Методы защиты средств вычислительной техники

Варианты атак

Для несанкционированного получения информации наиболее вероятными являются следующие варианты атак:

- 1. Атака целевым вирусом (закладкой).
- 2. Атака общим вирусом

Против атак можно применить различные

проверки целостности программного обеспечения (ПО),

которые, в свою очередь, могут быть нейтрализованы ***стелс-механизмами вирусов***

Однако существуют закладки, работающие в защищенном режиме микропроцессора (МП), блокирующие всякого рода попытки программ пользователя переключиться в защищенный режим и эмулирующие все известные способы обращения к расширенной памяти.

При таком подходе любые способы контроля целостности ПО не дадут корректного результата.

***Утверждение* 1:**

- гарантированно корректно работает та программа (закладка или средство защиты от нее), которая первой получает управление.

- Для гарантированно корректной работы средств защиты от закладок необходимо проверять целостность программных файлов до начала работы программы первичного загрузчика.

Электронные замки

Фирмы-разработчики BIOS предлагают парольную защиту входа в компьютер, при этом пароль хранится в виде свертки в энергонезависимой памяти компьютера (CMOS).

Такая защита неэффективна, так как в случае получения доступа к включенному компьютеру можно считать содержимое CMOS и тем самым получить доступ к информации о пароле.

***Утверждение 2*:**

для гарантированной работы электронного замка достаточно, чтобы программа защиты от закладок и свертка пароля были аппаратно защищены от чтения программными средствами во время работы компьютера

Защита от несанкционированного доступа

В общем случае несанкционированный доступ является реализацией **преднамеренной угрозы информационной безопасности**.

Варианты НСД

- доступ к носителям информации;
- локальный доступ к отдельным персональным компьютерам;
- локальный доступ к ресурсам сети;
- удаленный доступ к отдельным компьютерам или ресурсам сети.

НСД к носителям информации

Предотвращение НСД к носителям информации обеспечивается физическими мерами защиты (пропускной режим, охрана, замки на дверях, сейфы и т. д.).

Локальный доступ к отдельным персональным компьютерам

1) физические меры защиты (пропускной режим, охрана, замки на дверях, сейфы и т. д.).
2) программно-технические способы защиты

Парольная защита с помощью стандартных системных средств

Их особенностью является использование возможностей защиты, непосредственно встроенных в системные программы и операционные системы компьютеров.

Поэтому использование этих методов не требует дополнительных затрат на приобретение специализированных программ или дополнительных технических средств.

Парольная защита отдельных персональных компьютеров

Парольная защита отдельных персональных компьютеров

Основная задача этого вида парольной защиты — предотвратить доступ посторонних лиц к информации на личном компьютере в отсутствие владельца

Парольная защита отдельных персональных компьютеров

В системных средствах компьютера существуют два вида парольной защиты:

1. защита от включения компьютера
2. защита от доступа к включенному компьютеру в отсутствие пользователя-владельца.

Защита от включения компьютера

может быть реализована с помощью установки пароля в BIOS

Взлом:

- имеется аппаратный способ отключения пароля в BIOS
- во многих версиях BIOS имеются так называемые технологические пароли, введенные производителями. Списки этих паролей можно найти в Internet
- пароль можно подобрать или просто подсмотреть

Защита от включения компьютера

В качестве дополнительного средства защиты можно использовать так называемый **пароль Windows**, который блокирует только загрузку операционной системы, уже установленной на персональном компьютере.

Для более надежной защиты от несанкционированного включения компьютера в обоснованных случаях применяются специализированные программно-технические средства.

Защита от доступа к включенному компьютеру

выключение его на время отсутствия владельца.

- Однако это далеко не всегда удобно.
- Кроме того, частое включение/выключение снижает ресурс компьютера, поскольку возникающие при этом перепады температуры и напряжения отрицательно сказываются на электронных компонентах.

Защита от доступа к включенному компьютеру

установка паролей в программах, называемых хранителями экрана (Screen Savers), которые входят в состав всех версий Windows.

Защита от доступа к включенному компьютеру

установка паролей в программах, называемых хранителями экрана (Screen Savers), которые входят в состав всех версий Windows.

Reset

Поэтому важно, чтобы этот способ защиты сочетался с рассмотренной выше защитой от несанкционированного доступа при загрузке компьютера

Парольная защита в локальных сетях

Парольная защита в локальных сетях

парольная защита наряду с рассмотренными выше функциями выполняет и функции разграничения доступа пользователей к информационным ресурсам сети (администрирование сети)

Возможность установки подобного вида защиты заложена в стандартные средства известных операционных сред.

Парольная защита в локальных сетях

Для повышения надежности защиты информации ее целесообразно хранить непосредственно на сервере, доступ к которому ограничивается мерами физической защиты.

Парольная защита в локальных сетях

Однако даже правильно сконфигурированная сеть, информационные ресурсы сервера и персональных станций которой защищены паролями, не предоставляет, к сожалению, абсолютно надежной защиты информации. Дело здесь опять в том, что пароль можно «подсмотреть» (если он, например, записан на бумажке) или подобрать.