Восстановление (сброс) пароля BIOS (GNU/Linux)

Дешифрация существующего пароля BIOS

Существует немало программного обеспечения, как платного, так и свободно распространяемого, для дешифрации забытого пароля, хранящегося в энергонезависимой памяти CMOS. Но, к сожалению, универсальных "взломщиков" паролей не существует.

Даже профессиональные версии, стоящие приличные деньги, ориентированы на использование под конкретные модели материнских плат. Из бесплатно распространяемого ПО, очень неплохими возможностями обладает CmosPwd.

Официальный сайт - www.cgsecurity.org
sudo apt install cmospwd
Программа позволяет дешифрировать пароли к BIOS следующих производителей:

ACER/IBM BIOS
AMI BIOS
AMI WinBIOS 2.5
Award 4.5x/4.6x/6.0
Compaq (1992)
Compaq (New version)
IBM (PS/2, Activa, Thinkpad)
Packard Bell
Phoenix 1.00.09.AC0 (1994), a486 1.03, 1.04, 1.10 A03, 4.05 rev 1.02.943, 4.06 rev 1.13.1107
Phoenix 4 release 6 (User)
Gateway Solo - Phoenix 4.0 release 6
Toshiba
Zenith AMI

Примеры:

cmospwd /k - Сбросить CMOS
cmospwd /d - Выдать дамп содержимого CMOS
cmospwd /w mycmos.bin - записать содержимое CMOS в файл mycmos.bin
cmospwd /l mycmos.bin - загрузить содержимое CMOS из файла mycmos.bin
cmospwd /m1101 - выполнять поиск пароля выборочно (1 - проверка выполняется)

Если же подобрать пароль не удалось, попробуйте его сбросить. На большинстве материнских плат имеется специальный переключатель, обычно обозначаемый "Clear CMOS", позволяющий сбросить содержимое энергонезависимой памяти. Если же такого переключателя нет или нельзя вскрывать корпус компьютера, можно сбросить пароль программными средствами, например, использованием ключа /k выше упомянутой cmospwd.

Принцип сброса пароля основан на записи в ячейки CMOS какой-нибудь информации без изменения контрольной суммы. При выполнении самотестирования по включению питания (процедуры POST) выполняется проверка контрольной суммы содержимого CMOS и, в случае ошибки, выполняется сброс настроек по умолчанию (в Default) . При этом пароль также сбрасывается.

При отсутствии специальной программы для очистки CMOS, можно воспользоваться любой программой, позволяющей выполнять запись в порты ввода-вывода. Запись в порт 70H задает адрес ячейки CMOS, а запись в порт 71H - ее содержимое.

Идеальным вариантом было бы писать непосредственно в ту ячейку, где хранится контрольная сумма. Когда-то (кажется до появления PS/2) контрольная сумма хранилась в ячейках 2Eh и 2Fh и изменение их содержимого однозначно приводила к сбросу CMOS.