

УТВЕРЖДАЮ

Директор
МКОУ СОШ №2 г.Алагира

Сидомонидзе Ф.Н.

« 1 » 20 17 г.



ИНСТРУКЦИЯ

по организации парольной защиты на объекте информатизации «Информационная система персональных данных «АРМ» МКОУ СОШ №2 г.Алагира»

Настоящая инструкция определяет порядок организации парольной защиты на объекте информатизации «Информационная система персональных данных «АРМ» МКОУ СОШ №2 г.Алагира» (далее - ИСПДн).

1. Общие положения

1.1. Настоящая Инструкция предназначена для использования в работе на объекте информатизации и определяет порядок обеспечения защиты информации при использовании подсистемы парольной защиты от НСД.

1.2. Парольная защита при работе на ИСПДн осуществляется с целью предотвращения НСД к защищаемой информации.

1.3. Парольная защита ИСПДн является составной частью подсистемы управления доступом общей системы защиты от НСД.

К основным видам (категориям) паролей относятся:

- пароли BIOS;
- пароль доступа СЗИ от НСД;
- пароли систем доступа, встроенных в используемые ОС;
- пароли доступа к прикладным программам, обеспечивающим доступ к защищаемой информации;
- пароли доступа к специализированному программному обеспечению (СПО), предназначенному для работы с защищаемой информацией.

1.4. Порядок работы с паролями вводится с момента подписания данной Инструкции.

2. Требования к организации парольной защиты ОИ

2.1. Личные пароли доступа к ИСПДн, СЗИ от НСД, первично назначаются пользователям Администратором ИБ при формировании персонального идентификатора, при этом необходимо руководствоваться следующими требованиями:

- длина пароля должна быть не менее **шести** символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства, наименования ИСПДн, общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP, GUEST, ADMINISTRATOR и т.д.), и другие данные, которые могут быть подобраны путем анализа информации об ответственном исполнителе;
- 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, 123456 и т. п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее, чем в 4 позициях;

- в числе символов пароля могут присутствовать латинские буквы в верхнем и нижнем регистрах, цифры;
- не использовать ранее использовавшиеся пароли.

2.2. Лица, использующие пароли, обязаны:

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

2.3. При организации парольной защиты запрещается:

- записывать свои пароли в очевидных местах (внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.п.);
- хранить пароли в записанном виде в рабочих тетрадях, на отдельных листах бумаги;
- сообщать посторонним лицам свои пароли, а также сведения о применяемой системе защиты от НСД.

2.4. Руководитель подразделения, в ведении которого находится ИСПДн, несет личную ответственность за организацию работ по безусловному выполнению требований настоящей инструкции и других документов, регламентирующих использование парольной защиты.

2.5. Ответственность за непосредственную работу с паролями (своевременный ввод, замену и уничтожение) возлагается на Администратора ИБ ИСПДн.

2.6. На ответственного за ЗИ в ИСПДн возлагаются следующие задачи:

- обеспечение руководства над функционированием системы парольной защиты;
- контроль за реализацией требований по обеспечению безопасности информации при использовании паролей и их своевременную смену в ИСПДн.

3. Порядок применения парольной защиты

3.1. Порядок применения парольной защиты основанной на использовании СЗИ от НСД приведен в руководствах Администратора ИБ и пользователя ИСПДн.

Защита с применением паролей других программно – технических средств и программных продуктов осуществляется, при их наличии, в соответствии с эксплуатационной документацией на эти средства.

Полная плановая смена паролей в ИСПДн проводится регулярно Администратором ИБ ИСПДн и пользователями, не реже одного раза в 6 (шесть) месяцев.

3.2. Удаление (в т.ч. внеплановая смена) личного пароля должна производиться в следующих случаях:

- по окончании срока действия;
- в случае прекращения полномочий пользователя (увольнение, переход на другую работу, не связанную с обработкой защищаемой информации);
- по указанию начальника подразделения или ответственного за ЗИ ИСПДн.

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

3.4. Компрометация действующих паролей является нештатной ситуацией, о чем Администратор ИБ ИСПДн сообщает ответственному за ЗИ.

Под компрометацией понимается хищение, утрата действующих паролей, передача или сообщение их лицам, не имеющим на то право, другие действия должностных лиц, приведшие к получению его пароля лицами, не имеющими на то права.

3.6. Скомпрометированные пароли и связанные с ними персональные идентификаторы пользователей незамедлительно выводятся из действия.

Порядок внеплановой смены пароля аналогичен плановой смене паролей.

Ответственный за защиту информации



