ЧАСТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СТАВРОПОЛЬСКИЙ КООПЕРАТИВНЫЙ ТЕХНИКУМ»

СОГЛАСОВАНО
Протокол заседания
Студенческого совета
от «30» августа 2023 г. № 1
Председатель Совета
_____

УТВЕРЖДАЮ
Директор Частного профессионального образовательного учреждения «Ставропольский кооперативный техникум»
_____А.А. Намитоков
от «30» августа 2023 г. Приказ № 112

ИНСТРУКЦИЯ

по организации парольной защиты в информационной системе персональных данных «Автоматизированное рабочее место оператора УОП»

1. **Общие положения**

1.1. Настоящая инструкция регламентирует организационно-техническое обеспечение генерации, смены и прекращения действия паролей при организации доступа к информационной системе персональных данных «Автоматизированное рабочее место оператора УОП» (далее – ИСПДн), а также контроль за действиями пользователей системы при работе с паролями.

1.2. Настоящая инструкция разработана в соответствии с требованиями:

- Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. 31.07.2023);
- Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (ред. 06.02.2023);

1.3. Пользователем ИСПДн (далее – Пользователь) является сотрудник согласно должностной инструкции, 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 для доступа в ИСПДн, контроль за действиями пользователей при работе с паролями возлагается на администратора безопасности ИСПДн (далее – Администратор безопасности).

2. **Организация парольной защиты**

2.1. Личные пароли должны генерироваться и распределяться централизованно Администратором безопасности либо выбираться пользователями ИСПДн самостоятельно.

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

2.3. В случае формирования личных паролей пользователей централизованно, ответственность за правильность их формирования и распределения возлагается на Администратора безопасности ИСПДн.

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

2.5. Разблокирование учетной записи осуществляется Администратором.

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

2.7. В ИСПДн устанавливается ограничение на количество неуспешных попыток аутентификации (ввода логина и пароля) пользователя, равное 5, после чего учетная запись блокируется на период времени от 3 до 15 минут.

2.8 В случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п. технической необходимости использования имен и паролей некоторых пользователей в их отсутствие, такие пользователи обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте

передавать на хранение Администратору безопасности информации. Запечатанные конверты с паролями пользователей должны храниться в сейфе у Администратора безопасности.

2.9 В случае утечки информации о зарегистрированном пользователе необходимо немедленно удалить данные об этом пользователе и зарегистрировать заново его с новым идентификатором.

2.10 Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) Администратора безопасности.

2.11 В случае компрометации личного пароля пользователя должны быть немедленно предприняты меры в соответствии с п.2.4 или п.2.11 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

2.12 Хранение пользователем зарегистрированных идентификаторов и значений своих паролей на бумажном носителе допускается только в сейфе у Администратора безопасности.

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

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

3. **Требования к формированию паролей**

2.15 Пользователи и Администратор безопасности 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 ИСПДн, Пользователю необходимо уведомить Администратора безопасности для проведения процедуры разблокировки его учетной записи.
4.4. Запрещается записывать пароли на бумаге, записной книжке и других носителях информации, в том числе на предметах.
4.5. Запрещается сообщать другим Пользователям и регистрировать их в системе под своим паролем.

5. **Обязанности**

Пользователи и Администраторы ИСПДн обязаны:
5.1. Четко знать и строго выполнять требования настоящей инструкции и других руководящих документов ЧПОУ «Кооперативный техникум» по парольной защите.
5.2. Своевременно сообщать Администратору безопасности об утере, компрометации и несанкционированном изменении сроков действия паролей в АРМ и ИСПДн соответственно.
5.3. Ознакомиться под подпись с перечисленными в настоящей инструкции требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

6. **Ответственность**

6.1. Пользователи и Администраторы ИСПДн несут персональную ответственность за соблюдение требований настоящей инструкции, а также за своевременное информирование о необходимости смены паролей в ИСПДн.