**ИНСТРУКЦИЯ**

по организации парольной защиты информационной системы персональных данных администрации Грачевского муниципального округа Ставропольского края

**1 Общие сведения**

1. Данная Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных (далее - ИСПДн) администрации Грачевского муниципального округа Ставропольского края , а также контроль за действиями пользователей и обслуживающего персонала систем при работе с паролями.
2. Организационное и техническое обеспечение процессов генерации,  
   использования, смены и прекращения действия паролей во всех подсистемах и  
   контроль за действиями исполнителей и обслуживающего персонала системы  
   при работе с паролями возлагается на администратора информационной безопасности и ответственного за информационную безопасность (далее - ИБ).

**2 Требования к паролям**

**2.1** Личные пароли должны выбираться пользователями информационной системы персональных данных самостоятельно с учетом следующих требований:

* длина пароля должна быть не менее 6 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 4 позициях;
* личный пароль пользователь не имеет права сообщать никому.

1. 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.
2. Для генерации «стойких» значений паролей могут применяться  
   специальные программные средства. Система генерации паролей должна исключать возможность ознакомления других сотрудников с паролями исполнителей.

**3 Смена паролей**

1. Полная плановая смена паролей пользователей должна проводиться  
   регулярно, не реже одного раза в два месяца.
2. Внеплановая смена личного пароля или удаление учетной записи  
   пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и т.п.)должна производиться администраторами соответствующих средств защиты немедленно после окончания последнего сеанса работы данного пользователя с системой.
3. Внеплановая полная смена паролей всех пользователей должна  
   производиться в случае прекращения полномочий (увольнение, переход на  
   другую работу внутри организации и другие обстоятельства) администраторов  
   средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем ИСПДн.

**4 Хранение и контроль**

4.1 Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у ответственного за информационную безопасность или у руководителя подразделения в опечатанном личной печатью пенале.

1. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на начальников отделов, периодический контроль - возлагается на администраторов ИБ.
2. В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры по изменению пароля и выявлению последствий компрометации.