Подписано цифровой подписью: Пальчук М.И.
DN: cn=Пальчук М.И., o=ГБПОУ РК "Романовский колледж индустрии гостеприимства", ou=Директор, email=043@crimeaedu.ru, c=RU
Дата: 2023.05.11 11:10:35 +03'00'

УТВЕРЖДАЮ
Директор
ГБПОУ РК «РКИГ»
_____ Пальчук М. И.
Приказ № 37 от 09.03.2023 г.

Инструкция
по организации парольной защиты информационной системы персональных данных обмена информацией с ИСПДн центра обработки данных ФГБУ ФЦТ

1 Общие положения

1.1 Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) при организации доступа к безопасности информационной системы персональных данных обмена информацией с ИСПДн центра обработки данных ФГБУ ФЦТ (далее - ИСПДн ОИ ФЦТ) ГБПОУРК «РКИГ» (далее - Учреждение).

1.2 Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей для доступа к ИСПДн ОИ ФЦТ Учреждения, возлагается на Администратора безопасности ИСПДн ОИ ФЦТ Учреждения (далее - Администратор безопасности).

1.3 Повседневный контроль за действиями пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на Администратора безопасности.

2 Порядок организации парольной защиты

2.1 Личные пароли должны генерироваться и распределяться централизованно Администратором безопасности с учетом следующих требований:

- длина пароля должна быть не менее шести символов, алфавит пароля - не менее 30 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки - от 3 до 10 попыток;
- блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации - от 3 до 15 минут;
- в числе символов пароля обязательно должны присутствовать латинские 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 не менее чем в 4-х позициях;
- личный пароль пользователь не имеет права сообщать никому.

2.2 Ответственность за правильность формирования и распределения паролей возлагается на Администратора безопасности.

2.3 Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 180 дней.

2.4 Внеплановая смена личного пароля или удаление (блокирование) учетной записи пользователя системы в случае прекращения его полномочий (увольнение и т.п.) должна производиться Администратором безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой.

2.5 В случае прекращения полномочий Администратора безопасности производится полная внеплановая смена всех паролей.

2.6 В случае компрометации личного пароля пользователя системы должны быть немедленно предприняты меры в соответствии с п. 2.4 или п. 2.5. настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

2.7 Хранение пользователем значений своих паролей на бумажном носителе допускается только в опечатанном печатью конверте в сейфе у Администратора безопасности.

2.8 Повседневный контроль за действиями исполнителей при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на Администратора безопасности.

2.9 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 ОТВЕТСТВЕННОСТЬ

3.1 Ответственность за соблюдение требований хранения и использования паролей возлагается на их владельца.

3.2 Ответственность за соблюдение требований, а также за своевременное информирование о необходимости смены паролей в подразделении возлагается на Администратора безопасности ИСПДн ОИ ФЦТ.

Ведущий специалист по защите информации А. О. Грибенников