Утверждаю:
Директор ГБПОУ Областной многопрофильный техникум
_____Ю.А. Комков
Приказ № 24 от 14 января 2019 г

Инструкция

по парольной защите

р.п. Ардатов
2019 год

1. Общие положения

Настоящая Инструкция определяет основные требования к организации парольной защиты в ГБПОУ Областной многопрофильный техникум (далее – ОО).

Настоящая Инструкция является обязательной для исполнения всеми сотрудниками техникума (далее – пользователи).

2. Организация и обеспечение парольной защиты

2.1. Общие принципы и положения обеспечения парольной защиты

В техникуме установлены следующие принципы обеспечения парольной защиты:

- необходимая сложность пароля;
- конфиденциальность паролей;
- периодичность смены паролей;
- запрет совместного использования индивидуальных паролей;
- использование уникальных паролей для различных систем;
- обязательность смены паролей, установленных разработчиками по умолчанию, сразу после установки систем и (или) программного обеспечения, авторизации нового пользователя под новой учетной записью.

В ОО пароли подразделяются на следующие группы:

- временные (одноразовые) пароли;
- административные (конфигурационные) пароли, позволяющие вносить изменения в конфигурацию систем;
- пароли сервисных учетных записей;
- пользовательские пароли.

Требования к сложности и управлению паролями в зависимости от группы:

Критерий	Временный пароль	Администрат-ый пароль	Пароль сервисных учетных записей	Пользовател-ий пароль
Длина пароля	не менее 8 символов и букв	не менее 10 символов и букв	не менее 10 символов и букв	не менее 8 символов и букв
Сложность пароля	Пароль должен состоять из прописных букв латинского алфавита от A до Z, строчных букв латинского алфавита от a до z, цифр (от 0 до 9), неалфавитных символов (@, #, $, &, *, % и т.п.). Пароль не должен быть основан на информации, которая может быть легко угадана или получена из персональной информации пользователя и администратора, например, имена, даты рождения, номера документов и т.п., а также не должен включать в себя общепринятые сокращения и термины (qwerty, pa$$w0rd и т.п.).			
Повторение пароля	н/п	новый пароль должен отличаться	новый пароль должен отличаться от предыдущих паролей не менее чем 5 символами (буквами)	новый пароль должен отличаться от предыдущих паролей не менее чем 4 символами (буквами)
Периодичность смены пароля	н/п	раз в 45 дней	раз в 45 дней	раз в 90 дней
Количество попыток ввода до блокировки	3	3	3	3
Дополнительные требования	Обязательна смена пароля после первичной авторизации. Запрещена передача пароля по телефону или иным каналам связи	Обязательно хранение копии пароля в запечатанном конверте в специально отведенном месте	н/п	Запрет записи паролей (например, на бумаге, файле программного обеспечения) в случае, если не может быть обеспечено их надежное хранение

2.2. Создание, изменение и восстановление пароля

Создание временного пароля производится администратором системы (автоматизированного рабочего места пользователя (далее – АРМ)) при создании новой учетной записи. Создание административного пароля производится администратором системы сразу после установки системы и (или) программного обеспечения. Создание паролей для сервисных учетных записей производится администратором системы при необходимости. Пользовательские пароли создаются пользователями самостоятельно.

Изменение пароля производится пользователями самостоятельно, используя интерфейс системы управления паролями, встроенного в соответствующие операционные системы и прикладное программное обеспечение.

Восстановление забытого пользовательского пароля осуществляется следующим образом: пользователь сообщает администратору системы информацию о том, что пароль забыт;

администратор системы производит сброс пользовательского пароля, создает и передает пользователю временный пароль.

Внеплановая смена личного пароля или удаление учетной записи пользователя АРМ (системы) в случае прекращения его полномочий (прав доступа к АРМ (системе), увольнение и т.п.) производится администратором системы в течение 1 рабочего дня после окончания последнего сеанса работы данного пользователя с АРМ (системой).

2.3. Обязанности и запреты для пользователей

Пользователи должны:

– выполнять требования к необходимой сложности пароля при его создании;

– сохранять свои пароли в тайне (обеспечивать конфиденциальность);

– производить смену паролей во всех случаях, когда существуют признаки возможной компрометации системы или пароля;

– периодически производить смену пароля;

– использовать различные пароли на работе и в личных целях;

– блокировать рабочие сессии при завершении работы и (или) оставлении АРМ без присмотра;

– производить смену временных паролей при первом входе в систему;

– соблюдать парольную политику, установленную для системы ее администратором.

Пользователям запрещено использовать чужие пароли доступа к системам.

2.4. Система управления паролями

Встроенные в операционные системы и прикладное программное обеспечение системы управления паролями в ОО должны:

– обеспечить использование индивидуальных идентификаторов пользователей и паролей для обеспечения подотчетности;

– предоставлять пользователям возможность создания и смены своих паролей, и содержать процедуру подтверждения на случай ошибок ввода;

– гарантировать выбор качественных (с гарантированной сложностью) паролей;

– гарантировать смену паролей;

– принуждать пользователей производить смену временных паролей при первом входе в систему;

– вести учет предыдущих паролей пользователей и не допускать их повторного использования;

– в момент ввода паролей не показывать их на экране;

– хранить файл с паролями отдельно от данных прикладной системы;

– хранить и пересылать пароли в защищенном виде.

Согласовано и рассмотрено педагогическим советом
ГБПОУ Областной многопрофильный техникум
Протокол № 1 от 14.01.2019 г.