



Утверждаю:

Директор БОУ «Чебоксарская
общеобразовательная школа для
обучающихся с ограниченными
возможностями здоровья №2»
Минобразования Чувашии
Л.Г. Телеганова
Пр. №30/1 от 31.03.2017г.

Инструкция по организации парольной защиты в информационной системе персональных данных

1. Общие положения.

Настоящая инструкция устанавливает основные правила введения парольной защиты информационной системы персональных данных в БОУ «Чебоксарская общеобразовательная школа для обучающихся с ограниченными возможностями здоровья №2» Минобразования Чувашии (далее – Учреждение). Инструкция регламентирует организационно-техническое обеспечение генерации, смены и прекращения действия паролей в информационной системы персональных данных, а также контроль за действиями пользователей системы при работе с паролями. 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. Правила генерации паролей.

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

2.2. Длина пароля должна быть не менее 6 символов.

2.3. В составе пароля рекомендуется использовать буквы в верхнем и нижнем регистрах, цифры и специальные символы.

2.4. Пароль не должен включать в себя:

- легко вычисляемые сочетания символов;
- клавиатурные последовательности символов и знаков;
- общепринятые сокращения;
- аббревиатуры;
- номера телефонов, автомобилей;
- прочие сочетания букв и знаков, ассоциируемые с пользователем;

– при смене пароля новое сочетание символов должно отличаться от предыдущего не менее чем на 2 символа.

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

3. Порядок смены паролей.

3.1. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в три месяца.

3.2. Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий администраторов средств защиты или других сотрудников, которым по роду службы были предоставлены полномочия по управлению парольной защитой.

3.3. Полная внеплановая смена паролей должна производиться в случае компрометации личного пароля одного из администраторов ИСПДн.

3.4. 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.

4. Обязанности пользователей при работе с парольной защитой.

4.1. 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 к которым могут иметь свободный доступ иные лица.

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

5. Случаи компрометации паролей.

5.1. 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.

5.2. 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.

6. Ответственность пользователей при работе с парольной защитой.

6.1. Повседневный контроль за действиями сотрудников Учреждения при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на ответственного за систему защиты информации в информационной системе персональных данных.

6.2. 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.

6.3. Ответственность за организацию парольной защиты возлагается на ответственного за систему защиты информации в информационной системе персональных данных.

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