Утверждаю
Директор школы
И.М. Трухина
Приказ № 55 «в» от 31.08.2021 г.

Трухина Инна Михайловна

Трухина Инна Михайловна
C=RU, O="МБОУ ""Михайло-Павловская СОШ""", CN=Трухина Инна Михайловна, E=shkolamp1@rambler.ru
я подтверждаю этот документ своей удостоверяющей подписью
с. Михайло-Павловск
2022.04.13 18:06:47+09'00'

Положение по организации парольной защиты в МБОУ «Михайло-Павловская СОШ»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данное положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей), 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 Организации.

1.3. Требования настоящего Положения распространяются на всех работников подразделений, использующих в работе средства вычислительной техники (включая работу в локальной вычислительной сети Организации) и должны применяться для всех средств вычислительной техники, эксплуатируемой в Организации.

1.4. Организационное обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на Администратора ЛВС Техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей возлагается на администратора локальной вычислительной сети (далее - администратора ЛВС) Организации.

1.5. Ознакомление всех работников Организации, использующих средства вычислительной техники, с требованиями положения проводит Администратор ЛВС. 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, флэшнакопитель, 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 Организации, информационным ресурсам первоначально формируются администратором ЛВС, а в дальнейшем выбираются пользователями самостоятельно, но с учетом требований, изложенных ниже.

2.2. Личные пароли пользователей автоматизированной системы Организации 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 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.), 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 (Administrator, Guest) предназначены для служебного использования администратором ЛВС при настройке систем и не предназначены для повседневной работы.

3.2. Создание и использование локальных учетных записей на рабочих станциях, подключенных к АС Организации 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 Учреждения при первоначальном конфигурировании операционной системы.

3.4. Встроенная учетная запись Administrator (Администратор) должна быть защищена паролем согласно п. 2.3. настоящей инструкции.

3.5. BIOS рабочих станций в составе АС Учреждения должна быть защищена паролем согласно п. 2.3. настоящей инструкции.

4. БЕЗОПАСНОСТЬ ДОМЕННЫХ УЧЕТНЫХ ЗАПИСЕЙ

4.1. Создание, изменение, удаление доменных учетных записей, а также учетных записей сервисов АС Организации (корпоративная электронная почта и др.) необходимо производить в соответствии с положением «О порядке доступа к информационным, программным и аппаратным ресурсам».

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 Администратором ЛВС, работ и требующих знания пароля пользователя, допускается раскрытие значений своего пароля начальникам этих подразделений. По окончанию производственных, или проверочных работ работники 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 администратором ЛВС. 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 АС 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 АС 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 и возможность смены пароля без обращения к администратору сети.

4.8. Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение и т.п.) должна производиться администратором ЛВС 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) администратора ЛВС и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем АС.

4.10. 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.

4.11. 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 Администратора ЛВС.

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

4.13.Для предотвращения угадывания паролей администратор ЛВС 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 АС обязан обратиться к Администратору ЛВС Организации.

5. БЕЗОПАСНОСТЬ СЛУЖЕБНЫХ И ПРИВИЛЕГИРОВАННЫХ УЧЕТНЫХ ЗАПИСЕЙ

5.1. 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.

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 АС Организации, 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 АС Организации) 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. АППАРАТНЫЕ СРЕДСТВА АУТЕНТИФИКАЦИИ

6.1. Для повышения степени защиты критически важных объектов АС Организации (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).

6.2. Каждому пользователю АС Организации, для которого предусмотрена двухфакторная аутентификация, выдается персональный ключевой носитель информации,

Ключевые носители информации маркируются Администратором ЛВС Организации установленным образом (уникальный номер ключевого носителя).

6.3. 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.

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

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

7. КОНТРОЛЬ

7.1. 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 администратором ЛВС.

7.2. Администратор ЛВС проводит ежеквартальный выборочный контроль выполнения работниками Организации требований Положения. О фактах несоответствия качества паролей или условий обеспечения их сохранности Администратор ЛВС сообщает руководителю организации в форме служебной записки.

7.3. Контроль за выполнением требований данного Положения возлагается на Администратора ЛВС.

8. ОТВЕТСТВЕННОСТЬ

8.1. Пользователи АС Организации несут персональную ответственность за несоблюдение требований по парольной защите.

8.2. Администратор ЛВС, сотрудники несут ответственность за компрометацию и нецелевое использование привилегированных учетных записей.

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