн.

1.2. Инструкция устанавливает требования и ответственность при организации защиты информации, в ИСПДн от программно-математических воздействий и разрушающего воздействия компьютерных вирусов.

1.3. В целях закрепления знаний по вопросам практического исполнения требований Инструкции, разъяснения возникающих вопросов, проводятся организуемые Администратором ИСПДн семинарыи персональные инструктажи (при необходимости) пользователей ИСПДн.

1.4. Инструкция регулирует как вопросы организации антивирусной защиты, так и требования к порядку проведения антивирусного контроля при работе в ИСПДн.

2. Применение средств антивирусной защиты

2.1. Антивирусный контроль дисков и файлов ИСПДн после загрузки компьютера должен проводиться в автоматическом режиме (периодическое сканирование или мониторинг).

2.2. Периодически, не реже одного раза в неделю, должен проводиться полный антивирусный контроль всех дисков и файлов ИСПДн (сканирование).

2.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая информация по телекоммуникационным каналам связи, на съемных носителях (магнитных дисках, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед отправкой (записью на съемный носитель).

2.4. Установка (обновление и изменение) системного и прикладного программного обеспечения осуществляется в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных.

2.5. Обновление антивирусных баз должно проводиться регулярно, но не реже, чем 1 раз в неделю.

3. Функции Администратора ИСПДн по обеспечению антивирусной безопасности

Администратор ИСПДн обязан:

3.1. При необходимости проводить инструктажи пользователей ИСПДн по вопросам применения средств антивирусной защиты.

3.2. Настраивать параметры средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств.

3.3. Предварительно проверять устанавливаемое (обновляемое) программное обеспечение на отсутствие вирусов.

3.4. При необходимости производить обновление антивирусных программных средств.

3.5. Производить получение и рассылку (при необходимости) обновлений антивирусных баз.

3.6. При необходимости разрабатывать инструкции по работе пользователей с программными средствами САЗ.

3.7. Проводить работы по обнаружению и обезвреживанию вирусов.

3.8. Участвовать в работе комиссии по расследованию причин заражения ПК и серверов.

3.9. Хранить эталонные копии антивирусных программных средств.

3.10. Осуществлять периодический контроль за соблюдением пользователями ПК требований настоящей Инструкции;

3.11. Разрабатывать инструкции по работе пользователей с системой антивирусной защиты информации.

3.12. Проводить периодический контроль работы программных средств системы антивирусной защиты информации на ПК (серверах).

4. Функции пользователей

Пользователи ИСПДн:

4.1. Получают по ЛВС или от Администратора ИСПДн носители с обновлениями антивирусных баз (в случае отсутствия механизмов централизованного распространения антивирусных баз).

4.2. Проводят обновления антивирусных баз на ПК (в случае отсутствия механизмов централизованного распространения антивирусных баз).

4.3. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник подразделения самостоятельно или вместе с администратором ИСПДн должен провести внеочередной антивирусный контроль ПК.

При необходимости он должен пригласить Администратора ИСПДн для определения факта наличия или отсутствия компьютерного вируса.

4.4. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

4.4.1. приостановить работу;

4.4.2. немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя подразделения и Администратора ИСПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

4.4.3. совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

4.4.4. провести лечение или уничтожение зараженных файлов(при необходимости для выполнения требований данного пункта пригласить Администратора ИСПДн);

4.4.5. в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл на съемном носителе Администратору ИСПДн для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку;

4.4.6. по факту обнаружения зараженных вирусом файлов составить служебную записку Администратору ИСПДн, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации и выполненные антивирусные мероприятия.

5. Ответственность при организации антивирусной защиты

5.1.1. Ответственность за организацию антивирусной защиты ИСПДн и установление порядка ее проведения, в соответствии с требованиями настоящей Инструкции, возлагается на ответственного за защиту информации в ИСПДн.

5.1.2. Ответственность за поддержание установленного порядка и соблюдение требований настоящей Инструкции возлагается на Администратора в ИСПДн и пользователей (операторов).

5.1.3. Периодический контроль за выполнением всех требований настоящей Инструкции, и состоянием антивирусной защиты осуществляется Администратором ИСПДн.

Приложение 27
к распоряжению администрации
Харьковского сельского поселения
от 01.12.2022г. №85

ПРАВИЛА
работы с обезличенными данными

1.Общие положения

Настоящие Правила работы с обезличенными персональными данными администрации Харьковского сельского поселения разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и определяют порядок работы с обезличенными данными администрации Харьковского сельского поселения.

2.Термины и определения

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» в настоящих Правилах используются следующие понятия:

- персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (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;
- обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

3.Условия обезличивания

Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных администрации Харьковского сельского поселения и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

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 (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только населенный пункт)
- деление сведений на части и обработка в разных информационных системах;
- другие способы.

Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

4. Порядок работы с обезличенными персональными данными

Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- парольной политики;
- антивирусной политики;
- правил работы со съемными носителями (если они используется);
- правил резервного копирования;
- правил доступа в помещения, где расположены элементы информационных систем.

При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- правил хранения бумажных носителей;
- правил доступа к ним и в помещения, где они хранятся.