Утверждаю
Зав.отделом образования и
молодёжной политики
администрации МО
«Old Станшковский район»
_____/Васильева О.Ю.
«02» марта 2017 г.

ИНСТРУКЦИЯ
по применению парольной защиты и личных идентификаторов в Государственной региональной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования

1. Настоящая Инструкция определяет порядок использования, генерации, смены и прекращения действия присвоение идентификаторов и средств аутентификации пользователей в Государственной региональной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования (далее – ГИС), а также контроль действий пользователей при работе со средствами аутентификации.

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей, а также контроль действий пользователей при работе со средствами аутентификации возлагается на администратора безопасности информации.

3. Идентификаторы пользователей системы должны соответствовать следующим требованиям:

а) идентификатор должен однозначно идентифицировать пользователя;

б) должно быть исключено повторное использование идентификатора пользователя в течение трех лет;

в) должно быть обеспечено блокирование идентификатора пользователя через период времени неиспользования не более 45 дней;

4. Аутентификационные средства (пароли) пользователей ГИС должны выбираться с учетом следующих требований:

а) длина пароля должна быть не менее 6 буквенно-цифровых символов;

б) пароль должен содержать символы разного регистра (прописные/строчные);

в) пароль не должен включать в себя легко вычисляемые (угадываемые) сочетания символов (имена, фамилии, отчества, наименования организации и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER, ADM, ADMIN и т.п.);

г) максимальное действие пароля - не более 90 дней;

д) пароль не должен повторяться;

е) пользователь не может неправильно ввести пароль учетной записи более 5 раз, в этом случае должна происходить блокировка учетной записи пользователя, до момента снятия блокировки.

5. Пароли для администраторов ГИС должны выбираться с учетом следующих требований:

а) длина пароля должна быть не менее 10 буквенно-цифровых символов;

б) пароль должен содержать символы разного регистра (прописные/строчные);

в) пароль должен включать специальные символы;

г) пароль не должен включать в себя легко вычисляемые (угадываемые) сочетания символов (имена, фамилии, отчества, наименования организации и т.д.). а также общепринятые сокращения (ЭВМ, ЛВС, USER, ADM, ADMIN и т.п.);

д) максимальное действие пароля - не более 45 дней;

е) пароль не должен повторяться;

ж) пользователь не может неправильно ввести пароль учетной записи более 5 раз, в этом случае должна происходить блокировка учетной записи пользователя, до момента снятия блокировки.

6. Для генерации «стойких» значений паролей могут применяться специальные программные средства.

а) При первичной регистрации пользователя в системе присвоение идентификатора и выдачу средств аутентификации осуществляет администратор безопасности информации.

б) Пользователи ГИС обязаны хранить свою идентификационную и аутентификационную информацию в тайне от других и не передавать любым способом пароль третьим лицам.

в) Пользователь ГИС лично должен проводить смену пароля регулярно не реже одного раза в три месяца.

г) В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора безопасности информации.

д) Пользователь ГИС обязан хранить свое личное средство аутентификации (аппаратное) в недоступных для других сотрудников хранилищах.

е) Пользователю ГИС запрещается передавать свое личное средство аутентификации (аппаратное).

ж) В случае утери своего личного средства аутентификации (аппаратного), пользователь ГИС должен немедленно доложить об этом администратору безопасности информации.

з) При необходимости передачи пароля удаленному легальному пользователю ГИС администратор безопасности должен обеспечить сохранность передачи данному пользователю пароля путем передачи на электронном носителе в зашифрованном виде, по защищенному каналу связи

или путем личной передачи на бумажном носителе в опечатанном конверте. В случае если пользователь не подтвердил факт получения им пароля, администратор безопасности информации должен произвести смену пароля данного пользователя и произвести повторную передачу пароля.

7. При наличии технологической необходимости использования идентификатора и средств аутентификации пользователей в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), аутентификационная информация пользователя должны быть незамедлительно изменены администратором безопасности информации.

8. Полная плановая смена аутентификационной информации пользователей должна проводиться регулярно, но не реже одного раза в год.

9. В случае прекращения полномочий учетной записи пользователя ГИС (увольнение, переход на другую работу, в другой отдел или помещение, а также другие обстоятельства) учетная запись должна быть удалена, а её средство аутентификации должно быть сдано администратору безопасности информации после окончания последнего сеанса работы данного пользователя в ГИС.

10. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) администратора безопасности информации.

11. В случае компрометации или повреждения средств аутентификации пользователя администратором безопасности информации должны быть немедленно предприняты меры в соответствии с п. 11 настоящей Инструкции.

12. Администратор безопасности информации должен провести служебное расследование для выяснения причин компрометации средств аутентификации с целью выработки новых или совершенствования принятых технических и организационных мер по устранению такой угрозы в будущем, а также выяснению величины ущерба, который может быть нанесен собственнику информационных ресурсов.

13. Пользователи ГИС должны быть ознакомлены под роспись с личными средствами аутентификации и с требованиями настоящей Инструкции.

Разработал Иванова И.В.,
руководитель сектора
отдела образования
и молодёжной политики
администрации
МО «Осташковский район»

Ознакомлен _____ / Иванова И.В.

Дата «02» марта 2017 г