Приложение М
к Положению о защите
информации СФУ
(утверждено приказом
от 25.02.2015 № 200)

# Инструкция
# по организации парольной защиты
# при работе на средствах вычислительной техники

1 Ответственность за организацию системы парольной защиты несут:

в подразделении – руководитель подразделения;

в автоматизированной системе – руководитель подразделения, сопровождающего эту систему, и администратор системы;

на АРМ – пользователь.

2 Личные пароли генерируются и распределяются централизованно либо выбираются пользователями информационной системы (ПЭВМ) самостоятельно с учетом следующих требований:

– пароль должен состоять не менее чем из шести символов, а для административных учетных записей не менее десяти, большее количество символов повышает его надежность;

– пароль обязательно должен состоять из букв и цифр, использование букв в верхнем и нижнем регистрах и специальные символы (@, #, $, &, *, % и т.п.) повышают его надежность;

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т. п.), последовательности символов и знаков (123, abcd и т. п.), общепринятые сокращения (ЭВМ, ЛВС и т. п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе;

– новый пароль пользователя не должен совпадать с именем учетной записи пользователя и с предыдущими паролями, должен отличаться от старого не менее чем в шести позициях.

3 Пароли пользователей на доступ к различным ресурсам (для входа в операционную систему ПЭВМ, информационную систему, базы данных, электронной почты и др.) должны быть различными.

4 При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его видеть посторонними лицами (другими работниками, посетителями).

5 Запрещается включать пароли в какой-либо автоматизированный процесс начала сеанса, например с использованием хранимых макрокоманд или функциональных клавиш.

6 Смена паролей должна проводиться регулярно, не реже одного раза в три месяца, а также в случае прекращения полномочий пользователя (увольнение, переход на другую работу и т. п.) или в случае компрометации пароля (если он стал известен другим лицам или есть подозрение об этом).

7 Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т. п.) администраторов информационной системы и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

8 Смена пароля производится самостоятельно каждым пользователем в соответствии с п. 1. настоящей Инструкции и/или в соответствии с указанием в системном баннере-предупреждении (при наличии технической возможности).

9 Временный пароль, заданный системным администратором при регистрации нового пользователя, следует изменить при первом входе в систему.

10 Пользователь обязан сохранять в тайне свой индивидуальный пароль, не сообщать его другим лицам и не регистрировать их в системе под своим паролем.

11 Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации.

12 При технологической необходимости использования имен и паролей работников (исполнителей) в их отсутствие (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т. п.) работники обязаны значение своих паролей в запечатанном конверте передать на хранение руководителю подразделения или другому назначенному им лицу. Конверт с паролем должен храниться в месте (сейф, надежно запирающийся шкаф и др.), исключающем несанкционированный доступ.

13 В автоматизированных системах, обрабатывающих конфиденциальную информацию, необходимо использовать повышенные требования к парольной защите: автоматическую блокировку учетных записей пользователя в случае окончания срока действия пароля, после 3-5 неудачных попыток авторизации и в других случаях. При этом блокировка должна сниматься «вручную» системным администратором или специалистом службы технической поддержки с одновременной сменой пароля пользователя. В журнал системных событий сервера должно заноситься сообщение о многократно неудавшихся попытках авторизации пользователя.