Проблема несанкционированного доступа

Составил ученик МАОУ «СОШ №54»
г.Новоуральска
Виталий Гайнанов

Несанкционированный доступ (НСД)

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

Действия программы:

- Читать и/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.

Защита компьютеров от НСД

Защита компьютеров от НСД является одной из основных проблем защиты информации, поэтому в большинство операционных систем и популярных пакетов программ встроены различные подсистемы защиты от НСД.

Например, выполнение аутентификации в пользователей при входе в операционные системы семейства Windows. Однако, не вызывает сомнений тот факт, что для серьезной защиты от НСД встроенных средств операционных систем недостаточно.

К сожалению, реализация подсистем защиты большинства операционных систем достаточно часто вызывает нарекания из-за регулярно обнаруживаемых уязвимостей, позволяющих получить доступ к защищаемым объектам в обход правил разграничения доступа. Выпускаемые же производителями программного обеспечения пакеты обновлений и исправлений объективно несколько отстают от информации об обнаруживаемых уязвимостях.

Поэтому в дополнение к стандартным средствам защиты необходимо использование специальных средств ограничения или разграничения доступа. Данные средства можно разделить на две категории:

- **Средства ограничения физического доступа.**
- **Средства защиты от несанкционированного доступа по сети.**

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». Теоретически, любое программное средство контроля доступа может подвергнуться воздействию злоумышленника с целью искажения алгоритма работы такого средства и последующего получения доступа к системе.

Средства защиты от НСД по сети

Наиболее действенными методами защиты от несанкционированного доступа по компьютерным сетям являются виртуальные частные сети (VPN – Virtual Private Network) и межсетевое экранирование.

Виртуальные частные сети

Виртуальные частные сети обеспечивают автоматическую защиту целостности и конфиденциальности сообщений, передаваемых через различные сети общего пользования, прежде всего, через Интернет. Фактически, VPN – это совокупность сетей, на внешнем периметре которых установлены VPN-агенты. VPN-агент – это программа (или программно-аппаратный комплекс), собственно обеспечивающая защиту передаваемой информации путем выполнения описанных ниже операций. Перед отправкой в сеть любого IP-пакета VPN-агент производит следующее:

Перед отправкой в сеть любого IP-пакета VPN-агент производит следующее:

- Из заголовка IP-пакета выделяется информация о его адресате. Согласно этой информации на основе политики безопасности данного VPN-агента выбираются алгоритмы защиты и криптографические ключи, с помощью которых будет защищен данный пакет. В том случае, если политикой безопасности VPN-агента не предусмотрена отправка IP-пакета данному адресату или IP-пакета с данными характеристиками, отправка IP-пакета блокируется.

Перед отправкой в сеть любого IP-пакета VPN-агент производит следующее:

- С помощью выбранного алгоритма защиты целостности формируется и добавляется в IP-пакет электронная цифровая подпись (ЭЦП), имитоприставка или аналогичная контрольная сумма.
- С помощью выбранного алгоритма шифрования производится зашифрование IP-пакета.

Перед отправкой в сеть любого IP-пакета VPN-агент производит следующее:

- С помощью установленного алгоритма инкапсуляции пакетов зашифрованный IP-пакет помещается в готовый для передачи IP-пакет, заголовок которого вместо исходной информации об адресате и отправителе содержит соответственно информацию о VPN-агенте адресата и VPN-агенте отправителя. Т. е. выполняется трансляция сетевых адресов.

Перед отправкой в сеть любого IP-пакета VPN-агент производит следующее:

- Пакет отправляется VPN-агенту адресата. При необходимости, производится его разбиение и поочередная отправка результирующих пакетов.
- Из заголовка IP-пакета выделяется информация о его отправителе. В том случае, если отправитель не входит в число разрешенных (согласно политике безопасности) или неизвестен (например, при приеме пакета с намеренно или случайно поврежденным заголовком), пакет не обрабатывается и отбрасывается.

Перед отправкой в сеть любого IP-пакета VPN-агент производит следующее:

- Согласно политике безопасности выбираются алгоритмы защиты данного пакета и ключи, с помощью которых будет выполнено расшифрование пакета и проверка его целостности.
- Выделяется информационная (инкапсулированная) часть пакета и производится ее расшифрование.

Перед отправкой в сеть любого IP-пакета VPN-агент производит следующее:

- Производится контроль целостности пакета на основе выбранного алгоритма. В случае обнаружения нарушения целостности пакет отбрасывается.
- Пакет отправляется адресату (по внутренней сети) согласно информации, находящейся в его оригинальном заголовке.

Основное правило построения VPN

Основное правило построения VPN – связь между защищенной ЛВС и открытой сетью должна осуществляться только через VPN-агенты. Категорически не должно быть каких-либо способов связи, минующих защитный барьер в виде VPN-агента.

Т.е. должен быть определен защищаемый периметр, связь с которым может осуществляться только через соответствующее средство защиты.

Политика безопасности

Политика безопасности является набором правил, согласно которым устанавливаются защищенные каналы связи между абонентами VPN. Такие каналы обычно называют *туннелями*, аналогия с которыми просматривается в следующем:

- Вся передаваемая в рамках одного туннеля информация защищена как от несанкционированного просмотра, так и от модификации.
- Инкапсуляция IP-пакетов позволяет добиться сокрытия топологии внутренней ЛВС: из Интернет обмен информации между двумя защищенными ЛВС виден как обмен информацией только между их VPN-агентами, поскольку все внутренние IP-адреса в передаваемых через Интернет IP-пакетах в этом случае не фигурируют.

Политика безопасности

Правила создания туннелей формируются в зависимости от различных характеристик IP-пакетов, например, основной при построении большинства VPN протокол IPSec (Security Architecture for IP) устанавливает следующий набор входных данных, по которым выбираются параметры туннелирования и принимается решение при фильтрации конкретного IP-пакета:

- IP-адрес источника. Это может быть не только одиночный IP-адрес, но и адрес подсети или диапазон адресов.
- IP-адрес назначения. Также может быть диапазон адресов, указываемый явно, с помощью маски подсети или шаблона.
- Идентификатор пользователя (отправителя или получателя).
- Протокол транспортного уровня (TCP/UDP).
- Номер порта, с которого или на который отправлен пакет.

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:

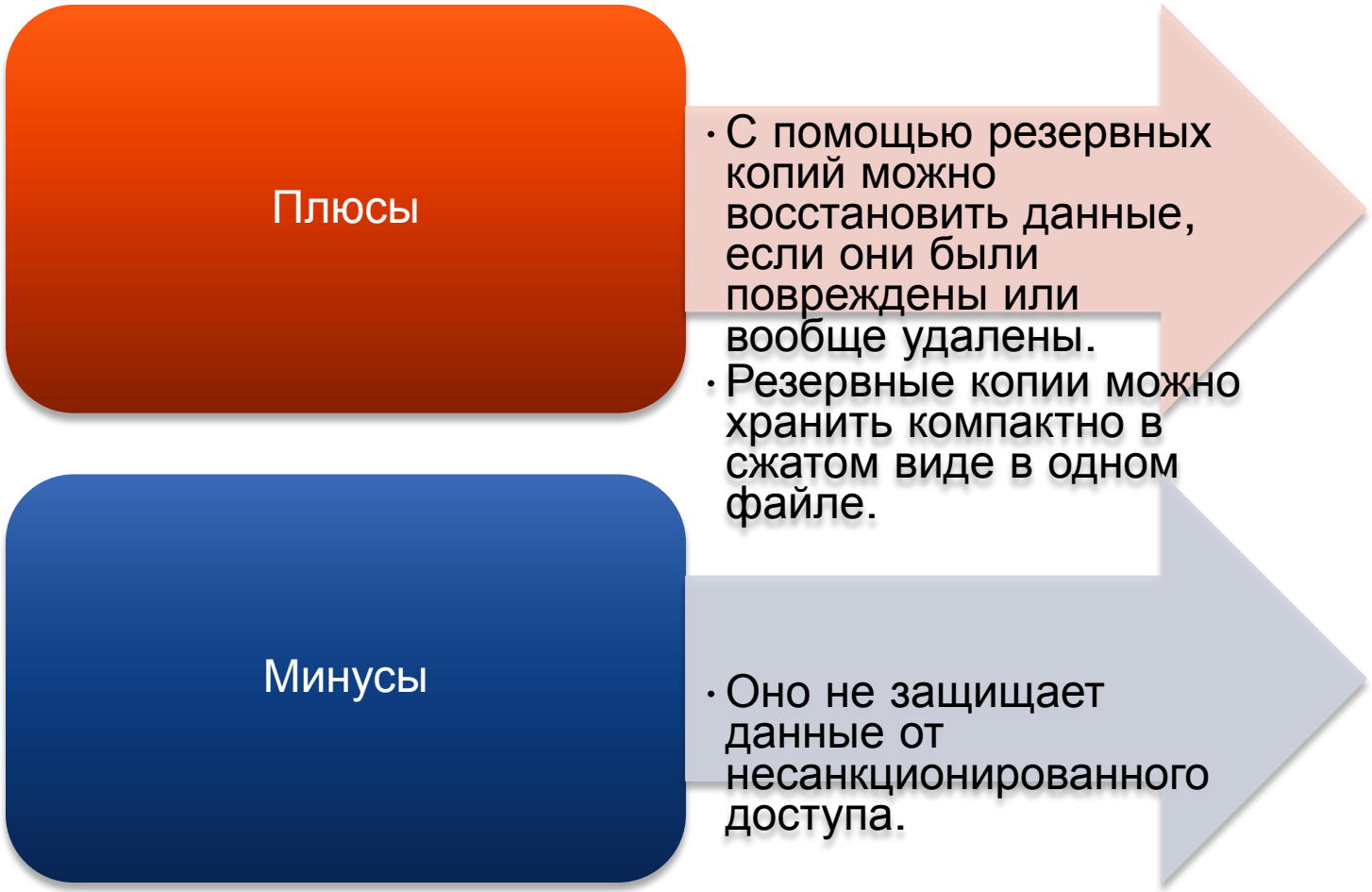
- Защита компьютера от физического доступа.
- Защита компьютера от НСД по сети и организация VPN.
- Шифрование файлов по требованию.
- Автоматическое шифрование логических дисков компьютера.
- Вычисление/проверка ЭЦП.
- Защита сообщений электронной почты.

Методы защиты информации

Итак, пусть у Вас на компьютере есть очень личная информация, доступ к которой хотите иметь только Вы.

Прежде чем рассматривать способы защиты информации от несанкционированного доступа, опишу вкратце стандартные рекомендации. Прежде всего, рекомендуется время от времени делать бэкап (резервное копирование) нужных Вам данных. Для этого можно использовать встроенную программу для резервного копирования от Microsoft. Или можно использовать программы сторонних производителей для резервного копирования, такие как Norton Ghost.

Резервное копирование



Если же для нужных Вам данных не было сделано резервных копий, и они были удалены, то есть вероятность, что их можно восстановить. Для этого существуют специальные Программы. Для общей защиты компьютерной безопасности обязательно надо иметь на компьютере хороший антивирус, файервол и программы защиты от Ad/Spyware и регулярно устанавливать заплатки для Вашей операционной системы.

Способы защиты от несанкционированного доступа

- Запись и хранение важной информации на сменных носителях (дискеты, CD, DVD)

Плюсы:

- Доступ к этой информации будете иметь только Вы (если, конечно, не допускать, чтобы эти сменные носители попали в чужие руки)

Минусы:

- Сменные носители могут быть повреждены и можно потерять информацию.
- Шифрование важных данных.

Рассмотрим два существующих способа шифрования: криптография и стеганография.

Криптография

Криптография – это кодирование информации с помощью какого-либо шифра. т.е превращение информации в нечто нераспознаваемое. В этом случае для получения доступа к информации нужен пароль, даже если сам способ шифрования известен и есть доступ к зашифрованной информации.

Стеганография

Стеганография – это скрытие самого факта наличия информации. Существуют алгоритмы, которые прячут информацию в файлы-контейнеры формата bmp, wav и некоторых других.

Картинки и аудио файлы хорошо подходят для этих целей, т.к. они достаточно велики и в них можно спрятать определенное кол-во информации. Файл-контейнер (картинка или звук со встроенными данными) практически не отличается от оригинала ни по размеру, ни по внешнему виду/звучанию.

Презентация подготовлена для конкурса «Интернешка» http://interneshka.org/