ПРИНЯТО:	СОГЛАСОВАНО:	УТВЕРЖДЕНО:
Общим собранием работников МБДОУ «Детский «Рябинушка	Председатель профсоюзного комитета МБДОУ «Детский сад № 7 «Рябинушка»	Приказом по МБДОУ «Детский сад № 7 «Рябинушка»
Протокол № 22.01.2020 г.	Филатова М.В. _____2020 г.	от 23.01.2020 г. № 18 о.д.

ПОЛОЖЕНИЕ ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ В МБДОУ «ДЕТСКИЙ САД №7 «РЯБИНУШКА» ГОРОДА - КУРОРТА ЖЕЛЕЗНОВОДСКА

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 МБДОУ «Детский сад № 7 « Рябинушка» города- курорта Железноводска (далее АС Учреждения), 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 Учреждения.

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

1.4. Организационное обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах АС Учреждения и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на отдел по защите информации.

1.5. Ознакомление всех работников Учреждения, использующих средства вычислительной техники, с требованиями Положения проводит программист Учреждения. 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 Учреждения, выбираются пользователями самостоятельно, но с учетом требований, изложенных ниже.

2.2. Личные пароли пользователей автоматизированной системы Учреждения 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 Учреждения, 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 Учреждения, 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. Создание и использование локальных учетных записей на рабочих станциях, подключенных к АС Учреждения и входящих в состав домена, либо в состав какого-либо из его поддоменов пользователям **ЗАПРЕЩЕНО**.

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

4. БЕЗОПАСНОСТЬ ДОМЕННЫХ УЧЕТНЫХ ЗАПИСЕЙ

4.1. Создание, изменение, удаление доменных учетных записей, а также учетных записей сервисов АС Учреждения (корпоративная электронная почта и др.) необходимо производить в соответствии с положением «о порядке доступа к информационным, программным и аппаратным ресурсам МБДОУ «Детский сад № 7 «Рябинушка».

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 отделом по защите информации, работ, проводимых отделом информационных технологий 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. 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.

4.5. 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 начальника отдела по защите информации.

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

4.7. При возникновении вопросов, связанных с использованием доменных учетных записей пользователь АС обязан обратиться программисту Учреждения.

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. 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».

5.3. 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;

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

5.5. 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 АС программистом Учреждения.

7. ОТВЕТСТВЕННОСТЬ

7.1. Пользователи АС Учреждения несут персональную ответственность за несоблюдение требований по парольной защите;

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