

УТВЕРЖДАЮ:  
Директор  
МАОУ «Косулинская СОШ № 8»  
И.А. Храмцова  
« 11 » ноября 20 12 г.



## Инструкция по организации парольной защиты в МАОУ «Косулинская СОШ № 8»

### 1. Общие положения

1.1. Инструкция по организации парольной защиты (далее Инструкция) разработана в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Указом Президента Российской Федерации от 06.03.1997 № 188 (в ред. от 23.09.2005) «Об утверждении перечня сведений конфиденциального характера», постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», иными нормативными правовыми актами Российской Федерации.

1.2. Настоящая Инструкция регламентирует организационно-техническое обеспечение процессов установки, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах МАОУ «Косулинская СОШ № 8» (далее — Школа).

1.3. Инструкция призвана регламентировать контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.4. Организационное и техническое обеспечение процессов установки, использования, смены и прекращения действия паролей в информационных системах Школы и контроль за действиями исполнителей при работе с паролями возлагается на директора Школы.

### 2. Правила формирования паролей

2.1. Личные пароли устанавливаются и распределяются централизованно с учетом следующих требований:

2.1.1. Пароль должен состоять не менее чем из шести символов.

2.1.2. В пароле обязательно должны присутствовать буквы из верхнего и нижнего регистров, цифры и специальные символы.

2.1.3. Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, abcd и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно основываясь на информации о пользователе.

2.1.4. При смене пароля новый пароль должен отличаться от старого не менее чем в четырех позициях.

2.2. Пароли пользователей регистрируются в журнале, форма которого установлена в *Приложение 1*. Страницы журнала регистрации паролей пользователей нумеруются,

прошиваются и скрепляются печатью и подписью директора Школы. Журнал регистрации паролей пользователей должен храниться в сейфе ответственного за информационную безопасность — директора Школы.

2.3. При технологической необходимости смены паролей некоторых работников (исполнителей), в том числе в их отсутствие (в случае возникновения внештатных ситуаций, форс-мажорных обстоятельств и т.п.), все изменения вносятся в журнал регистрации паролей пользователей.

### 3. Ввод пароля

3.1. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

## 4. Порядок смены личных паролей

4.1. Смена паролей проводится регулярно, не реже одного раза в три месяца.

4.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) ответственный за информационную безопасность - директор Школы должен немедленно удалить его учетную запись сразу после окончания последнего сеанса работы данного пользователя с системой.

4.3. Срочная (внеплановая) полная смена паролей производится в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

4.4. Смена пароля производится самостоятельно каждым пользователем в соответствии с пунктом 2.1 настоящей Инструкции.

4.5. Временный пароль, заданный ответственным за информационную безопасность - директором Школы, при регистрации нового пользователя, следует изменить при первом входе в систему.

## 5. Хранение паролей

5.1. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе либо в сейфе директора Школы.

5.2. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации.

5.3. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

## 6. Действия в случае утери и компрометации пароля

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 (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.

6.3. В случае утери или компрометации пароля пользователя должны быть немедленно приняты меры в соответствии с пунктом 4.3 или пунктом 4.4 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

## **7. Обязанности пользователей при работе с парольной защитой**

7.1. 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 информационной системе персональных данных посторонним лицам;

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

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

## **8. Ответственность при организации парольной защиты**

8.1. Ответственность за правильность формирования личных паролей пользователей возлагается на директора Школы.

8.2. Владельцы паролей должны быть ознакомлены под расписку с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение информации о пароле.

8.3. Ответственность за организацию парольной защиты в Школе возлагается на ответственного за информационную безопасность - директора Школы.

8.4. Пользователи за несоблюдение или нарушение парольной защиты несут ответственность в соответствии с действующим законодательством Российской Федерации.

## **9. Ответственность пользователей при работе с парольной защитой**

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

9.2. 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.

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

9.4. 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.

## **10. Заключительные положения**

10.1. Работники и лица, имеющие отношение к обработке персональных данных в информационных системах Школы, должны быть ознакомлены с настоящей Инструкцией под расписку.

