Муниципальное бюджетное общеобразовательное учреждение ПГО
«Основная общеобразовательная школа пос. Станционный - Полевской»

УТВЕРЖДАЮ
Директор школы
_____ О.А. Попова
Приказ № 1/8 – Д от 09.01.2019г.

ИНСТРУКЦИЯ
по организации парольной защиты информационных систем персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция устанавливает основные правила введения парольной защиты информационной системы персональных данных МБОУ ПГО «ООШ п. Станционный – Полевской» (далее – Учреждение).

1.2. Инструкция регламентирует организационно-техническое обеспечение генерации, смены и прекращения действия паролей в информационной системе персональных данных, а также контроль за действиями пользователей системы при работе с паролями.

1.3. Настоящая инструкция оперирует следующими основными понятиями:

- **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** - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или АС

2. ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ

2.1. Личные пароли должны создаваться Пользователями самостоятельно.

2.2. В случае формирования личных паролей Пользователей централизованно, ответственность за правильность их формирования и распределения возлагается на Администратора безопасности ИСПДн и на АРМ Пользователей соответственно.

2.3. Персональные пароли должны генерироваться специальными программными средствами административной службы.

2.4. Длина пароля должна быть не менее 6 символов.

2.5. В составе пароля рекомендованы буквы в верхнем и нижнем регистрах, цифры и специальные символы, не принадлежащие алфавитно-цифровому набору (например, !, @, #, $, &, *, % и т.п.).

2.6. Пароль не должен включать в себя:

- легко вычисляемые сочетания символов («112», «911» и т.п.);
- клавиатурные последовательности символов и знаков (12345, zxcvb и т.п.);
- повторяющуюся комбинацию из нескольких символов (1111111, wwwww и т.п.);
- общепринятые сокращения (например, «ЭВМ», «ЛВС», «USER» и т.п.);
- аббревиатуры;
- прочие сочетания букв и знаков, ассоциируемые с пользователем;

2.7. Пароль не должен основываться на именах и датах рождения Пользователя или его родственников, кличек домашних животных, номеров автомобилей, телефонов и т.д., которые можно угадать, основываясь на информации о Пользователе.

2.8. Допускается использование единого пароля для доступа субъекта доступа к различным информационным ресурсам одной ИСПДн объекта образования.

2.9. Запрещается:

- сообщать свой пароль полностью или частично другим пользователям;
- спрашивать или подсматривать пароль других пользователе;
- регистрировать других пользователей в ИС ПДн со своим личным паролем;
- входить в ИС ПДн под учётной записью и паролем другого пользователя.

2.10. Сотрудникам допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например Кожзгсф7!).

2.11. Для обеспечения возможности использования имён и паролей некоторых сотрудников в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), сотрудники обязаны сразу же после установки своих паролей передавать их на хранение вместе с именами своих учетных записей администратору безопасности ИС ПДн в запечатанном конверте или опечатанном пенале.

3. ПРАВИЛА РАБОТЫ ПАРОЛЬНОЙ ЗАЩИТЫ

3.1. Пользователи во время процедуры аутентификации (ввода логина и пароля) на АРМ и в ИСПДн должны исключить произнесение логина и пароля вслух, возможность их подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

3.2. Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.

3.3. В ИСПДн устанавливается ограничение на количество неуспешных попыток аутентификации (ввода логина и пароля) Пользователя, равное 7, после чего учетная запись блокируется.

3.4. После 15 минут бездействия (неактивности) Пользователя в АРМ или ИСПДн происходит автоматическое блокирование сеанса доступа в АРМ и ИСПДн соответственно.

3.5. В случае блокировки учетной записи Пользователя после превышения попыток ввода данных аутентификации (логина и пароля) в АРМ или ИСПДн необходимо уведомить Администратора безопасности ИСПДн для проведения процедуры генерации нового пароля.

4. ПОРЯДОК СМЕНЫ ПАРОЛЕЙ

4.1. Смена паролей должна проводиться регулярно, не реже одного раза в год, самостоятельно каждым Пользователем.

4.2. Полная внеплановая смена паролей всех пользователей или удаление учетной записи должна производиться Администратором безопасности ИСПДн в случае прекращения полномочий сотрудников, которым по роду службы были предоставлены полномочия по управлению парольной защитой (увольнение, переход на другую должность в ИСПДн и т.п.) немедленно после окончания последнего сеанса работы Пользователя в АРМ и в ИСПДн соответственно.

4.3. 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.

4.4. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

4.5. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 6-ти позициях.

5. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ ПРИ РАБОТЕ С ПАРОЛЬНОЙ ЗАЩИТОЙ

5.1.Четко знать и строго выполнять требования настоящей инструкции

5.2. 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.

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

5.4. При вводе пароля исключить возможность его перехвата сторонними лицами и техническими средствами.

5.5. Своевременно сообщать Ответственному и Администратору об утере, компрометации и несанкционированном изменении сроков действия паролей в АРМ и ИСПДн соответственно.

6. СЛУЧАИ КОМПРОМЕНТАЦИИ ПАРОЛЕЙ

6.1. Под компрометацией следует понимать:

- 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;
- перехват пароля при распределении идентификаторов;
- сознательная передача информации постороннему лицу.

6.2. Действия при компрометации пароля:

- скомпрометированный пароль сразу же выводится из действия, взамен его вводятся запасной или новый пароль;
- о компрометации немедленно оповещаются все участники обмена информацией. Пароль вносится в специальные списки, содержащие скомпрометированные пароли и учетные записи.

7. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЕЙ ПРИ РАБОТЕ С ПАРОЛЬНОЙ ЗАЩИТОЙ

7.1. Ответственность за организацию парольной защиты и повседневный контроль за действиями сотрудников Учреждения при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на Администратора безопасности информационных систем персональных данных.

7.2. Ответственность в случае несвоевременного уведомлении ответственного за систему защиты информации в информационной системе персональных данных о случаях утери, кражи, взлома или компрометации паролей возлагается на владельца взломанной учетной записи.

7.3. 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.