Приложение № 11
к распоряжению Администрации
ЗАТО г. Железногорск
от 30.06.2014 № 132пр

ИНСТРУКЦИЯ

по организации парольной защиты в информационных системах персональных данных
Администрации ЗАТО г. Железногорск

2013

1 Общие положения

Настоящая инструкция предназначена для использования в работе пользователями информационных систем персональных данных (ИСПДн) «Бухгалтерия», «Гаражи и усадьбы», «Кадры», «СОТО», «АРМ «Административная комиссия», «АРМ «Договора», «АРМ «ЖФСИ», «АРМ «Общественная приемная», «АРМ «Спортсмены», «АРМ «Учет карточек профсоюза», «АРМ «Формирование изменений списков избирателей» Администрации ЗАТО г. Железногорск и определяет порядок обеспечения защиты от несанкционированного доступа к информации (НСД).

Парольная защита при работе в ИСПДн осуществляется с целью предотвращения НСД к конфиденциальной информации и персональным данным, обрабатываемым в ней.

Парольная защита является составной частью подсистемы управления доступом системы защиты информации от НСД.

Компрометация действующих паролей является служебным проступком, о чем администратор безопасности сообщает ответственному за защиту и обработку конфиденциальной информации и персональных данных.

Под компрометацией понимается хищение, утрата действующих паролей, передача или сообщение их лицам, не имеющим на то право, другие действия сотрудника, приведшие к получению его пароля лицами, не имеющими на то право. Скомпрометированные пароли выводятся из действия немедленно.

2 Требования к организации парольной защиты

Личные пароли доступа ОС выбираются пользователями самостоятельно, но при этом необходимо руководствоваться следующими требованиями:

- длина пароля должна быть не менее 6 символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имя, фамилия, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства, наименования АРМ, общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP, GUEST, ADMINISTRATOR и т.д.), и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе;
- не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
- не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 или 1йфячыц2 и т. п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 5 позициях;
- не использовать ранее использованные пароли.

Лица, использующие пароли, обязаны:

– четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по использованию парольной защиты;
– своевременно сообщать администратору безопасности обо всех нештатных ситуациях и нарушениях работы подсистем защиты от НСД, возникающих при работе с паролями.

При организации парольной защиты запрещается:

– записывать свои пароли в очевидных местах (стикерах, мебели, на обратной стороне клавиатуры и т.п.);
– сообщать посторонним лицам свои пароли, а также сведения о применяемой системе защиты информации от НСД.
– самостоятельно производить смену пароля для входа в операционную систему.

3 Смена пароля пользователя

Плановая смена паролей в ИСПДн проводится регулярно, не реже одного раза в 6 месяцев.

Удаление (в том числе внеплановая смена) личного пароля любого пользователя ИСПДн должна производиться в следующих случаях:

– по окончании срока действия;
– в случае прекращения его полномочий (увольнение, переход на другую работу) после окончания последнего сеанса работы;
– при обнаружении факта успешной попытки несанкционированного доступа к элементам ИСПДн;
– по указанию администратора безопасности.

Пароли, используемые для доступа к ресурсам ИСПДн, вводятся пользователем с клавиатуры.

Лист ознакомления

С настоящей инструкцией ознакомлен:

ФИО	Должность	Подпись	Дата