несанкционированного доступа.

Подготовила ученица
9 класса
Желязкова Ульяна.

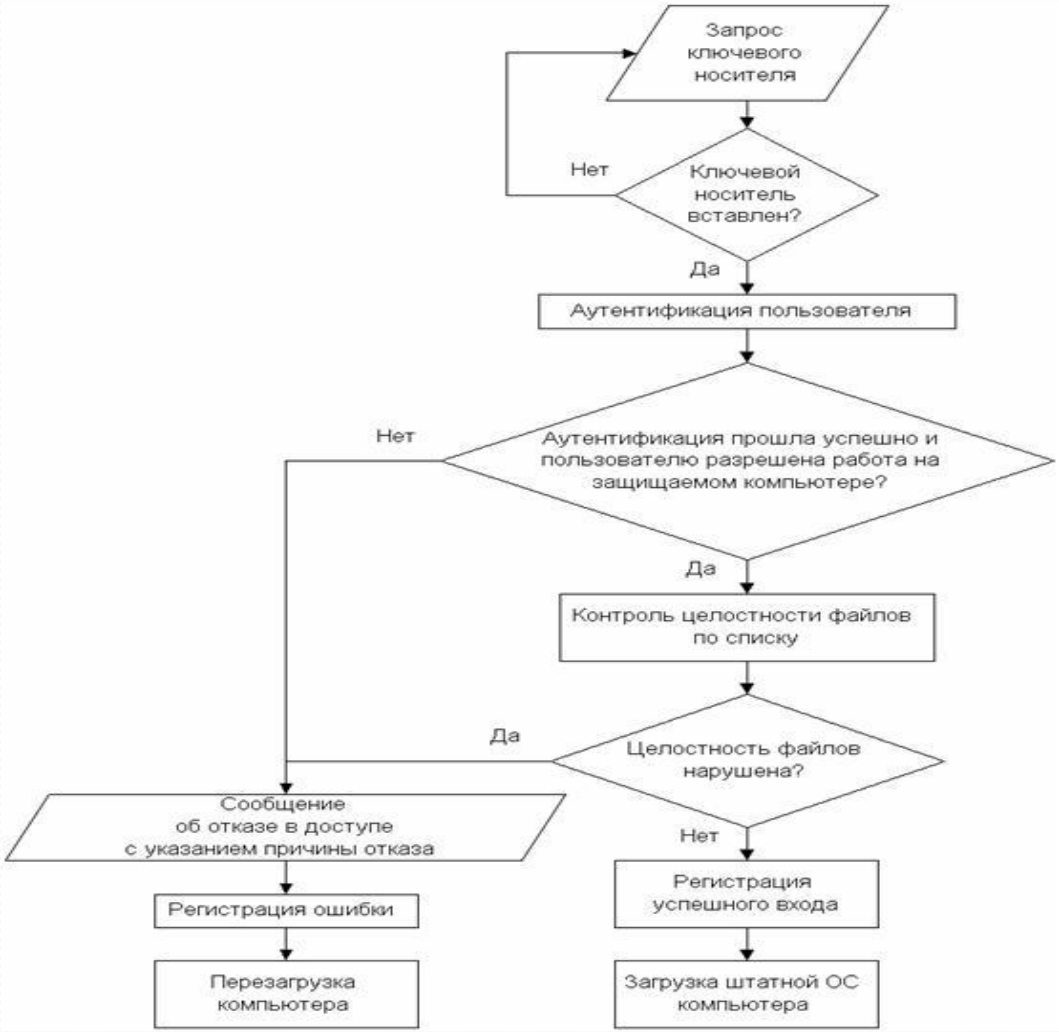
Проблема несанкционированного доступа

Несанкционированный доступ (НСД) злоумышленника на компьютер опасен не только возможностью прочтения или модификации обрабатываемых электронных документов, но и возможностью внедрения злоумышленником управляемой программной закладки, которая позволит ему предпринимать следующие действия:

- Читать или модифицировать электронные документы, которые в дальнейшем будут храниться или редактироваться на компьютере.
- Осуществлять перехват различной ключевой информации, используемой для защиты электронных документов.
- Использовать захваченный компьютер в качестве плацдарма для захвата других компьютеров локальной сети.
- Уничтожить хранящуюся на компьютере информацию или вывести компьютер из строя путем запуска вредоносного программного обеспечения.

Средства ограничения физического доступа

Наиболее надежное решение проблемы ограничения физического доступа к компьютеру – использование аппаратных средств защиты информации от НСД, выполняющихся до загрузки операционной системы. Средства защиты данной категории называются «электронными замками».



Злоумышленник может просто вытащить замок из компьютера. Однако, существует ряд мер противодействия:

*Различные организационно-технические меры: пломбирование корпуса компьютера, обеспечение отсутствие физического доступа пользователей к системному блоку компьютера и т. д.

* Существуют электронные замки, способные блокировать корпус системного блока компьютера изнутри специальным фиксатором по команде администратора – в этом случае замок не может быть изъят без существенного повреждения компьютера.

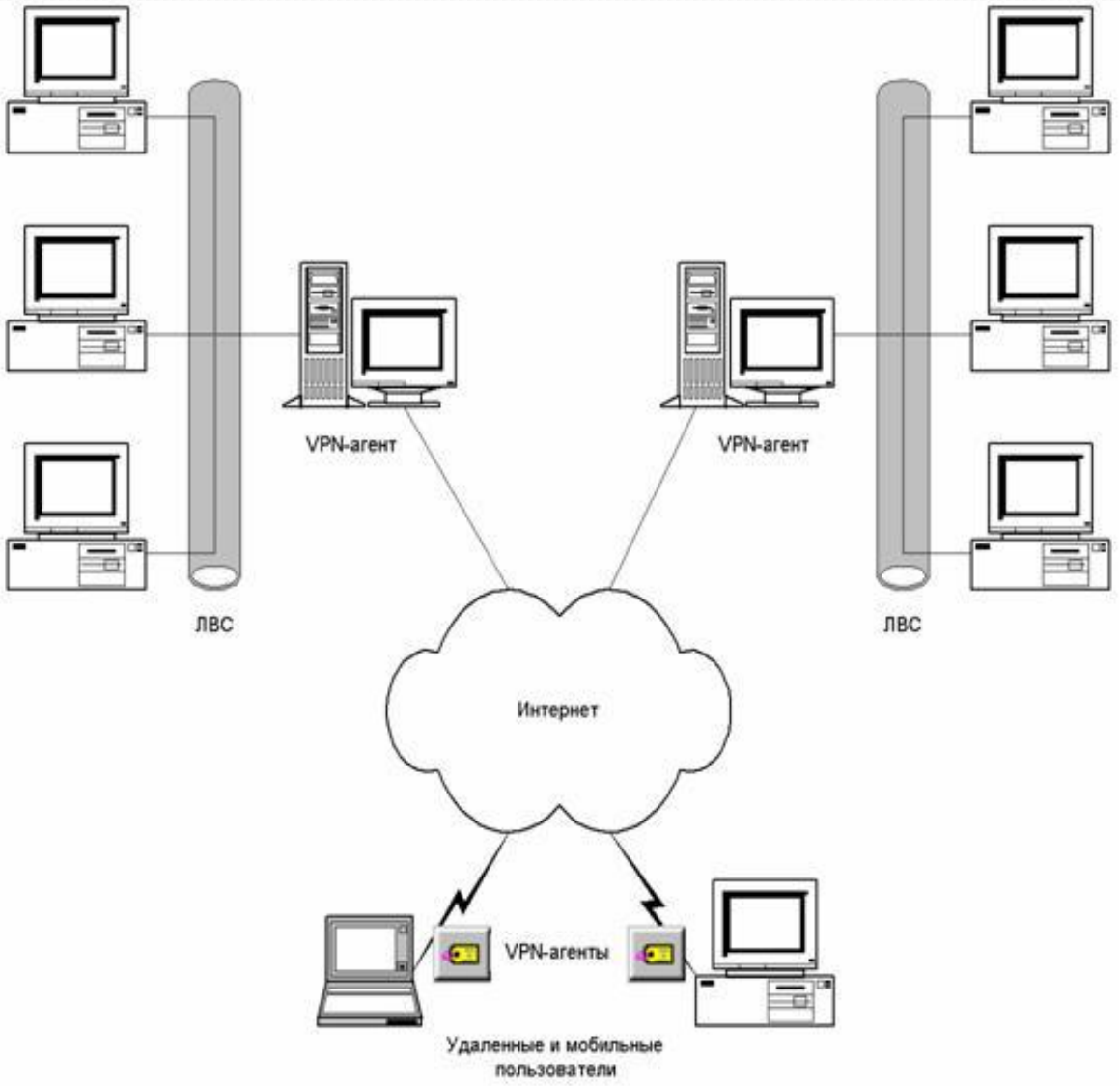
Средства защиты от НСД по сети

- Наиболее действенными методами защиты от несанкционированного доступа по компьютерным сетям являются виртуальные частные сети и межсетевое экранирование.

Виртуальные частные сети

Виртуальные частные сети обеспечивают автоматическую защиту целостности и конфиденциальности сообщений, передаваемых через различные сети общего пользования. Фактически, VPN – это совокупность сетей, на внешнем периметре которых установлены VPN-агенты. VPN-агент – это программа, собственно обеспечивающая защиту передаваемой информации путем выполнения определенных операций.

VPN-агент может находиться непосредственно на защищаемом компьютере. В этом случае с его помощью защищается информационный обмен только того компьютера, на котором он установлен, однако описанные выше принципы его действия остаются неизменными.



Межсетевое экранирование

Межсетевой экран представляет собой программное или программно-аппаратное средство, обеспечивающее защиту локальных сетей и отдельных компьютеров от несанкционированного доступа со стороны внешних сетей путем фильтрации двустороннего потока сообщений при обмене информацией. Фактически, межсетевой экран является «урезанным» VPN-агентом, не выполняющим шифрование пакетов и контроль их целостности, но в ряде случаев имеющим ряд дополнительных функций, наиболее часто из которых встречаются следующие:

- антивирусное сканирование;
- контроль корректности пакетов;
- контроль корректности соединений;
- контент-контроль.

Межсетевые экраны, не обладающие описанными выше функциями и выполняющими только фильтрацию пакетов, называют пакетными фильтрами.

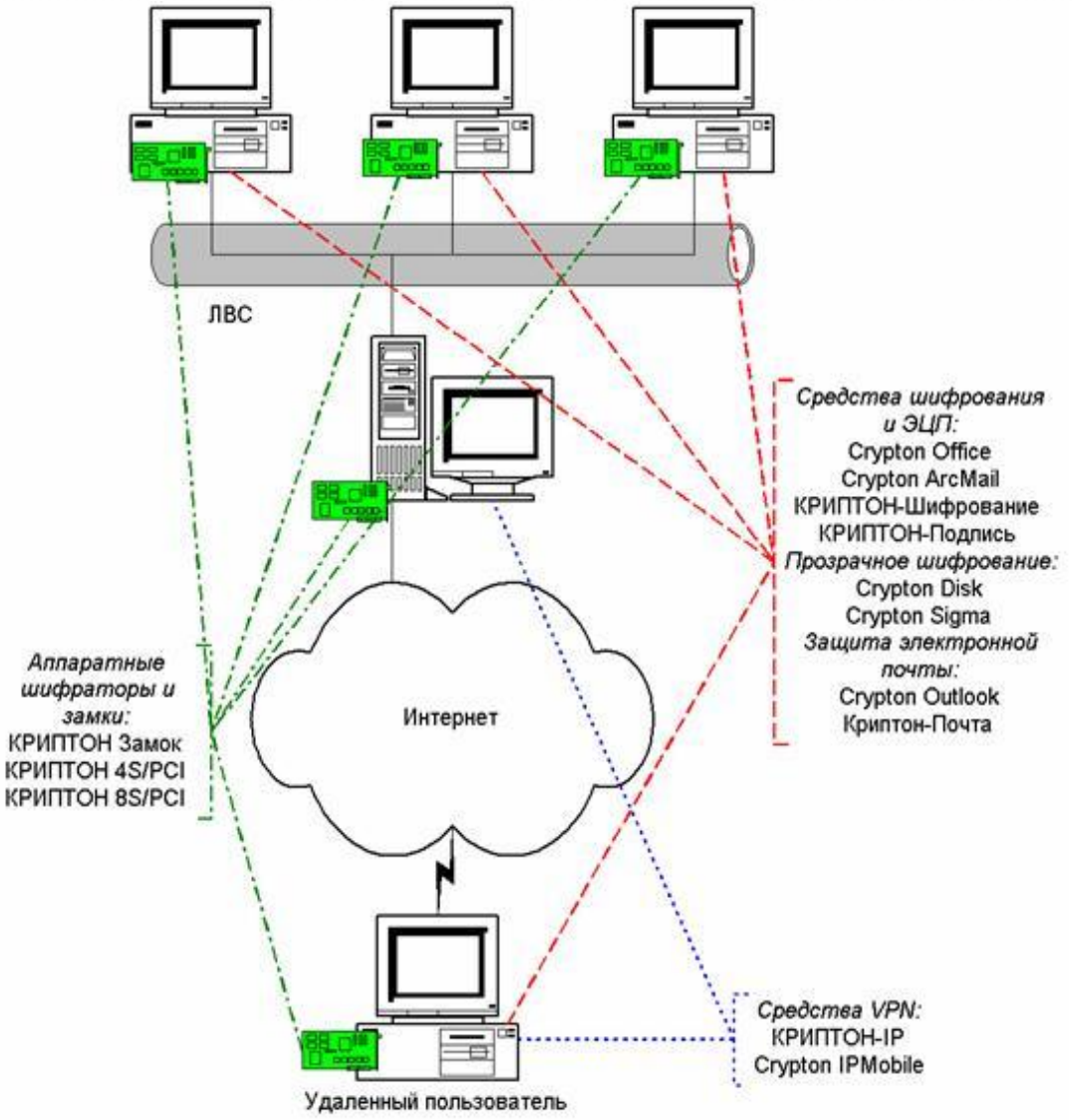
По аналогии с VPN-агентами существуют и персональные межсетевые экраны, защищающие только компьютер, на котором они установлены.

Межсетевые экраны также располагаются на периметре защищаемых сетей и фильтруют сетевой трафик согласно настроенной политике безопасности.

Комплексная защита

Электронный замок может быть разработан на базе аппаратного шифратора. В этом случае получается одно устройство, выполняющее функции шифрования, генерации случайных чисел и защиты от НСД. Такой шифратор способен быть центром безопасности всего компьютера, на его базе можно построить полнофункциональную систему криптографической защиты данных, обеспечивающую, например, следующие возможности:

- Защита компьютера от физического доступа.
- Защита компьютера от НСД по сети и организация VPN.
- Шифрование файлов по требованию.
- Автоматическое шифрование логических дисков компьютера.
- Вычисление/проверка ЭЦП.
- Защита сообщений электронной почты.



Благодарю за внимание!