Приложение 12
к приказу от 14.02.2022 № 8

МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ
«ЦЕНТР МОЛОДЕЖНЫХ ИНИЦИАТИВ»
КОРСАКОВСКОГО ГОРОДСКОГО ОКРУГА САХАЛИНСКОЙ ОБЛАСТИ
(МАУ «ЦМИ»)
Адрес: 694020, Сахалинская область, г.Корсаков, ул.Восточная, 29/2,
телефон: 8(42435)4-00-59, e-mail: mbu_cmi2016@mail.ru

УТВЕРЖДАЮ:
и.о. директора МАУ «ЦМИ»
_____ Д.М. Шпачук
Приказ № 8 от 14.02.2022

ПОЛОЖЕНИЕ
О ПАРОЛЬНОЙ ЗАЩИТЕ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИНОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В МУНИЦИПАЛЬНОМ АВТОНОМНОМ УЧРЕЖДЕНИИ «ЦЕНТР МОЛОДЕЖНЫХ ИНИЦИАТИВ» КОРСАКОВСКОГО ГОРОДСКОГО ОКРУГА САХАЛИНСКОЙ ОБЛАСТИ

Корсаков
2022

1. Общие положения

1.1. Настоящее Положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей на рабочих местах (далее - РМ) муниципального автономного учреждения «Центр молодежных инициатив» Корсаковского городского округа Сахалинской области (далее МАУ «ЦМИ»), а также контроль за действиями Пользователей и персонала при работе с паролями в МАУ «ЦМИ». Парольная защита требует соблюдения ряда правил, изложенных в настоящем Положении.

1.2. Целью настоящего Положения является определение требований МАУ «ЦМИ» к парольной защите информационных систем.

1.3. Положение распространяется на всех пользователей и информационные системы МАУ «ЦМИ», использующих парольную защиту.

2. Термины и определения.

РМ - в данном случае любое рабочее место, для работы с которым необходима аутентификация пользователя.

Пароль - секретный набор символов, используемый для аутентификации пользователя.

Пользователи - администратор и работники МАУ «ЦМИ», а также доступ к ресурсам сети Интернет.

Учетная запись - идентификатор пользователя, используемый для доступа к РМ.

3. Порядок парольной защиты информационных систем МАУ «ЦМИ».

3.1. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями РМ самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;
- 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 не менее чем в 6 позициях;
- личный пароль Пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

3.2. В случае, если формирование личных паролей Пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора. Для генерации «стойких» значений паролей могут применяться специальные программные средства.

3.3. При наличии технологической необходимости (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.) использования имен и паролей некоторых работников (Пользователей) в их отсутствие, такие работники обязаны сразу же после смены своих паролей сообщать руководителю их новые значения.

3.4. Внеплановая смена личного пароля Пользователя РМ в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться администратором немедленно после окончания последнего сеанса работы данного Пользователя с системой.

3.5. Внеплановая полная смена паролей всех Пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) администратора и других работников, которым по роду работы были предоставлены полномочия по управлению парольной защитой РМ.

3.6. Хранение Пользователем своих паролей на бумажном носителе не допускается.

3.7. Повседневный контроль за действиями Пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на администратора.

4. Роли и ответственность.

4.1. Пользователи:

4.1.1. Исполняют требования положения и несут ответственность за ее нарушение.

4.1.2. Информируют администратора парольной защиты обо всех ставших им известных случаях нарушения настоящего Положения.

4.2. Администратор парольной защиты:

4.2.1. Принимает обращения Пользователей по вопросам парольной защиты (например, блокировка учетных записей, нарушение положения и др.), ведет их учет.

4.2.2. Организует консультации Пользователей по вопросам использования парольной защиты.

4.2.3. Контролирует действия Пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования.

4.2.4. Отвечает за безопасное хранение паролей встроенных административных учетных записей.