Частное образовательное учреждение дополнительного
профессионального образования
«Автошкола Максимум»

ПРИКАЗ № 40

« 10 » Марта 2015 г. г. Владивосток

**Об утверждении Положения
о парольной защите при обработке персональных данных
и иной конфиденциальной информации**

Руководствуясь требованиями федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных", федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" и иных нормативных правовых актов в сфере защиты информации,

ПРИКАЗЫВАЮ

1. Утвердить Положение о парольной защите при обработке персональных данных и иной конфиденциальной информации (далее Положение) (Приложение 1).

2. Руководителю Ражеву Л.И.:

2.1. Довести Положение до сведения руководителей структурных подразделений, где осуществляется обработка персональных данных и иной конфиденциальной информации, а также до сведения Пользователей, допущенных к обработке персональных данных и иной конфиденциальной информации;

2.2. Обеспечить режим парольной защиты при обработке персональных данных и иной конфиденциальной информации в соответствии с утверждённым Положением.

3. Контроль за выполнением настоящего приказа возложить на заместителя руководителя Ражеву О.В.

Директор Ражев Л.И.

Приложение 1
к приказу от10.03.2015 № 40

ПОЛОЖЕНИЕ
о парольной защите при обработке персональных данных и иной конфиденциальной информации

Данное Положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (учетных записей Пользователей) в информационных системах (ИС) образовательного учреждения (далее Оператора), а также контроль за действиями Пользователей и обслуживающего персонала при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех ИС и контроль за действиями Пользователей и обслуживающего персонала при работе с паролями возлагается на сотрудников отдела автоматизированных информационных систем (АИС *или иного соответствующего подразделения, или на уполномоченное лицо) Оператора*) - администраторов парольной защиты.

2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИС самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- личный пароль Пользователь не имеет права сообщать никому.

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. В случае, если формирование личных паролей Пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных сотрудников отдела АИС (*или иного соответствующего подразделения (или уполномоченного лица) Оператора*). Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления самих уполномоченных сотрудников отдела АИС (*или иного соответствующего подразделения (или уполномоченного лица) Оператора*) с паролями других сотрудников подразделений Оператора.

4. При наличии технологической необходимости (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.) использования имен и паролей некоторых сотрудников (Пользователей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей передавать на хранение руководителю своего подразделения их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте. Опечатанные конверты с паролями Пользователей должны храниться в сейфе. Для опечатывания конвертов

должны применяться личные печати владельцев паролей (при их наличии у Пользователей), либо печать отдела АИС (*или иного соответствующего подразделения (или уполномоченного лица) Оператора*).

5. Полная плановая смена паролей Пользователей должна проводиться регулярно, не реже одного раза в квартал *(или в иные установленные Оператором сроки)*.

6. Внеплановая смена личного пароля или удаление учетной записи Пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться сотрудниками отдела АИС (*или иного соответствующего подразделения (или уполномоченного лица) Оператора*) немедленно после окончания последнего сеанса работы данного Пользователя с системой.

7. Внеплановая полная смена паролей всех Пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС.

8. В случае компрометации личного пароля Пользователя ИС должны быть немедленно предприняты меры в соответствии с п. 6 или п. 7 настоящего Положения в зависимости от полномочий владельца скомпрометированного пароля.

9. Хранение Пользователем своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя подразделения в опечатанном личной печатью конверте (возможно вместе с персональными ключевыми носителями и идентификатором Touch Memory).

10. Повседневный контроль за действиями Пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на руководителей подразделений, периодический контроль – возлагается на сотрудников отдела АИС (*или иного соответствующего подразделения (или уполномоченного лица) Оператора*) – администраторов парольной защиты.