УТВЕРЖДЕНО
Приказом руководителя
МУ ДО «СШ № 1»
от «28» декабря 2024 г. № 134-ОД

Инструкция по организации парольной защиты в Муниципальном бюджетном учреждении дополнительного образования Петрозаводского городского округа «Спортивная школа № 1» (МУ ДО «СШ № 1»)

Общие положения

Инструкция по организации парольной защиты устанавливает основные правила введения парольной защиты и регламентирует организационно - техническое обеспечение генерации, смены и прекращения действия паролей, а также контроль за действиями пользователей системы при работе с паролями.

В данном локальном нормативном акте используются следующие термины и определения:

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

ИСПДн - информационная система персональных данных.

Компрометация - факт доступа постороннего лица к защищаемой информации, а также подозрение на него.

Объект доступа - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Пароль - уникальный признак субъекта доступа, который является его (субъекта) секретом.

Правила доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Субъект доступа - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Несанкционированный доступ (НСД) - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированной системы (АС).

1. Правила генерации паролей

1.1. Пароли доступа ко всем информационным ресурсам первоначально формируются администратором ИСПДн, а в дальнейшем изменяются пользователями самостоятельно, но с учетом требований, изложенных ниже.

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

- ¬ длина пароля должна быть не менее 8 символов;
- ¬ пароли должны содержать символы из четырех следующих групп:
  - прописные латинские буквы: ADCDEFG....;
  - строчные латинские буквы: abcdefg....;
  - цифры:12345...90;
  - специальные символы: !@#$%& и т.д.
- ¬ 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, p@sswOrd и т.п.);
- ¬ при смене пароля новый пароль должен отличаться от старого не менее чем двумя символами.

2. Порядок смены паролей

2.1. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 3 месяца (90 дней).

2.2. Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий администратора ИСПДн или других сотрудников, которым были предоставлены полномочия по управлению парольной зашитой.

2.3. Полная внеплановая смена паролей должна производиться в случае компрометации личного пароля администратора ИСПДн.

2.4. В случае компрометации личного пароля пользователя надлежит немедленно ограничить доступ к информации с данной учетной записи, до момента вступления в силу новой учетной записи пользователя или пароля.

3. Обязанности пользователей при работе с парольной защитой

3.1. При работе с парольной защитой пользователям запрещается:

- разглашать кому-либо персональный пароль и прочие идентифицирующие сведения;
- предоставлять доступ от своей учетной записи к информации, хранящейся в ИСПДн, посторонним лицам;
- записывать пароли на бумаге, файле, электронных и прочих носителях информации, в том числе и на предметах.

3.2. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля, сейфе.

3.3. При вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами и техническими средствами.

4. Случаи компрометации паролей

4.1. Под компрометацией следует понимать следующее: физическая утеря носителя с информацией; передача идентификационной информации по открытым каналам связи; проникновение постороннего лица в помещение физического хранения носителя парольной информации или алгоритма, или подозрение на него (срабатывание сигнализации, повреждение устройств

контроля НСД (слепков печатей), повреждение замков и т. п.); визуальный осмотр носителя идентификационной информации посторонним лицом; сознательная передача информации постороннему лицу.

4.2. Действия при компрометации пароля:

- скомпрометированный пароль сразу же выводится из действия, взамен его вводится новый пароль;
- о компрометации немедленно оповещается Администратор информационной безопасности организации;
- пароль вносится в специальные списки, содержащие скомпрометированные пароли и учетные записи.

5. Ответственность пользователей при работе с парольной защитой

5.1. Повседневный контроль за действиями сотрудников организации при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на ответственного за организацию обработки персональных данных. Рекомендуется использовать доменные политики или иные средства автоматизации для контроля за сроком действия и сложностью паролей пользователей.

5.2. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации (лист ознакомления прилагается).

5.3. Ответственность за организацию парольной защиты возлагается на администратора информационной системы.

5.4. Ответственность в случае несвоевременного уведомления Администратора информационной безопасности о случаях утери, кражи, взлома или компрометации паролей возлагается на владельца взломанной учетной записи.