МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ «СПОРТИВНАЯ ШКОЛА № 3»

Рассмотрено и принято на заседании
Общего собрания
Протокол № 1 от «06» 02 2024 г.

Утверждаю
Директор МБУДО СШ № 3
_____ О.А. Комарова
Приказ № 33 от 06.02 2024 г.

Парольная политика МБУДО СШ №3

(далее – Политика)

1. Общие положения

1.1. Парольная политика МБУДО СШ №3 (далее соответственно – Политика, Учреждение) определяет основные требования к организации парольной защиты защищаемых информационных систем Учреждения, автоматизированных рабочих мест Учреждения (далее – АРМ) и иных средств вычислительной техники (далее – СВТ), участвующих в обработке и хранении защищаемой информации.

1.2. Под защищаемой информационной системой (далее – ИС) понимается: государственная информационная система; информационная система персональных данных; иная информационная система, обрабатываемая информация, которая подлежит защите в соответствии с требованиями действующего законодательства.

1.3. Под защищаемой информацией понимается информация, которая подлежит защите в соответствии с требованиями действующего законодательства, а также информация, на ограничение доступа (распространения) к которой наложен запрет.

1.4. Настоящая Политика является обязательной для исполнения:

1) ответственным лицом за обеспечение парольной защиты

2) пользователями ИС;

3) пользователями АРМ, к которым относятся сотрудники Учреждения.

2. Обеспечение парольной защиты

2.1. Парольная защита ИС достигается применением паролей при непосредственном доступе в ИС, при доступе к АРМ, с которых осуществляется доступ в ИС / к средствам защиты информации Учреждения (далее – СрЗИ), используемым в составе системы защиты ИС / техническим средствам, используемым в составе ИС (далее – ТС), при доступе к СрЗИ и иным ТС.

2.2. Установлены следующие принципы обеспечения парольной защиты:

1) необходимая сложность пароля;

2) конфиденциальность паролей;

3) периодичность смены паролей;

4) запрет совместного использования индивидуальных паролей;

5) использование уникальных паролей для разных ИС, СрЗИ, АРМ и СВТ (ТС);

6) обязательность смены паролей, установленных разработчиками по умолчанию, сразу после установки ИС и (или) программного обеспечения (далее – ПО), авторизации нового пользователя под новой учетной записью.

2.3. Используются следующие группы паролей:

1) временные пароли;

2) административные пароли;

3) пользовательские пароли.

2.4. Соблюдаются следующие требования к паролям и управлению ими в зависимости от группы:

Критерий	Временный пароль	Административный пароль	Пользовательский пароль
Длина пароля	Не менее 8 символов и букв	Не менее 12 символов и букв	Не менее 8 символов и букв
Сложность пароля	Пароль должен состоять из прописных букв латинского алфавита (символы верхнего регистра) от A до Z, строчных букв латинского алфавита (символы нижнего регистра) 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 (администратора безопасности) ИС, например, имена, даты рождения, памятные даты, номера документов, телефонов		

	и т.п. Пароль не должен включать в себя общепринятые сокращения и термины (например, qwerty, pa$$w0rd, user и т.п.). Пароль не должен содержать комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.). Пароль не должен быть словом русского либо английского языка, в котором заменены некоторые символы (например, о→0, s→$, а→@ и т.п.).		
Повторение пароля	Не установлено	Новый пароль должен отличаться от предыдущего не менее чем 4 позициями (символами), расположенными на подряд. Новый пароль не должен повторять последние 4 сгенерированных паролей	Новый пароль должен отличаться от предыдущего не менее чем 2 позициями (символами). Новый пароль не должен повторять последние 3 сгенерированных пароля
Периодичность смены пароля	Не установлено	Раз в 90 дней	Раз в 90 дней
Количество попыток ввода до блокировки учетной записи	5	5	5
Дополнительные требования	Запрет записи паролей (например, на бумаге, в электронном файле, в очевидных местах (монитор АРМ, обратная сторона клавиатуры и т.п.). Обязательна смена пароля после первичной авторизации. Запрещена передача пароля по телефону или иным каналам связи	Запрет записи паролей (например, на бумаге, в электронном файле, в очевидных местах (монитор АРМ, обратная сторона клавиатуры и т.п.). Копия пароля обязательно хранится в запечатанном конверте в специально отведенном месте, исключающим несанкционирован-ный доступ	Запрет записи паролей (например, на бумаге, в электронном файле, в очевидных местах (монитор АРМ, обратная сторона клавиатуры и т.п.)

2.5. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей (установления парольной политики) возложено на ответственного за обеспечение парольной защиты.

2.6. Временный пароль используется пользователями ИС для доступа в ИС при первом входе и после сброса пользовательского пароля. Временный пароль ограничен по времени действия и подлежит изменению на пользовательский пароль при первом входе в ИС. Ограничения вводятся администратором ИС.

Создание временного пароля проводится администратором ИС при создании новой учетной записи пользователя, а также в случае, если пароль забыт пользователем, путем сброса пользовательского пароля и генерации временного. Пользователь ИС, получивший временный пароль, информируется об ограничениях, связанных с его пользованием.

2.7. Административный пароль используется для доступа к управлению ИС / СрЗИ / АРМ / СВТ (ТС), и позволяет вносить изменения в конфигурацию.

Создание административного пароля для ИС проводится администратором ИС сразу после установки ИС. Создание административного пароля для АРМ / СВТ (ТС) и (или) ПО проводится ответственного за обеспечение парольной защиты сразу после его установки.

Внеплановая смена административного пароля или удаления учетной записи уполномоченного лица, указанного в пункте 2.5 настоящей Политики, в случае прекращения прав доступа к ИС / СрЗИ / АРМ / СВТ (ТС), проводится в соответствии с компетенцией, предоставленной пунктом 2.5 настоящей Политики, новым администратором при участии действующего (сложившего полномочия) немедленно после окончания последнего сеанса работы действующего администратора с ИС / СрЗИ / АРМ / СВТ (ТС). В указанных целях действующий администратор самостоятельно вводит своей административный пароль, после чего вновь назначенный администратор самостоятельно создает свой административный пароль или учетную запись администратора, сохраняя их в тайне.

2.8. Пользовательский пароль используется пользователями ИС и пользователями АРМ для постоянного доступа в ИС и к АРМ соответственно в рамках срока действия прав доступа.

Пользовательские пароли выбираются и генерируются пользователями самостоятельно.

В случае компрометации либо утери пароля незамедлительно должна проводиться его внеплановая смена.

Внеплановая смена пользовательского пароля, создание или удаление учетной записи пользователя проводится ответственным за обеспечение парольной защиты по требованию руководителя Учреждения, на основании письменной заявки, согласованной с лицом, ответственным за защиту информации.

При возникновении необходимости срочного доступа к АРМ временно отсутствующего пользователя ответственный за обеспечение парольной защиты осуществляет внеплановую смену пароля пользователя по требованию руководителя на основании письменной заявки.

Полная внеплановая смена паролей всех пользователей ИС (пользователей АРМ) проводится в случае прекращения полномочий администратора ИС (системного администратора), а также в случае компрометации его административного пароля.

2.9. Для генерации административных и временных паролей допустимо применение специализированного ПО.

2.10. Пользователи ИС (пользователи АРМ) и уполномоченные лица, указанные в пункте 2.5 настоящей Политики, обязуются:

1) соблюдать при создании своих паролей требования пункта 2.4 настоящей Политики;

2) сохранять свои пароли в тайне и не сообщать их другим лицам;

3) изменять свои пароли с установленной периодичностью;

4) обеспечивать несоответствие своих паролей, используемых в ИС / для доступа к СрЗИ / АРМ / СВТ (ТС), паролям, используемым в личных и иных целях (например, для доступа к иным программным средствам);

5) блокировать рабочие сессии при завершении работы и оставлении ИС / СрЗИ / АРМ / СВТ (ТС) без присмотра (если применимо);

6) проводить смену своего пароля немедленно во всех случаях, когда имели место компрометация пароля или несанкционированный доступ в ИС / к СрЗИ / АРМ / СВТ (ТС), либо существуют признаки возможной компрометации / несанкционированного доступа;

7) не использовать чужие пароли доступа;

8) менять временные пароли при первом входе в ИС (только для пользователей ИС);

9) соблюдать установленную парольную политику.

2.11. В целях принятия оперативных мер реагирования, о фактах (признаках) компрометации своего пароля:

1) пользователь АРМ сообщает немедленно системному администратору и администратору безопасности;

2) пользователь ИС сообщает немедленно администратору ИС (при компрометации паролей в отношении учетной записи ИС), системному администратору (при компрометации паролей в отношении учетной записи АРМ), а также администратору безопасности ИС;

3) уполномоченное лицо, указанное в пункте 2.5 настоящей Политики, сообщает немедленно о фактах (признаках) компрометации паролей руководителю Учреждения.

2.12. Контроль за действиями пользователей ИС / АРМ при работе с паролями, соблюдением порядка их создания, смены, хранения и использования возлагается на ответственного за обеспечение парольной защиты.

Контроль проводится ежеквартально, выборочно в отношении пользователей ИС / АРМ, ответственного за обеспечение парольной защиты. Выявленные в результате контроля нарушения устраняются немедленно.

3. Ответственность

3.1. Ответственность за организацию парольной защиты ИС в соответствии с требованиями настоящей Политики возложена на ответственного за обеспечение парольной защиты.

3.2. Ответственность за соблюдение требований настоящей Политики возложена на уполномоченное лицо в соответствии с действующим законодательством.