ПОРЯДОК
парольной защиты в информационных системах персональных данных в ГКУ Пензенской области «Ресурсный центр социального обслуживания населения Пензенской области»

2022 г.

Используемые сокращения

АРМ	-	автоматизированное рабочее место;
ИСПДн	-	информационная система персональных данных;
ЛВС	-	локальная вычислительная сеть;
ПДн	-	персональные данные;
СВТ	-	средства вычислительной техники;
ФИО	-	фамилия, имя, отчество;
ЭЦП	-	электронно-цифровая подпись.

1. Общие положения

1.1. Настоящий порядок включает в себя комплекс организационно-технических мер, регламентирующих организационно-техническое обеспечение процессов генерации, хранения, смены, уничтожения и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных ГКУ Пензенской области « Ресурсный центр социального обслуживания населения Пензенской области» (далее Центр).

1.2. Требования настоящего Порядка являются неотъемлемой частью комплекса мер безопасности и защиты информации в Центре.

1.3. Требования настоящего порядка распространяются на всех должностных лиц и сотрудников Центра, использующих в работе ИСПДн, а также всех видов программного обеспечения, используемого в Центре.

1.4. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в информационных системах персональных данных Центра возлагается на ответственного за организацию и проведение работ по защите информации.

2. Объекты парольной защиты

2.1. Паролями в Центре должны быть защищены следующие объекты:

- локальные учетные записи администраторов компьютеров;
- доменные учетные записи пользователей;
- учетные записи администраторов ИСПДн;
- учетные записи пользователей ИСПДн;
- учетные записи ИС сторонних организаций;
- учетные записи электронных почтовых ящиков;
- ЭЦП сотрудников.

3. Функции сотрудников

3.1. Непосредственное исполнение, организация и контроль исполнения требований настоящего Порядка осуществляется всеми пользователями ИСПДн.

3.2. Функции пользователей ИСПДн:

- надежное хранение используемых паролей;
- регулярная (с частотой, установленной настоящим Порядком) смена используемых паролей;
- выбор паролей с качеством, установленным настоящим порядком.

3.3. Функции администратора:

- организационно-методическое обеспечение процессов создания, смены и удаления паролей;
- создание учетных записей с формированием одноразового пароля;

- восстановление доступа к учетной записи (разблокирование) с формированием одноразового пароля;
- блокировка учетной записи (временная или постоянная);
- формирование заявок на создание учетных записей для стороннего программного обеспечения;
- текущий контроль действий пользователей по работе с паролями.

4. Требования к парольной информации

4.1. Личные пароли должны создаваться пользователями самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля могут присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего;
- личный пароль пользователь не имеет права сообщать никому.

4.2. Допускается хранение личных паролей в запечатанном конверте. На конверте указывается ФИО владельца пароля, а на местах склейки проставляется подпись владельца пароля. Опечатанные конверты с паролями исполнителей должны храниться в сейфе.

5. Меры обеспечения безопасности паролей

5.1. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в три месяца. В ИСПДн и в домене периодичность смены пароля устанавливается администратором информационной безопасности для автоматического вызова процедуры смены пароля.

5.2. Внеплановая смена личного пароля проводится пользователем самостоятельно. Блокирование учетной записи пользователя в ИСПДн и в домене в случае прекращения его полномочий (увольнение, переход на другую работу) должно производиться администратором информационной безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой.

5.3. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу, другие обстоятельства) администраторов и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой организации.

5.4. В случае компрометации личного пароля, пользователь должен немедленно довести информация о компрометации пароля до администратора информационной безопасности и до директора Центра.

5.5. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора информационной безопасности.

5.6. Пользователь и администратор безопасности несут ответственность за качество и своевременность выполнения задач и функций, возложенных на них в соответствии с настоящим Порядком.