Муниципальное бюджетное учреждение
дополнительного образования
«Детско-юношеская спортивная школа г.Пошехонье»

УТВЕРЖДАЮ
ВрИО директора МБУ ДО
«ДЮСШ г.Пошехонье»
_____ /М.А.Тутынин/
(Подпись) (Ф.И.О.)
Приказ № 10/2
«07» 02 2020 г.

Приложение № 6

ПОЛОЖЕНИЕ
по организации парольной защиты в МБУ ДО «ДЮСШ г.Пошехонье»

1. Общие положения

1.1. Данное положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в автоматизированной системе МБУ ДО «ДЮСШ г.Пошехонье» (далее АС ОУ), меры обеспечения безопасности при использовании паролей, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.
1.2. Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации в ОУ.
1.3. Требования настоящего Положения распространяются на всех работников подразделений, использующих в работе компьютерную технику (включая работу в локальной сети ОУ) и должны применяться для всех персональных компьютеров, эксплуатируемых в ОУ.
1.4. Организационное обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах АС ОУ и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на системного администратора. Техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей возлагается на системного администратора ОУ.
1.5. Ознакомление всех работников Организации, использующих ПК, с требованиями положения проводит системный администратор. При ознакомлении с Положением внимание работников акцентируется на предупреждении их о персональной ответственности за разглашение парольной информации.
1.6. Термины и определения:

Автоматизированная система (АС) - совокупность программных и аппаратных средств, предназначенных для хранения, передачи и обработки данных и информации и производства вычислений.

Информационная безопасность (ИБ) – обеспечение защищенности информации (ее конфиденциальности, целостности, доступности) от широкого спектра угроз с целью обеспечения непрерывности бизнеса, минимизации рисков бизнеса и максимального увеличения возможностей бизнеса.

Несанкционированный доступ (НСД) - доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа.

Учетная запись - информация о сетевом пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе. Учетная запись может содержать дополнительную информацию (адрес электронной почты, телефон и т.п.).

Принцип минимальных привилегий - принцип, согласно которому «каждому субъекту системы предоставляется минимальный набор полномочий (или минимальный допуск), необходимый для выполнения вверенных задач. Применение этого принципа ограничивает ущерб, наносимый в случае случайного, ошибочного или несанкционированного использования.

Компрометация – утрата доверия к тому, что информация недоступна посторонним лицам.

Ключевой носитель – электронный носитель (дискета, флэш-накопитель, компакт-диск и т.п.), на котором находится ключевая информация (сертификаты и т.п.).

2. Общие требования к паролям

2.1. Пароли доступа ко всем подсистемам АС ОУ, информационным ресурсам первоначально формируются системным администратором, а в дальнейшем выбираются пользователями самостоятельно, но с учетом требований, изложенных ниже.

2.2. Личные пароли пользователей автоматизированной системы ОУ должны выбираться с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы, цифры и (или) специальные символы (@, #, $, &, *, % и т.п.). Исключение составляют подсистемы АС ОУ, в которых использование подобных спецсимволов недопустимо;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения и термины (qwerty, pa$$w0rd, и т.п.);
- при смене пароля новый пароль должен отличаться от старого не менее, чем двумя символами.

3. Безопасность локальных учетных записей

3.1. Локальные учетные записи компьютеров предназначены для служебного использования системным администратором при настройке систем и не предназначены для повседневной работы.

3.2. Создание и использование локальных учетных записей на рабочих станциях, подключенных к АС ОУ и входящих в состав домена, либо в состав какого-либо из его поддоменов пользователям **ЗАПРЕЩЕНО**.

3.3. Встроенная учетная запись Guest (Гость) должна быть заблокирована на всех рабочих станциях в составе АС ОУ при первоначальном конфигурировании операционной системы.

3.4. Встроенная учетная запись Administrator (Администратор) должна быть защищена паролем согласно п. 2.2. настоящей инструкции.

4. Безопасность доменных учетных записей

4.1. Создание, изменение, удаление доменных учетных записей, а также учетных записей сервисов АС ОУ (электронная почта и др.) необходимо производить в соответствии с положением «о порядке доступа к информационным, программным и аппаратным ресурсам МБУ ДО «ДЮСШ г.Пошехонье».

4.2. Пользователь несет персональную ответственность за сохранение в тайне личного пароля. Запрещается сообщать пароль другим лицам, а также хранить записанный пароль в общедоступных местах.

4.3. В случае необходимости (командировка, отпуск и т.п.), при проведении проверочных мероприятий, выполняемых системным администратором, работ, требующих знания пароля пользователя, допускается раскрытие значений своего пароля начальникам этих подразделений и системному администратору ОУ.

4.4. По окончанию производственных, или проверочных работ работники самостоятельно производят немедленную смену значений "раскрытых" паролей.

4.5. В случае возникновении нештатных ситуаций, форс-мажорных обстоятельств, а также технологической необходимости использования имен и паролей работников (в их отсутствие) допускается изменение паролей системным администратором ОУ. В подобных случаях, сотрудники, чьи пароли были изменены, обязаны сразу же после выяснения факта смены своих паролей, создать их новые значения.

4.6. Пароли учетных записей пользователей АС должны соответствовать требованиям п. 2.2. Настоящего Положения.

4.7. К управлению доменными учетными записями пользователей необходимо подходить исходя из принципа «минимальных привилегий», т.е. пользователь не должен иметь прав доступа как к локальной системе, так и к ресурсам АС больше, чем это необходимо ему для выполнения своих должностных обязанностей.

4.8. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на работу в другое подразделение внутри Организации и другие обстоятельства) системного администратора и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем АС.

4.9. В случае длительного отсутствия пользователя АС (командировка, болезнь и т.п.) его учетная запись блокируется, и, в случае необходимости, изменяются права доступа других пользователей в отношении ресурсов данного пользователя в соответствии с положением «о порядке доступа к информационным, программным и аппаратным ресурсам МБУ ДО «ДЮСШ г.Пошехонье».

4.10. В случае компрометации личного пароля пользователя АС либо подозрении на компрометацию должны быть немедленно предприняты меры по внеплановой смене личного пароля самим пользователем с немедленным информированием системного администратора ОУ.

4.11. Смена забытого пользовательского пароля производится системным администратором ОУ на основании сообщения пользователя с обязательной установкой параметра «Требовать смену пароля при следующем входе в систему».

4.12. Для предотвращения угадывания паролей системный администратор ОУ обязан настроить механизм блокировки учетной записи на 20 минут при пятикратном неправильном вводе пароля.

4.13. При временном оставлении рабочего места в течение рабочего дня рабочая станция в обязательным порядке блокируется нажатием комбинации клавиш «Win + L».

4.14. При возникновении вопросов, связанных с использованием доменных учетных записей пользователь АС обязан обратиться системному администратору ОУ.

5. Временные учетные данные

5.1. Для предоставления временного доступа к ресурсам АС ОУ (для лиц, не являющихся сотрудниками ОУ, для сотрудников, которым необходимо получить временный доступ к ресурсам АС, и т.п.) необходимо использовать процедуру временных учетных записей.

5.2. Временная учетная запись – учетная запись, имеющая ограничение по времени действия, имеющая ограниченные права по доступу. Для временных учетных записей проводится подробное протоколирование их использования. Процедура получения временных учетных записей состоит в следующем:

- сотрудник ОУ через руководителя своего подразделения либо лицо, не являющее сотрудником ОУ через доверенное лицо оформляет соответствующим образом Заявку «на предоставление доступа к информационным, программным и аппаратным ресурсам ОУ, указав в заявке, что требуемая учетная запись временная и определив временные рамки ее использования;
- заявка направляется системному администратору ОУ для рассмотрения;
- временная учетная запись создается системным администратором;
- пользователь, получивший временную учетную запись информируется об ограничениях, связанных с ее использованием.

6. Безопасность служебных и привилегированных учетных записей

6.1. К служебным учетным записям относятся учетные записи, используемые отделами либо техническим персоналом АС для доступа к ресурсам, необходимым для выполнения их функций. К привилегированным учетным записям относятся учетные записи, используемые для управления работой АС.

6.2. При использовании привилегированных учетных записей (администратора) необходимо руководствоваться принципом «минимальных привилегий», т.е. привилегии администратора должны использоваться только администратором и только если выполняемая задача требует наличия таких привилегий.

6.3. Использование привилегированных учетных записей в повседневной работе, не связанной с необходимостью их использования (установка, конфигурирование, восстановление и т.п. операционной системы и сервисов) недопустимо, в случае необходимости запуска программы с правами Администратора пользователь обязан использовать команду «Run As» либо «вторичный вход в систему».

6.4. Учетная запись администратора домена должна использоваться только при установке, конфигурировании, восстановлении контроллера домена и иных действиях, при которых использование других учетных записей невозможно. Для этой учетной записи необходимо подробное протоколирование всех событий ее использования, а также немедленное расследование любого нецелевого ее использования;

6.5. Использование принципа «минимальных привилегий» необходимо для служб и сервисов, выполняющихся на серверах АС ОУ, т.е. службы и сервисы должны работать с минимально возможными для их корректной работы привилегиями исходя из следующей иерархии:

- локальная служба.
- сетевая служба.
- уникальная учетная запись локального пользователя.
- уникальная учетная запись пользователя домена.
- локальная система
- учетная запись локального администратора.
- учетная запись администратора домена.

6.6. К серверам высокой степени безопасности (контроллеры домена, серверы баз данных, иные серверы, от которых зависит бесперебойная работа АС ОУ) необходимо предъявлять повышенные требования к минимизации привилегий доступа со стороны как удаленных, так и локальных пользователей, и служб.

6.7. В случае компрометации, либо подозрении на компрометацию привилегированной учетной записи необходима внеплановая смена паролей всех зависящих от нее учетных записей.

7. Аппаратные средства аутентификации

7.1. Для повышения степени защиты критически важных объектов АС ОУ (рабочие станции и мобильные компьютеры с информацией высокой степени конфиденциальности, иные объекты) от несанкционированного доступа необходимо использование двухфакторной аутентификации (по паролю и предмету – далее ключевой носитель информации).

7.2. Каждому пользователю АС ОУ для которого предусмотрена двухфакторная аутентификация, выдается персональный ключевой носитель информации, который учитывается системным администратором установленным образом (однозначное сопоставление ключевого носителя и его владельца).

7.3. Ключевые носители информации маркируются отделом по защите информации ОУ установленным образом (уникальный номер ключевого носителя).

7.4. В случае прекращения необходимости использования персонального ключевого носителя (увольнение пользователя, прекращение функционирования объекта, для аутентификации на котором носитель использовался и т.п.) информация с данного носителя стирается установленным образом, либо уничтожается сам носитель в случае невозможности его очистки.

7.5. Пользователям АС ОУ и категорически запрещается оставлять без личного присмотра, а также передавать другим лицам персональные ключевые носители, сообщать коды от персонального ключевого носителя, если таковые имеются.

7.6. В случае утраты персонального ключевого носителя пользователь обязан немедленно сообщить об инциденте руководителю своего подразделения и системному администратору ОУ. При возникновении подобного инцидента необходимо незамедлительно принять меры для недопущения несанкционированного использования утраченного персонального ключевого носителя.

8. Контроль

8.1. Повседневный контроль над соблюдением требований данного Положения заключается в контроле процессов использования и изменения учетных записей, процессов доступа к ресурсам, процессов изменения учетных записей и предоставления доступа к ресурсам АС системным администратором ОУ.

8.2. Отдел по защите информации проводит ежеквартальный выборочный контроль выполнения работниками ОУ требований Положения. О фактах несоответствия качества паролей или условий обеспечения их сохранности отдел по защите информации сообщает руководителю организации в форме служебной записки.

8.3. Контроль за выполнением требований данного Положения возлагается на системного администратора ОУ.

9. Ответственность

9.1. Пользователи АС ОУ несут персональную ответственность за несоблюдение требований по парольной защите;

9.2. Системный администратор несёт ответственность за компрометацию и нецелевое использование привилегированных учетных записей.

9.3. Форма и размер ответственности определяются исходя из вида и размера ущерба, нанесенного ресурсам АС ОУ действиями либо бездействием соответствующего пользователя.