|  |  |
| --- | --- |
|  | Приложение №22 к распоряжению администрациимуниципального образования Первомайский поссоветОренбургского района Оренбургской областиот \_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_ |

**Инструкция по парольной защите в информационных системах персональных данных администрации муниципального образования Первомайский поссовет Оренбургского района**

**1. Общие положения**

1.1. Настоящая инструкция по парольной защите в информационных системах персональных данных администрации муниципального образования Первомайский поссовет Оренбургского района (далее – Инструкция) является руководящим документом для пользователей информационных систем персональных данных (далее – ИСПДн) администрации муниципального образования Первомайский поссовет Оренбургского района (далее – Пользователь), указанных в Матрице доступа к информационным системам персональных данных администрации муниципального образования Первомайский поссовет Оренбургского района (приложение № 11 к настоящему распоряжению).

1.2. Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в ИСПДн администрации муниципального образования Первомайский поссовет Оренбургского района.

1.3. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн администрации муниципального образования Первомайский поссовет Оренбургского района и контроль за действиями Пользователей при работе с паролями возлагается на администратора безопасности информационных систем персональных данных администрации муниципального образования Первомайский поссовет Оренбургского района (далее – Администратор безопасности), назначенного настоящим распоряжением.

2**. Требования к парольной защите**

2.1. Личные пароли должны генерироваться и распределяться централизованно либо выбираться Пользователями самостоятельно с учетом следующих требований:

2.1.1. обеспечение конфиденциальности пароля;

2.1.2. минимальная длина пароля должна быть не менее 6 символов;

2.1.3. пароль не должен быть подвержен легкому угадыванию или вычислению с использованием персональной информации, связанной с владельцем пароля (имен, номеров телефонов, дат рождения и т.д.);

2.1.4. пароль не должен содержать последовательных идентичных символов и не состоять из полностью числовых или полностью буквенных групп;

2.1.5. при смене пароля новое значение должно отличаться от предыдущего, должно быть исключено повторное или цикличное использование старых паролей.

2.2. Полная плановая смена паролей Пользователей должна проводиться регулярно, не реже одного раза в 360 дней.

2.3. Внеплановая смена личного пароля или удаление учетной записи Пользователя в случае прекращения его полномочий должна производиться Администратором безопасности немедленно после окончания последнего сеанса работы данного Пользователя с системой.

2.4. Внеплановая полная смена паролей всех Пользователей должна производиться в случае прекращения полномочий Администратора безопасности, а также при наличии любого признака возможной компрометации системы или пароля.

2.5. В случае компрометации личного пароля (утери пароля или передачи его другому лицу) Пользователя должны быть немедленно предприняты меры в соответствии с пунктом 2.3 или пунктом 2.4 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

2.6. Хранение Пользователем значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе Администратора безопасности или руководителя подразделения, эксплуатирующего информационную систему персональных данных администрации муниципального образования Первомайский поссовет Оренбургского района.

2.7. Должно быть исключено коллективное использование индивидуальных паролей.

2.8. Запрещается включать пароли в автоматизированный процесс регистрации (например, с использованием хранимых макрокоманд или функциональных клавиш).

2.9. Контроль за действиями Пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на Администратора безопасности.

**3. Контроль в отношении паролей**

3.1. Предоставление паролей должно контролироваться посредством формализованного процесса управления, который должен предусматривать:

3.1.1. в случаях, когда от Пользователей требуется управление собственными паролями, необходимо обеспечивать предоставление безопасного первоначального временного пароля, который Пользователя принуждают сменить при первой регистрации в системе. Временные пароли используются в тех случаях, когда Пользователи забывают свой личный пароль, и должны выдаваться только после идентификации Пользователя;

3.1.2. обеспечение безопасного способа выдачи временных паролей Пользователям. Следует избегать использования незащищенных (открытый текст) сообщений электронной почты или сообщений по электронной почте от третьей стороны. Пользователям необходимо подтверждать получение паролей.

3.1.3. Пароли никогда не следует хранить в компьютерной системе в незащищенной форме. При необходимости следует рассматривать возможности других технологий для идентификации и аутентификации Пользователя, такие как биометрия (проверка отпечатков пальцев), проверка подписи, и использование аппаратных средств идентификации (чип-карт, микросхем).

\_\_\_\_\_\_\_\_\_\_\_