«Утверджаю»

Директор МБОУ «СОШ №17»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Грань В.Н.

**Инструкция**

**по организации парольной защиты в ОУ**

1. **Общие положения**

Настоящая инструкция устанавливает основные правила введения парольной защиты информационной системы персональных данных в МБОУ СОШ № 17 (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:

1. **Правила генерации паролей**
   1. Персональные пароли должны генерироваться специальными программными средствами административной службы.
   2. Длина пароля должна быть не более 8 символов.
   3. В составе пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы.
   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.

1. **Порядок смены паролей**
   1. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже однго раза в месяц.
   2. Полная внеплановая смена паролей всех пользователей должна производиться случае прекращения полномочий администраторов средств защиты или других сотрудников, которым по роду службы были предоставлены полномочия по управлению парольной зашитой.
2. **Обязанности пользователей при работе с парольной защитой**
   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 МБОУ СОШ №17 посторонним лицам;
* записывать пароли на бумаге, файле, электронных и прочих носителях информации, в том числе и на предметах.
  1. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе.
  2. При вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами и техническими средствами.

1. **Случаи компрометации паролей**
   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.
  1. 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.

1. **Ответственность пользователей при работе с парольной защитой**
   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.
   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.
   3. Ответственность за организацию парольной защиты возлагается на ответственного за систему защиты информации в информационной системе персональных данных.
   4. 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.

**Лист ознакомления**

**с Инструкцией**

**по организации парольной защиты в МБОУ СОШ № 17**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Фамилия, имя, отчество работника** | **Дата ознакомления с Инструкцией** | **Подпись работника** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |