УТВЕРЖДЕНО
приказом директора МАУ ДО
«Детско-юношеский центр»
№ 23 от 14 января 2019 года

Инструкция

по организации парольной защиты в муниципальном автономном учреждении дополнительного образования «Детско-юношеский центр»

1. Общие положения

1.1.Настоящий документ разработан в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными правовыми актами по защите информации, и регламентирует процессы генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в «Сетевой Город. Образование» и Е-услуги. Образование» (далее – информационная система, ИС) Муниципального автономного учреждения дополнительного образования «Детско-юношеский центр» *(далее – Организация),* а также контроль над действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.2.Осуществление процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИС возлагается на системного администратора

1.3.Контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора безопасности информации.

2. Правила формирования паролей

2.1.Временный пароль – комбинация символов (буквы, цифры, знаки препинания, специальные символы), устанавливаемые системным администратором при создании новой учетной записи.

2.1.1. Установку первичного пароля производит системный администратор при создании новой учетной записи. Ответственность за сохранность временного пароля лежит на системном администраторе.

2.1.2. Временный пароль может содержать несложную комбинацию символов, либо повторяющиеся символы.

2.1.3. При создании временного пароля, системный администратор обязан установить опцию, требующую смену пароля при первом входе в систему, а также уведомить владельца учетной записи о необходимости произвести смену пароля.

2.1.4. Временный пароль так же используется при сбросе забытого пароля на учетную запись.

2.2.Основной пароль – комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная только сотруднику организации, используемая для подтверждения подлинности владельца учетной записи.

2.2.1. Установку основного пароля производит пользователь при первом входе в систему с новой учетной записью.

2.2.2. При выборе пароля необходимо руководствоваться «Требованиями к паролям» (Приложение № 1).

2.3.В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора безопасности информации.

2.4.При настройке парольной политики должны быть учтены следующие требования к характеристикам паролей:

- длина пароля не менее шести символов;
- алфавит пароля не менее 60 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 5 до 30 минут;
- смена паролей не реже 1 раза в 120 дней.

3. Ввод пароля

3.1.При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его просмотра посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

3.2.Для предотвращения угадывания паролей системный администратор обязан настроить механизм блокировки учетной записи при многократном неправильном вводе пароля.

3.3.Разблокирование учетной записи пользователя осуществляется системным администратором на основании заявки владельца учетной записи или автоматически через продолжительный промежуток времени.

4. Порядок смены личных паролей

4.1. Смена паролей должна проводиться регулярно, не реже одного раза в 4 месяца, самостоятельно каждым пользователем.

4.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учетной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

4.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственного за защиту информации, администратора безопасности информации и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

4.4. Восстановление забытого основного пароля пользователя осуществляется системным администратором путем изменения (сброса) основного пароля пользователя на временный пароль на основании письменной либо электронной заявки пользователя.

4.5. Устная заявка пользователя на изменение пароля не является основанием для проведения таких изменений.

4.6. Администратор безопасности информации ведет «Журнал учета паролей пользователей», в котором он отмечает причины внеплановой смены паролей пользователей.

5. Хранение пароля

5.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других предметах и носителях информации.

5.2. Запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей.

5.3. Запрещается регистрировать других пользователей в ИС со своим личным паролем.

5.4. Запрещается входить в ИС под учетной записью и паролем другого пользователя.

6. Действия в случае утери и компрометации пароля

6.1. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователю необходимо немедленно сообщить об этом системному администратору и администратору безопасности информации.

6.2. Системным администратором должна быть немедленно проведена внеплановая процедура смены пароля.

7. Ответственность

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

7.2. Ответственность за контроль проведения мероприятий по организации парольной защиты в отделах возлагается на ответственного за защиту информации.

7.3. За разглашение информации ограниченного доступа и нарушение порядка работы со средствами ИС, обрабатывающими защищаемую информации, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

Приложение №1
к инструкции
по организации
парольной защиты

Требования к паролям

Пароли НЕ ДОЛЖНЫ состоять из:

- Вашего имени, отчества или фамилии ни в каком виде (т.е. написаны в строчном, в прописном, в смешанном виде, задом наперед, два раза и т.д.)
- Вашего идентификатора входа (login) ни в каком виде.
- Имен супруга или детей.
- Не используйте какую-либо информацию о себе. Сюда входят: номера телефонов, номера в пропусках и других документах, номер или марка вашего автомобиля, Ваш почтовый адрес и т.д. и т.п.
- Только цифр или одинаковых букв.
- Слов, которые можно найти в словаре (любом, включая иностранные) или в каком-либо списке слов.
- Меньше чем шести символов.

Пароли ДОЛЖНЫ:

- Содержать строчные и прописные буквы.
- Содержать небуквенные символы (т.е. цифры, знаки пунктуации, специальные символы).
- Быть легко запоминаемы, чтобы не было необходимости записывать их.
- Быть составлены так, чтобы Вы могли быстро набрать их на клавиатуре. Это осложнит возможность подглядеть пароль.

Несмотря на такие жесткие требования, есть несколько способов выбора паролей, которые все же соответствуют этим правилам:

- Выберите предложение из песни или стихотворения, и отберите только первые буквы каждого слова (хотя в примере использовано английское предложение, Вы можете воспользоваться и другими языками)

Pretty woman walking down the street становится Pwwdts.

- Выберите два коротких слова и соедините их с помощью
- пунктуационных знаков и спецсимволов:

Dog+rain, kid<Goat, TOP^rank

Приложение № 2
к инструкции
по организации
парольной защиты

ЖУРНАЛ УЧЕТА ПАРОЛЕЙ ПОЛЬЗОВАТЕЛЕЙ

Начат «___»_____20__ г.

Окончен «___»_____20__ г.

На _____листах

_____	_____	_____
(должность руководителя)	(подпись)	(Фамилия И.О.)

№ п/п	ФИО пользователя получившего пароль	Пароль	Дата установки пароля	Дата проверки или изменения пароля	Роспись ответственного лица	Роспись пользователя получившего пароль
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						