

# АДМИНИСТРАЦИЯ

# ТУПИКОВСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ

# ХОЛМ – ЖИРКОВСКОГО РАЙОНА СМОЛЕНСКОЙ ОБЛАСТИ

**РАСПОРЯЖЕНИЕ**

от 29 февраля 2024 года № 5

|  |  |
| --- | --- |
| Об утверждении перечня принимаемых организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных в Администрации Тупиковского сельского поселения Холм-Жирковского района Смоленской области |  |

В соответствии с приказом ФСТЭК РФ 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»:

1. Утвердить перечень принимаемых организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных в Администрации Тупиковского сельского поселения Холм-Жирковского района Смоленской области согласно приложению.

2. Настоящее распоряжение вступает в силу со дня подписания.

Глава муниципального образования

Тупиковского сельского поселения

Холм-Жирковского района

Смоленской области М.В. Козел

Приложение

к распоряжению Администрации

Тупиковского сельского поселения

Холм-Жирковского района

Смоленской области

от 29.02.2024 № 5

**Перечень**

**принимаемых организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных в Администрации Тупиковского сельского поселения Холм-Жирковского района**

 **Смоленской области**

1. Идентификация и аутентификация субъектов доступа и объектов доступа.

1.1. Идентификация и аутентификация пользователей, являющихся сотрудниками Администрации Тупиковского сельского поселения Холм-Жирковского района Смоленской области (далее – Администрация).

1.2. Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов.

1.3. Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.

1.4. Защита обратной связи при вводе аутентификационной информации.

2. Управление доступом субъектов доступа к объектам доступа.

2.1. Управление (заведение, активация, блокирование и уничтожение) учетными записями сотрудников Администрации.

2.2. Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа.

2.3. Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами.

2.4. Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы.

2.5. Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.

2.6. Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе).

2.7. Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети.

2.8. Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).

2.9. Обеспечение доверенной загрузки средств вычислительной техники.

3. Регистрация событий безопасности.

3.1. Определение событий безопасности, подлежащих регистрации, и сроков их хранения.

3.2. Определение состава и содержания информации о событиях безопасности, подлежащих регистрации.

3.3. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения.

3.4. Защита информации о событиях безопасности.

4. Антивирусная защита.

4.1. Реализация антивирусной защиты.

4.2. Обновление базы данных признаков вредоносных компьютерных программ (вирусов).

5. Контроль (анализ) защищенности персональных данных.

5.1. Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей.

5.2. Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.

5.3. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.

5.4. Контроль состава технических средств, программного обеспечения и средств защиты информации.

6. Защита технических средств.

6.1. Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения Администрации, в которых они установлены.

6.2. Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

7. Защита информационной системы, ее средств, систем связи и передачи данных.

7.1. Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи.