СОГЛАСОВАНО
Начальник сервисного центра
в г.Мурманск ЗАО «Гринатом»
«06» октября 2015 г.

_____ В.Б. Удин

УТВЕРЖДЕНО
Приказом № 68-02 от 06.10.2015 г.
ректор Мурманской академии
экономики и управления
д-р экон. наук, профессор
_____ Н.Н. Щебарова

ИНСТРУКЦИЯ
по организации парольной защиты информации

Мурманск
2015 г.

1. Общие положения

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в ИСПДн МАЭУ, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

2. Порядок парольной защиты

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в ИСПДн возлагается на техника ЦИТ. Контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на сотрудника, ответственного за безопасность персональных данных в подразделении.

2. Личные пароли должны генерироваться и распределяться централизованно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER, PASSWORD 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. Формирование личных паролей пользователей осуществляется централизованно. Ответственность за правильность их формирования и распределения возлагается на уполномоченного сотрудника техника ЦИТ. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления (самих уполномоченных сотрудников, а также руководителей подразделений) с паролями других сотрудников подразделений.

4. Списки паролей подлежат уничтожению сразу после выдачи их пользователям и хранению не подлежат.

5. Полная плановая смена паролей пользователей должна проводиться регулярно.

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

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

8. Хранение сотрудником (исполнителем) значений своих паролей на материальном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя подразделения.

9. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены и использования в подразделениях возлагается на сотрудника, отвечающего за безопасность персональных данных в подразделении.

3. Ответственность

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