АДМИНИСТРАЦИЯ ПЕРЕКОПСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ
КЛЕТСКОГО МУНИЦИПАЛЬНОГО РАЙОНА
ВОЛГОГРАДСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

от 20.03.2024 г. № 9-р х. Перекопка

О назначении ответственного
за информационную безопасность

Руководствуясь Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а так же принимая во внимание представление прокуратуры от 28.02.2024 № 7-31-2024 об устранении нарушений законодательства о защите информации

1. Назначить ответственным за информационную безопасность в администрации Перекопского сельского поселения заместителя главы администрации Перекопского сельского поселения Баксарову Анастасию Викторовну.
2. Возложить на сотрудника, указанного в пункте 1 настоящего распоряжения, выполнение следующих обязанностей:
- организация комплексной защиты информации в администрации Перекопского сельского поселения;
- оценка рисков при использовании сотрудниками администрации Перекопского сельского поселения информационных систем;
- организация исполнения и применения процедур безопасности при использовании сотрудниками администрации Перекопского сельского поселения информационных систем;
- организация обновления программ безопасности (антивирусных программ, версий программного обеспечения);
- обеспечение восстановления информационных систем после атак или иных отказов в работе;
- разработка проектов локальных нормативных актов в сфере обеспечения информационной безопасности при использовании информационных систем в администрации Перекопского сельского поселения;
- систематическое разъяснение сотрудникам администрации Перекопского сельского поселения требований информационной безопасности, установленных законодательством РФ.
3. Утвердить меры по обеспечению безопасности персональных данных, реализуемых в рамках защиты персональных данных с учетом актуальных угроз безопасности и применяемых информационных технологий (Приложение 1).
4. Утвердить план мероприятий по защите персональных данных (Приложение 2).
5. Утвердить форму журнала учета событий информационной безопасности (Приложение 3).
6. Контроль за выполнением настоящего распоряжения оставляю за собой.

Глава Перекопского
сельского поселения С.Г. Кудрин

С распоряжением ознакомлены:

Баксарова А.В._____

Мараховская С.В. _____

Гурко Р.Г. _____

Нестерова С.Н. _____

Фролова А.Ю._____

Кудрин М.С. _____

Прокопенко С.А._____

Мальцева О.А._____

Колесниченко Л.В._____

Вохминцева Н.А. _____

Крутикова М. В. _____

Глазунова Л.В._____

Чудина Л.В. _____

Мороз И.А_____

Приложение 1

Меры по обеспечению безопасности персональных данных, реализуемых в рамках защиты персональных данных с учетом актуальных угроз безопасности и применяемых информационных технологий

N	Перечень мер	Цель реализации
1	идентификация и аутентификация субъектов доступа и объектов доступа	обеспечение присвоения субъектам и объектам доступа уникального признака (идентификатора), сравнения, предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверка принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности)
2	управление доступом субъектов доступа к объектам доступа	обеспечение управления правами и привилегиями субъектов доступа, разграничения доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также контроля за соблюдением этих правил
3	ограничение программной среды	обеспечение установки и (или) запуска только разрешенного к использованию в информационной системе программного обеспечения или исключение возможности установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения
4	защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные	исключение возможности несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированного использования съемных машинных носителей персональных данных
5	регистрация событий безопасности	обеспечение сбора, записи, хранения и защиты информации о событиях безопасности в информационной системе, а также возможности просмотра и анализа информации о таких событиях и реагирования на них
6	антивирусная защита	обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации

		средств защиты информации, а также реагирование на обнаружение этих программ и информации
7	обнаружение (предотвращение) вторжений	обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия
8	контроль (анализ) защищенности персональных данных	обеспечение контроля уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных
9	обеспечение целостности информационной системы и персональных данных	обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных
10	обеспечение доступности персональных данных	авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы
11	защита среды виртуализации	исключение несанкционированного доступа к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействия на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям
12	защита технических средств	Исключение несанкционированного доступа к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы, и в помещения, в

		которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей
13	защита информационной системы, ее средств, систем связи и передачи данных	обеспечение защиты персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных
14	выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них	обеспечение обнаружения, идентификации, анализа инцидентов в информационной системе, а также принятия мер по устранению и предупреждению инцидентов
15	управление конфигурацией информационной системы и системы защиты персональных данных	обеспечение управления изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирования этих изменений

Приложение 2

План мероприятий по защите персональных данных
в администрации Перекопского сельского поселения на 2024 год

№ п/п	Наименование мероприятия	Срок выполнения	Ответственный за выполнение	Примечание
1.	Актуализация локальных актов, регламентирующих защиту персональных данных	По мере необходимости		Необходимость определяется внесением изменений в действующее законодательство РФ
2.	Определение уровня защищенности персональных данных при их обработке в информационных системах персональных данных (ИСПДн)	По мере необходимости		Проводится при оформлении доступа к ИСПДн, при выявлении в ИСПДн изменения ее состава или структуры
3.	Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных	Ежеквартально		Проводится путем непосредственной проверки на рабочих местах ответственных сотрудников
4.	Проверка сведений, содержащихся в уведомлении об обработке персональных данных, размещенных в Реестре операторов персональных данных на сайте Роскомнадзора	По мере необходимости		В Роскомнадзор направляется актуальная редакция уведомления об обработке персональных данных
5.	Уничтожение персональных данных при достижении целей их обработки и сроков хранения	ежемесячно		Проводится по представлению руководителей структурных подразделений
6.	Контроль эффективности средств защиты персональных данных	декабрь		При необходимости привлекается организация, имеющая лицензию на осуществление деятельности по технической защите конфиденциальной информации

Приложение 3

Журнал
учета событий информационной безопасности

Журнал начат « » _____ 20__ г.	Журнал завершен « » _____ 20__ г.
Должность	Должность
_____/	_____/
_____/	_____/

N п/п	Дата события	Основания возникновения события	Описание события (мероприятия)	Характеристика события	(ФИО, субъекта)	Должность, ФИО и подпись ответственного за ведение журнала	Примечание