emblem

**УПРАВЛЕНИЕ ПО ОБЕСПЕЧЕНИЮ ДЕЯТЕЛЬНОСТИ**

**МИРОВЫХ СУДЕЙ НОВОСИБИРСКОЙ ОБЛАСТИ**

**ПРИКАЗ**

«\_\_\_» \_\_\_\_\_\_\_\_ 2017г. № \_\_\_\_\_

г. Новосибирск

**Об утверждении инструкции по организации парольной защиты автоматизированной системы**

В соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» в целях реализации постановления Правительства Российской Федерации от 21.03.2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, **п р и к а з ы в а ю :**

1. Утвердить инструкцию по организации парольной защиты автоматизированной системы (Приложение №1).

2. Контроль за исполнением приказа оставляю за собой.

|  |  |
| --- | --- |
| Начальник управления | В.А. Чиркунов |

ПРИЛОЖЕНИЕ № 1

УТВЕРЖДЕНО

приказом начальника управления по обеспечению деятельности мировых судей

Новосибирской области

от «\_\_\_\_»\_\_\_\_\_2017 №\_\_

**Инструкция по организации парольной защиты**

**автоматизированной системы**

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в автоматизированной системе Управления (АС Управления), а также контроль за действиями сотрудников Управления при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах АС Управления и контроль за действиями сотрудников Управления при работе с паролями возлагается на сотрудника Управления - администратора средств защиты, содержащих механизмы идентификации и аутентификации (подтверждения подлинности) пользователей по значениям паролей.

2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями автоматизированной системы 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 уполномоченного сотрудника Управления. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления самих уполномоченных сотрудников Управления, а также ответственных за информационную безопасность в Управлении.

4. При наличии в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей некоторых сотрудников в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение ответственному за информационную безопасность в Управлении. Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при их наличии у исполнителей), либо печать уполномоченного сотрудника Управления.

5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в месяц.

6. Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу внутри Управления и т.п.) должна производиться уполномоченными сотрудниками Управления 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 внутри управления и другие обстоятельства) сотрудника Управления и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем АС.

8. В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п.6 или п.7 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

9. Хранение сотрудником значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у ответственного за информационную безопасность в опечатанном личной печатью пенале (возможно вместе с персональными ключевыми дискетами и идентификатором Touch Memory).

10. Повседневный контроль за действиями сотрудников Управления при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственных за информационную безопасность в Управлении.