Министерство образования, науки и молодежи Республики Крым
Государственное бюджетное специализированное учреждение Республики Крым
«Керченский межрегиональный социально-реабилитационный центр для несовершеннолетних»

УТВЕРЖДЕНО
Приказом и. о директора
ГБСУ РК «Керченский
МСРЦН» № 241-ХД
«01» 09 2020 года

ИНСТРУКЦИЯ
по организации парольной защиты в информационных системах ГБСУ РК «Керченский межрегиональный социально-реабилитационный центр для несовершеннолетних»

1 Общие положения

1.1. Настоящая инструкция регламентирует организационно техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаление учетных записей пользователей) в информационной системе персональных данных (далее – ИСПДн) Государственном бюджетном специализированном учреждении Республики Крым «Керченский межрегиональный социально-реабилитационный центр для несовершеннолетних» (далее –Центр).

1.2. Настоящая инструкция разработана в соответствии с руководящими и нормативными документами регуляторов Российской Федерации в области защиты персональных данных.

1.3. Пользователем ИСПДн (далее – Пользователь) является сотрудник центра, участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки персональных данных (далее – ПДн) и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты информации ИСПДн (далее – СЗИ).

1.4. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на системного администратора.

2. Организация парольной защиты

1.1. Личные пароли должны создаваться Пользователями самостоятельно.

1.2. В случае формирования личных паролей Пользователей централизованно, ответственность за правильность их формирования и распределения возлагается на Ответственного и Администратора в ИСПДн и на АРМ Пользователей соответственно.

1.3. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

1.4. Внеплановая смена личного пароля Пользователя или удаление учетной записи в случае прекращения его полномочий (увольнение, переход на другую должность в ИСПДн и т.п.) должна производиться Администратором и Ответственным немедленно после окончания последнего сеанса работы Пользователя в АРМ и в ИСПДн соответственно.

1.5. В ИСПДн устанавливается ограничение на количество неуспешных попыток аутентификации (ввода логина и пароля) Пользователя, равное 7, после чего учетная запись блокируется.

1.6. Разблокирование учетной записи осуществляется Администратором и Ответственным для учетных записей Пользователя для АРМ и для ИСПДн соответственно.

1.7. После 15 минут бездействия (неактивности) Пользователя в АРМ или ИСПДн происходит автоматическое блокирование сеанса доступа в АРМ и ИСПДн соответственно.

3. Требования к формированию паролей

Пользователи при формировании паролей должны руководствоваться следующими требованиями:

3.1. Длина пароля должна быть не менее 8 символов.

3.2. В пароле должны обязательно присутствовать символы не менее 3-х категорий из следующих:

- буквы в верхнем регистре;
- буквы в и нижнем регистре;
- цифры;
- специальные символы, не принадлежащие алфавитно-цифровому набору (например, !, @, #, $, &, *, % и т.п.).

3.3. Пароль не должен включать в себя легко вычисляемые сочетания символов (например, «112», «911» и т.п.), а также общепринятые сокращения (например, «ЭВМ», «ЛВС», «USER» и т.п.).

3.4. Пароль не должен содержать имя учетной записи Пользователя или наименование его АРМ, а также какую-либо его часть.

3.5. Пароль не должен основываться на именах и датах рождения Пользователя или его родственников, кличек домашних животных, номеров автомобилей, телефонов и т.д., которые можно угадать, основываясь на информации о Пользователе.

3.6. Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов (например, «1111111», «wwwww» и т.п.).

3.7. Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, «1234567», «qwerty» и т.п.).

3.8. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях.

4. Правила ввода паролей

Пользователи во время процедуры аутентификации (ввода логина и пароля) на АРМ и в ИСПДн должны руководствоваться следующими правилами:

4.1. Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.

4.2. Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и пр.).

4.3. В случае блокировки учетной записи Пользователя после превышения попыток ввода данных аутентификации (логина и пароля) в АРМ или ИСПДн, Пользователю необходимо уведомить Администратора или Ответственный соответственно для проведения процедуры генерации нового пароля.

5. Обязанности пользователей при работе с парольной защитой

Пользователи ИСПДн обязаны:

5.1. Четко знать и строго выполнять требования настоящей инструкции и других руководящих документов ГБОУ РК «КШИФ» по парольной защите.

5.2. Своевременно сообщать Ответственному и Администратору об утере, компрометации и несанкционированном изменении сроков действия паролей в АРМ и ИСПДн соответственно.

5.3. Ознакомиться под роспись с перечисленными в настоящей инструкции требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

6. Случаи компрометации паролей

6.1. Под компрометацией следует понимать:

- физическая утеря носителя с информацией;
- передача идентификационной информации по открытым каналам связи;
- проникновение постороннего лица в помещение физического хранения носителя парольной информации или алгоритма или подозрение на него (срабатывание сигнализации, повреждение устройств контроля НСД (слепков печатей), повреждение замков и т. п.);
- визуальный осмотр носителя идентификационной информации посторонним лицом;
- перехват пароля при распределении идентификаторов;
- сознательная передача информации постороннему лицу.

6.2. Действия при компрометации пароля:

- скомпрометированный пароль сразу же выводится из действия, взамен его вводятся запасной или новый пароль;
- о компрометации немедленно оповещаются все участники обмена информацией. Пароль вносится в специальные списки, содержащие скомпрометированные пароли и учетные записи.

7. Ответственность пользователей при работе с парольной защитой

7.1. Каждый пользователь ИСПДн несет персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения компрометации пароля его учетной записи.

7.2. За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн, обрабатывающими персональные данные, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.