Подписан: Ситникова Оксана Викторовна
DN: OU=И.О. диретора, O=Школа № 240 г. Борзи, CN=Ситникова Оксана Викторовна, E=brzschool240@mail.ru
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: место подписания
Дата: 2022.12.16 16:04:37+03'00'
Foxit PDF Reader Версия: 11.1.0

Муниципальное общеобразовательное учреждение
“Средняя общеобразовательная школа № 240 г. Борзи”

Рассмотрено и одобрено на заседании
педагогического совета
Школа 240 г.Борзи
«15» декабря 2022 г.

УТВЕРЖДАЮ
И. о. директора Школы №240 г. Борзи
Ситникова О.В.
«15» декабря 2022 г.

ПОЛОЖЕНИЕ
ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ В ШКОЛЕ № 240 Г. БОРЗИ

1. Общие положения

1.1. Данное положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей на платформах предназначенных для выполнения своих должностных обязанностей) в автоматизированной системе Школы № 240 г. Борзи (далее ОУ), меры обеспечения безопасности при использовании паролей, а также контроль за действиями пользователей 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, средства вычислительной техники (включая работу в локальной вычислительной сети ОУ) и должны применяться для всех средств вычислительной техники, эксплуатируемой в ОУ.

1.4. Организационное обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ОУ и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на Технического специалиста Школы № 240 г. Борзи (далее технический специалист). Техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей возлагается на также возлагается на технического специалиста.

1.5. Ознакомление всех работников ОУ, использующих средства вычислительной техники, с требованиями положения проводит технически специалист. 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) оширокого 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 ОУ, информационным ресурсам для первой авторизации формируются техническим специалистом, далее пользователь меняет пароль для обеспечения защищенности персональных данных, 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 Организации, 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;

2.3. Пароли служебных и привилегированных учетных записей автоматизированной системы должны выбираться с учетом следующих требований:

- длина пароля должна быть не менее 12 символов;
- в числе символов пароля обязательно должны присутствовать, цифры и (или) специальные символы (@, #, $, &, *, % и т.п.). Исключение составляют подсистемы 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.), пароль не должен быть словом русского либо английского языка, в котором заменены некоторые символы (o->0,s->$, a->@ и т.п.).
- при смене пароля новый пароль должен отличаться от старого не менее, чем четырьмя символами, расположенными не подряд;
- при создании паролей служебных учетных записей возможно использование специализированного программного обеспечения для генерации сложных для подбора легко запоминаемых паролей.

3. Безопасность локальных учетных записей

3.1. Локальные учетные записи компьютеров (Администраторы) предназначены для служебного использования техническим специалистом при настройке систем и не предназначены для повседневной работы.

3.2. Встроенная учетная запись Guest (Гость) должна быть заблокирована рабочих станциях предназначенных для выполнения административной работы и использующихся для авторизации на государственных порталах при первоначальном конфигурировании операционной системы.

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

3.4. BIOS рабочих станций ОУ должен быть защищен паролем согласно п. 2.2. настоящего положения.

3.5. Встроенная учетная запись Guest (Гость) может быть использована для сотрудников совместителей, только после блокирования доступа ко всем файлам ответственного за АРМ.

4. Безопасность доменных учетных

4.1. Создание, изменение, удаление доменных учетных записей, а также учетных записей сервисов ОУ (корпоративная электронная почта и др.) производит технический специалист по приказу директора.

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 производственной необходимости (командировка, отпуск и т.п.), при проведении проверочных мероприятий, выполняемых техническим специалистом, работ и требующих знания пароля пользователя, допускается раскрытие значений своего пароля техническому специалисту. По окончанию производственных, или проверочных работ работник ОУ ответственный за АРМ самостоятельно производят немедленную смену значений "раскрытых" паролей.

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

4.5. Пароли учетных записей пользователей ОУ должны соответствовать требованиям п. 2.2. Настоящего Положения.

4.6. 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 ОУ больше, чем это необходимо ему для выполнения своих должностных обязанностей.

4.7. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 2 месяца. Плановая смена должна предусматривать информирование пользователя о необходимости сменить пароль, сменой пароля занимается технический специалист.

4.8. Внеплановая смена личного пароля или удаление учетной записи

пользователя автоматизированной системы в случае прекращения его полномочий (увольнение и т.п.) должна производиться техническим специалистом немедленно после окончания последнего сеанса работы данного пользователя с системой.

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

4.10. В случае длительного отсутствия пользователя ОУ (командировка, болезнь и т.п.) его учетная запись блокируется, и, в случае необходимости, изменяются права доступа других пользователей в отношении ресурсов данного пользователя.

4.11. В случае компрометации личного пароля пользователя ОУ либо подозрении на компрометацию должны быть немедленно предприняты меры по внеплановой смене личного пароля самим пользователем с немедленным информированием технического специалиста.

4.12. Смена забытого пользовательского пароля производится техническим специалистом на основании сообщения пользователя с обязательной установкой параметра «Требовать смену пароля при следующем входе в систему».

4.13. Для предотвращения угадывания паролей технический специалист обязан настроить механизм блокировки учетной записи на 20 минут при пятикратном неправильном вводе пароля.

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

4.15. При возникновении вопросов, связанных с использованием доменных учетных записей пользователь ОУ обязан обратиться к техническому специалисту.

5. Безопасность служебных учетных записей

5.1. К служебным учетным записям относятся учетные записи, используемые АУП для доступа к ресурсам, необходимым для выполнения их функций. К привилегированным учетным записям относятся учетные записи, используемые для управления работой ЭИОС.

5.2. 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.

5.3. 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».

5.4. 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;

5.5. Использование принципа «минимальных привилегий» необходимо для служб и сервисов, выполняющихся на серверах 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.

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

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

6. Контроль

6.1. 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 ОУ техническим сециалистом.

6.2. Технический специалист проводит 1 раз в 2 месяца выборочный контроль выполнения работниками Организации требований Положения. О фактах несоответствия качества паролей или условий обеспечения их сохранности технический спечиалист сообщает руководителю ОУ в форме служебной записки.

6.3. Контроль за выполнением требований данного Положения возлагается на технического специалиста.

7. Ответственность

7.1. Пользователи в ОУ несут персональную ответственность за несоблюдение требований по парольной защите;

7.2. Технический специалист и сотрудники несут ответственность за компрометацию и нецелевое использование привилегированных учетных записей.

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

7.4. Все действия связанные с парольной политикой обязательно регистрируются техническим специалистом в журнале парольной политике (Приложение № 1 и приложение №2);

7.5. Хранение журнала в общедоступном месте запрещено.

Приложение № 1 к Положению по организации парольной политики в Школе № 240 г. Борзи

Форма
журнала учета паролей

N п/п	ФИО владельца (работника)	Должность	Логин (имя пользователя)	Дата генерации пароля	ФИО, выдавшего пароль	Первичный пароль