Защита информации

Проблема обеспечения защиты информации охватывает как физическую защиту данных и системных программ, так и защиту от несанкционированного доступа к данным, передаваемых по линиям связи и находящихся на накопителях.

Три обобщенных механизма управления доступа к данным:

- идентификация пользователя (определяет доступ к различным базам данных или их частям);
- непосредственная физическая защита данных (кодирование);
- поддержка прав доступа пользователя к данным с возможностью их передачи.

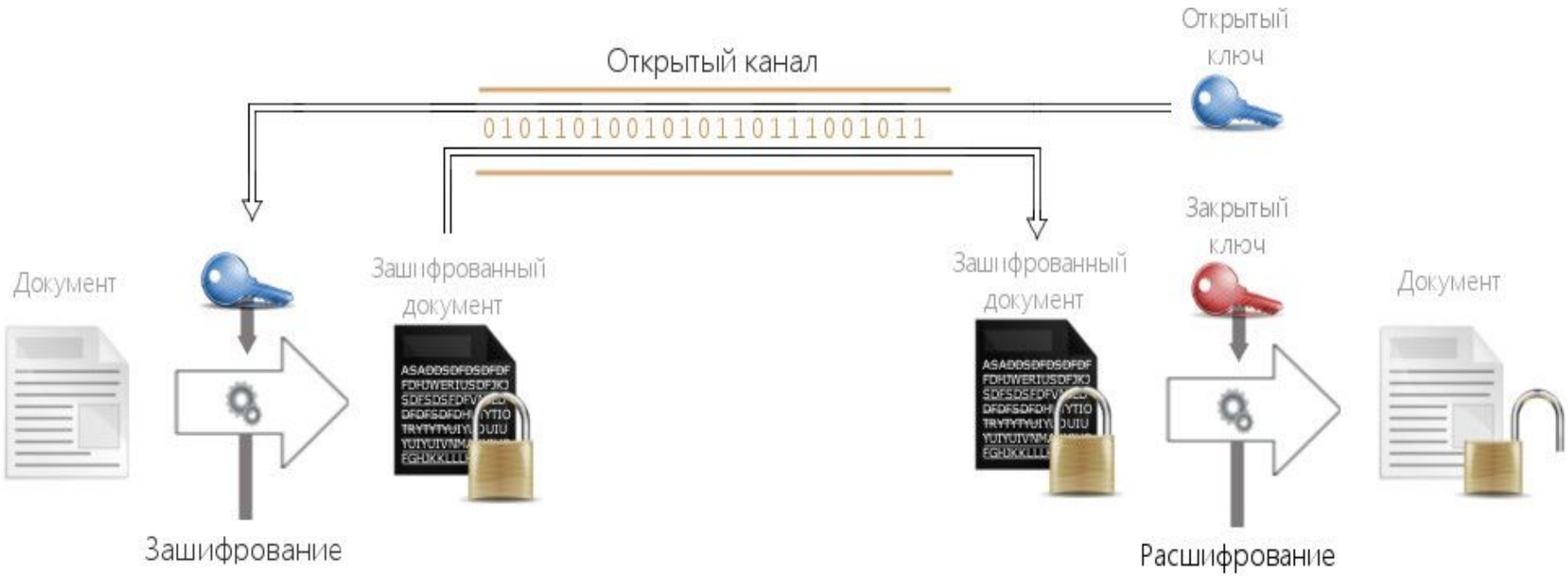
Методы защиты информации

- *Методы защиты при помощи программных паролей* (реализуется программными средствами).

- *Метод автоматического обратного вызова.*

- *Метод симметричного шифрования данных.*

- *Метод асимметричного шифрования данных (с открытым ключом).*



Способы защиты информации

Препятствия предусматривают создание преград, физически не допускающих к информации.

Управление доступом – способ защиты информации за счет регулирования использования всех ресурсов системы (технических, программных и др.).

Маскировка информации, как правило, осуществляется путем ее криптографического закрытия.

Регламентация заключается в реализации системы организационных мероприятий, определяющих все стороны обработки информации.

Средства защиты информации разделяют на:

- технические,
- программные
- социально-правовые.

Среди технических средств защиты выделяют физические и аппаратные.

- *Криптографические программы* основаны на использовании методов шифрования (кодирования) информации.

Средства защиты информации от компьютерных вирусов

Следует отметить, что используемые антивирусные программы и аппаратная часть не дают полной гарантии защиты от вирусов.

Вирусы бывают:

- загрузочные (boot) – заражают программу начальной загрузки, хранящуюся в загрузочном секторе диска, запускаются при загрузке компьютера;
- файловые – заражают исполняемые файлы (.exe);

- загрузочно-файловые – имеют признаки и тех, и других;
- драйверные – заражают драйверы устройств компьютера;
- сетевые – распространяются в сетях.

Антивирусные программы :

Детекторы – обнаруживают вирусы. В настоящее время в чистом виде очень редки.

Фаги, или программы-доктора – программы, которые способны не только обнаружить вирус, но и уничтожить его, т. е. удалить его код из зараженных программ и восстановить их работоспособность (Symantec Antivirus, Panda Antivirus, Norton Antivirus, Doctor Web).

Вакцины, или иммунизаторы – резидентная программа, предотвращающая заражение файлов.

Ревизоры – запоминают исходное состояние программ, каталогов и системных областей диска, когда компьютер не заражен, периодически сравнивая текущее состояние с исходным.

Сторожа – это резидентная программа, постоянно находящаяся в памяти компьютера и контролирующая операции, связанные с попыткой коррекции файлов (.exe, .com) и изменением атрибутов файлов, записи загрузочного сектора диска, прямой записи на диск.