Локальный акт № 37

Принято
На заседании педагогического совета
МБОУ СОШ № 3 с. Астраханка
Протокол № 6 от «29» 01 2021 г

Утверждено
Приказом директора
МБОУ СОШ № 3 сАстраханка
№ 12 от « 29 » 01 2021

ИНСТРУКЦИЯ

по организации парольной защиты в муниципальном бюджетном общеобразовательном учреждении «Средняя общеобразовательная школа № 3» с. Астраханка Ханкайского муниципального округа Приморского края

1. Общие положения

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) и обслуживающего персонала системы при работе с паролями.

Порядок парольной защиты

1. Организованное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей возлагается на учителя информатики Контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на специалиста по защите информации.
2. Личные пароли должны генерироваться и распределяться централизованно с учетом следующих требований:
- длина пароля должна быть не менее 6 символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена. Фамилии, наименование АРМ и т.д), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего;
- личный пароль пользовватель 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 организации.

3. Формирование личных паролей пользователей осуществляется централизованно. Ответственность за правильность их формиррования и

Локальный акт № 37

Принято	Утверждено
На заседании педагогического совета	Приказом директора
МБОУ СОШ № 3 с. Астраханка	МБОУ СОШ № 3 сАстраханка
Протокол № __ от «__» _____20__г	№___ от «____» _____2021

ИНСТРУКЦИЯ

по организации парольной защиты в муниципальном бюджетном общеобразовательном учреждении «Средняя общеобразовательная школа № 3» с. Астраханка Ханкайского муниципального округа Приморского края

1. Общие положения

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) и обслуживающего персонала системы при работе с паролями.

Порядок парольной защиты

1. Организованное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей возлагается на учителя информатики Контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на специалиста по защите информации.
2. Личные пароли должны генерироваться и распределяться централизованно с учетом следующих требований:
- длина пароля должна быть не менее 6 символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена. Фамилии, наименование АРМ и т.д), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего;
- личный пароль пользовватель 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 организации.

3. Формирование личных паролей пользователей осуществляется централизованно. Ответственность за правильность их формиррования и

распределения возлагается на уполномоченного сотрудника (системного администратора).

4. Списки паролей в отпечатанном виде хранятся в сейфе директора.

5. Полная плановая смена паролей пользователей должна проводиться раз в год.

6. Внеплановая смена личного пароля или удаление учетной записи пользователя в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.)должна производиться по представлению администратора безопасности уполномоченными сотрудниками немедленно после окончания последнего сеанса работы данного пользователя с системой.

7. В случае компрометации личного пароля пользователя должны быть немедленно предприняты меры в соответствии с п.6 настоящей Инструкции.

8. Хранение сотрудником (исполнителем) значений своих паролей на материальном носителе допускается.

9. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены и использования в подразделениях возлагается на администратора безопасности подразделения.

Ответственность

Пользователь и администратор безопасности несут ответственность за качество и своевременность выполнения задач и функций, возложенных на них в соответствии с настоящей Инструкцией.