ЗАЩИТА ИНФОРМАЦИИ

Цель: Показать, для чего необходима защита информации и как защитить её.

Задачи: Ввести понятия: неограниченный доступ, программы-шпионы, защита информации;
рассмотреть различные способы защиты информации.

Преподаватель ФГОУ СПО ПЛТТ

Максименкова Н.В.

Защита данных

- ПК и ПО, установленное на нём, является дорогостоящим средством работы с информацией. Однако данные, которые создаются с их помощью, всё-таки являются более ценными.
- Воссоздание данных может быть невозможным.
- В лучшем случае, это дорогой и долгий процесс, потребуется возможно переустановка программ и их настройка, программного обеспечения.
- Поэтому, если защита компьютера от его потери или кражи, а также вирусов важна, то сохранение системных конфигураций и данных – жизненно важно.

УГРОЗЫ БЕЗОПАСНОСТИ

- Некомпетентность пользователей (проблема – слабые пароли и пренебрежение требованиям безопасности)
- Хакеры в Интернете и увеличение числа вирусных и «шпионских» программ типа «троянского коня»

Несанкционированный доступ

Несанкционированный доступ к информации — доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных Несанкционированный доступ к информации — доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных Несанкционированный доступ к информации — доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых Несанкционированный доступ к информации — доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификацииНесанкционированный доступ к информации — доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д.

Причины несанкционированного доступа к информации

- ошибки конфигурации (прав доступа, ограничений на массовость запросов к базам данных)
- слабая защищённость средств авторизации (хищение паролей, смарт-карт, физический доступ к плохоохраняемому оборудованию, доступ к незаблокированным рабочим местам сотрудников в отсутствие сотрудников)
- ошибки в программном обеспечении
- злоупотребление служебными полномочиями (воровство резервных копий, копирование информации на внешние носители при праве доступа к информации)
- прослушивание каналов связи при использовании незащищённых соединений внутри ЛВС
- использование клавиатурных шпионов, вирусов и троянов на компьютерах сотрудников для имперсонализации.

Несанкционированно устанавливаемые мониторинговые программы, то есть программы-шпионы

Их применение позволяет злоумышленнику:

- несанкционированно перехватывать чужую информацию;
- осуществлять экономический шпионаж;
- осуществлять политический шпионаж;
- получить несанкционированный доступ к системам "банк-клиент";
- получить несанкционированный доступ к системам криптографии пользователя персонального компьютера - открытым и закрытым ключам, парольным фразам;
- получить несанкционированный доступ к авторизационным данным кредитных карточек;
- и так далее.

Продукты-шпионы представляют серьезную опасность защите отдельных и соединенных в сеть компьютерных систем.

Одна из наиболее опасных особенностей всех программ-шпионов и аппаратных устройств-кейлоггеров - регистрация нажатий клавиш, сделанных пользователем, с целью контроля компьютерной активности. Когда пользователь набирает на клавиатуре пароль и данные своей кредитной карточки, возможно, в этот момент записывается каждое нажатие клавиши. Кроме этого, современные программы-шпионы позволяют захватывать текст из окон приложений и делать снимки (скриншоты) экрана и отдельных окон. Другими словами, программа-шпион может перехватить текст из документа, даже если пользователь его не набирал с клавиатуры, а просто открыл и просмотрел файл.

Приемы несанкционированного доступа к информации

- **За дураком** - физическое проникновение в производственные помещения - злоумышленник ожидает у закрытого помещения, держа в руках предметы связанные с работой на компьютерной технике (элементы маскировки), пока не появится кто-либо, имеющий легальный доступ в него, затем остается только войти внутрь вместе с ним или попросить его помочь занести якобы необходимые для работы на компьютере предметы. Другой вариант - электронное проникновение в СВТ - подключение дополнительного компьютерного терминала к каналам связи с использованием шлейфа "шнурка" в тот момент времени, когда законный пользователь кратковременно покидает свое рабочее место, оставляя свой терминал или персональный компьютер в активном режиме.
- **За хвост** - злоумышленник подключается к линии связи законного пользователя и терпеливо дожидается сигнала, обозначающего конец работы, перехватывает его на себя, а потом, когда законный пользователь заканчивает активный режим, осуществляет доступ к системе. Подобными свойствами обладают телефонные аппараты с функцией удержания номера, вызываемого абонентом.
- **Компьютерный абордаж** - злоумышленник вручную или с использованием автоматической программы подбирает код (пароль) доступа к системе с использованием обычного телефонного аппарата.

Приемы несанкционированного доступа к информации

- **Неспешный выбор** - злоумышленник изучает и исследует систему защиты от несанкционированного доступа, используемую в компьютерной системе, ее слабые места, выявляет участки, имеющие ошибки или неудачную логику программного строения, разрывы программы (брешь, люк) и вводит дополнительные команды, разрешающие доступ.
- **Маскарад** - злоумышленник проникает в компьютерную систему, выдавая себя за законного пользователя с применением его кодов (паролей) и других идентифицирующих шифров.
- **Мистификация** - злоумышленник создает условия, когда законный пользователь банковской системы осуществляет связь с нелегальным терминалом, будучи абсолютно уверенным в том, что он работает с нужным ему законным абонентом. Формируя правдоподобные ответы на запросы законного пользователя и поддерживая его заблуждения некоторое время, злоумышленник добывает коды (пароли) доступа или отклик на пароль.
- **Аварийный** - злоумышленник создает условия для возникновения сбоев или других отклонений в работе СВТ банковской компьютерной системы. При этом включается особая программа, позволяющая в аварийном режиме получать доступ к наиболее ценным данным. В этом режиме возможно “отключение” всех имеющихся в банковской компьютерной системе средств защиты информации, что облегчает доступ к ним злоумышленника.

Под СВТ понимается совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Программные кейлоггеры, предназначенные для контроля информации, вводимой пользователем персонального компьютера

Программные кейлоггеры (keyloggers, key loggers, keystroke loggers, key recorders, key trappers, key capture programs и множество других вариантов названия) принадлежат к той группе программных продуктов, которые осуществляют контроль над деятельностью пользователя персонального компьютера.

Первоначально программные продукты этого типа предназначались исключительно для записи информации о нажатиях клавиш клавиатуры, в том числе и системных, в специализированный журнал регистрации (Log-файл), который впоследствии изучался человеком, уставившим эту программу. Log-файл может отправляться по сети на сетевой диск, ftp сервер в сети Интернет, по Email и другие.

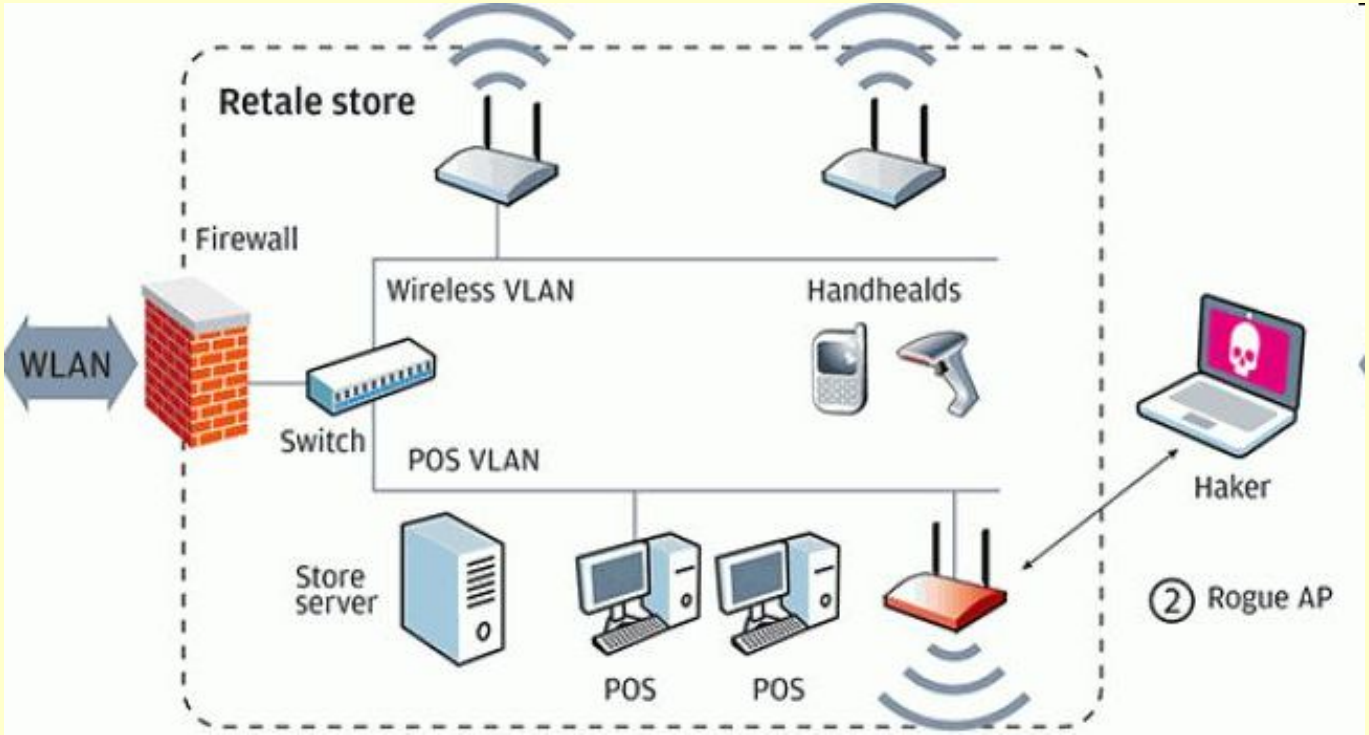
В последнее время программные продукты, имеющие данное название, выполняют много дополнительных функций - это перехват информации из окон, перехват кликов мыши, "фотографирование" снимков экрана и активных окон, ведение учета всех полученных и отправленных E-mail, мониторинг файловой активности, мониторинг системного реестра, мониторинг очереди заданий, отправленных на принтер, перехват звука с микрофона и видео-изображения с веб-камеры, подключенных к компьютеру и другие.

Аппаратные кейлоггеры, предназначенные для контроля информации, вводимой пользователем персонального компьютера с клавиатуры

Аппаратные кейлоггеры (keystroke recording device, hardware keylogger и пр.) представляют собой миниатюрные приспособления, которые могут быть прикреплены между клавиатурой и компьютером или встроены в саму клавиатуру. Они регистрируют все нажатия клавиш, сделанные на клавиатуре. Процесс регистрации абсолютно невидим для конечного пользователя. Аппаратные кейлоггеры не требуют установки какой-либо программы на компьютере интересующего объекта, чтобы успешно перехватывать все нажатия клавиш. Такое устройство может быть тайно прикреплен к ПК объекта кем угодно - коллегой, уборщицей, посетителем и т.д.. Когда аппаратный кейлоггер прикрепляется, абсолютно не имеет значения, в каком состоянии находится компьютер - включенном или выключенном.

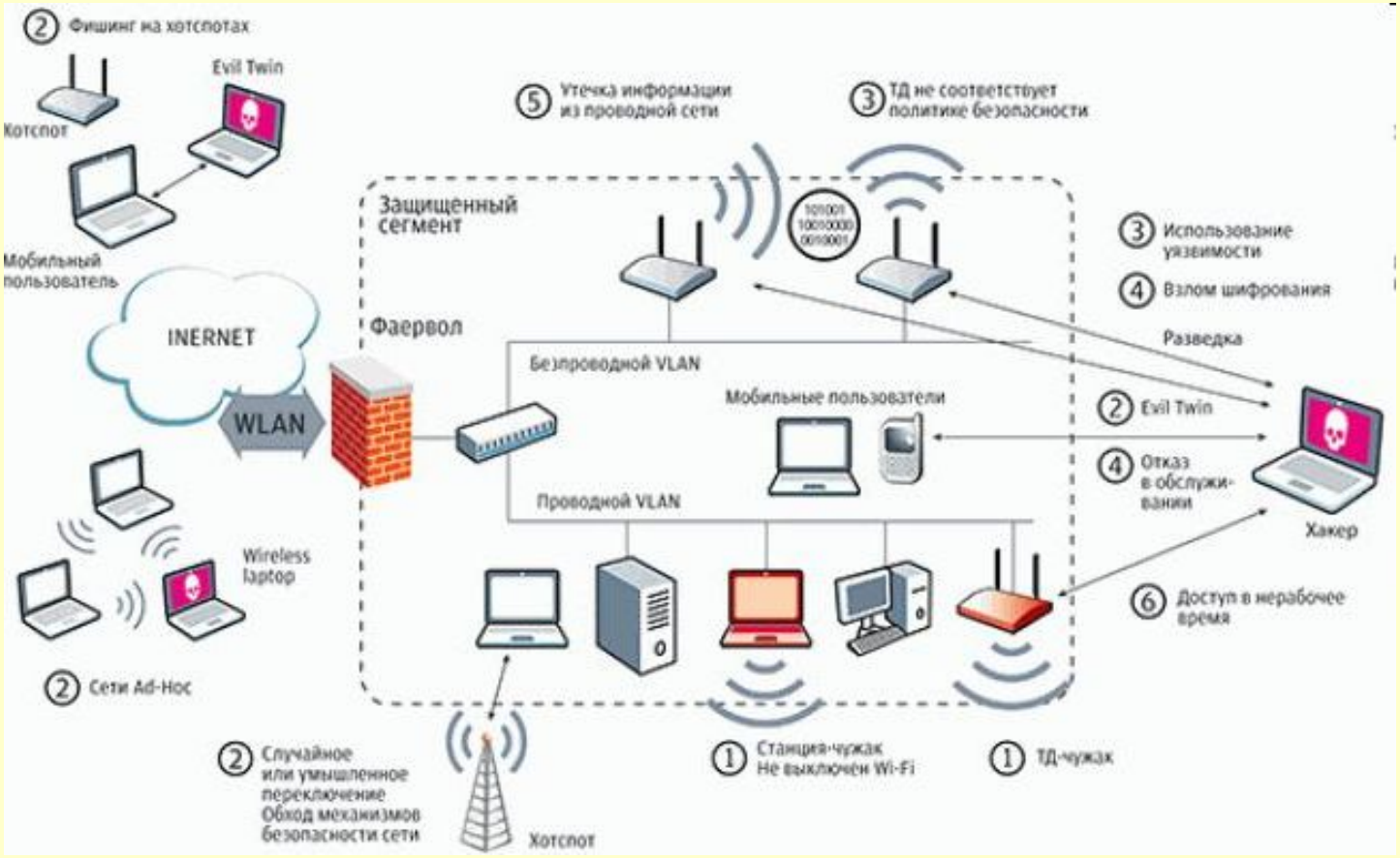
Беспроводным угрозам подвержены те, кто использует или нет Wi-Fi

Как и множество других инновационных технологий, беспроводные сети сулят не только новые выгоды, но и риски. Бум Wi-Fi породил целое поколение хакеров, специализирующихся на изобретении новых способов взлома корпоративных инфраструктур и атак пользователей.



Распространенность беспроводных технологий в наше время ставит под угрозу и те сети, где они уже применяются, и те, где никогда не должны использоваться.

Традиционные средства защиты бессильны против принципиально новых классов беспроводных угроз (см.рис.). При этом ситуация осложняется тем, что необходимо защищать также и своих пользователей (которые могут находиться и вдали от офиса), не нарушая при этом функционирования сетей соседей, каким бы подозрительным оно не выглядело.



Основные составляющие информационной безопасности

- Доступность информации
- Целостность
- Конфиденциальность

Классификация средств защиты

Уровень 1. Законодательный

Уровень 2. Административный и процедурный

Уровень 3. Программно-технический

Законодательный уровень

Глава 28 УК РФ. Преступления в сфере компьютерной информации.

Статья 272. Неправомерный доступ к компьютерной информации.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Кроме этого, принят Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, -

   наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.
2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, -

   наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами -

   наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, -

   наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, -

   наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

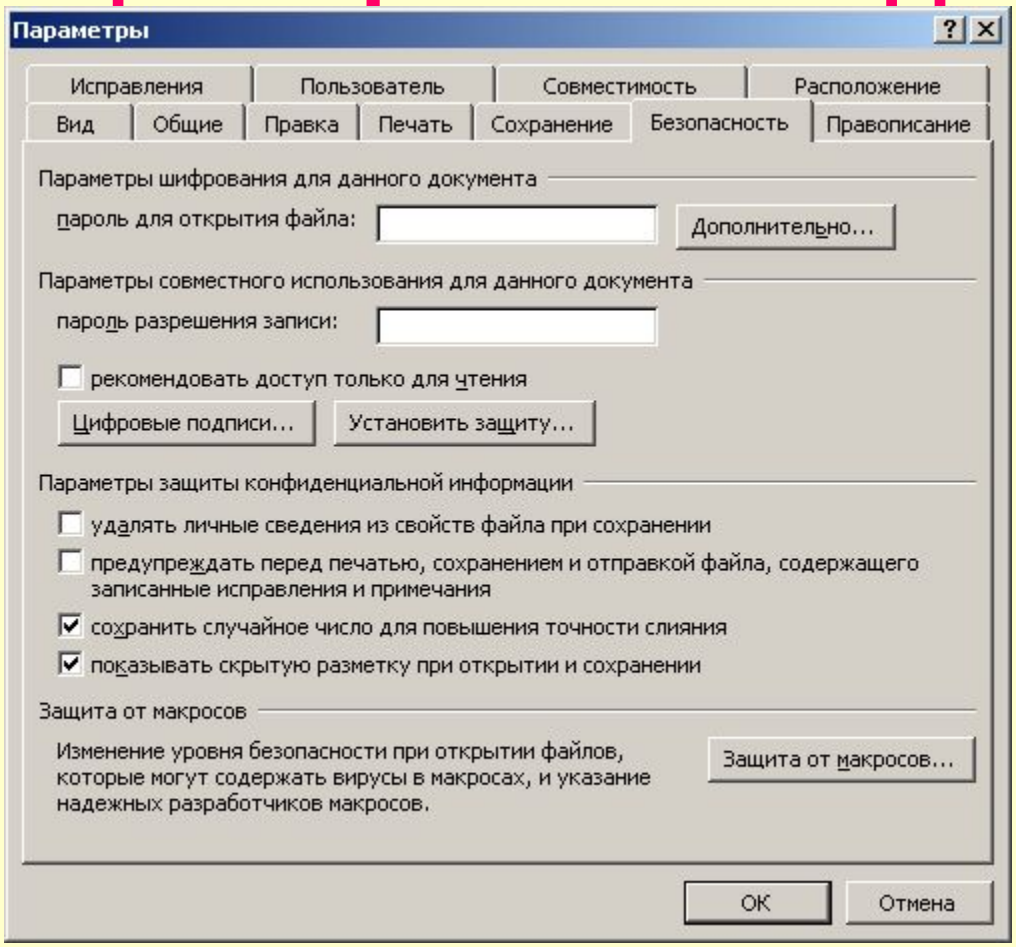
2. То же деяние, повлекшее по неосторожности тяжкие последствия, -

   наказывается лишением свободы на срок до четырех лет.

Методы защиты компьютера

- Защита жёсткого диска (создание аварийной загрузочной дискеты)
- Резервное копирование данных
- Дефрагментация жёсткого диска
- Установка паролей на документ

Защита файла от несанкционированного доступа



Диалоговое окно Параметры с открытой вкладкой Безопасность

Система паролей

- На рабочем компьютере, домашнем ПК или в сети используют множество мер предосторожностей. Одной из таких мер является система паролей.
- Простейший способ предотвратить чтение файлов – использовать защищённую паролем заставку. Для любопытных это будет достаточным барьером.
- Чтобы установить защищённую паролем заставку, необходимо щёлкнуть по Рабочему столу правой кнопкой мыши и открыть окно «Свойства экрана», открыть вкладку «Заставка» и выбрать заставку из списка.
- Отметьте опцию «Пароль» и щёлкните по кнопке «Изменить». Введите пароль ещё раз в установленном поле для его подтверждения.

Пароль для файла

- Чтобы определить пароль для файла MS Word, выберите в линейке меню режим «Файл», «Сохранить» или «Сохранить как». Напечатайте имя файла и щёлкните по кнопке «Инструменты» и выберите режим «Параметры».
- Введите пароль в окне «Пароль» для открытия файла, если необходимо ограничить доступ. Напечатать пароль в окне «Пароль» разрешения записи, если необходимо позволить людям открывать, но не изменять файл. По щелчку «Ок» подтвердите пароль.

Защита файла

- Следующий уровень защиты – это защита самих файлов паролем. Пароль можно установить в диалоговом окне «Сохранить». Возможности паролей различаются, но всегда есть возможность предотвратить загрузку файла без пароля. Также можно установить урони ограниченного доступа, такие, как читать, но не изменять файл.
- Чтобы не позволить кому-либо обойти пароль открытия файла с помощью другой программы, когда устанавливается пароль, можно перемешать структуру файла так, что если эксперт откроет его в другом редакторе, содержимое будет непонятным.

Выполняемый файл

- Это программа, которая имеет специальное значение в терминах шифровки файлов. Данную программу можно запустить на любом ПК, вне зависимости от установленных на нем программ. При этом файл шифруется как выполняемый, получателю не нужно иметь экземпляр шифрующей программы.
- Получатель запустит программу и введёт пароль, который должен быть передан для расшифровки внутри сообщения.

Ограничение доступа

- Чтобы ограничить доступ к папкам сети, используйте «Мой компьютер», чтобы выбрать папку для защиты. В меню «Файл» щелкните по «Свойства» и выберите «Доступ». Введите пароль, который люди должны иметь для того, чтобы читать или писать в папку.
- Гораздо сложнее защитить систему, которой пользуются дети. Они могут неосторожно запустить программы, которыми не умеют пользоваться, и случайно удалить важные файлы.
- Об одноразовом пароле можно подробно узнать в статье М.Давлетханова «Методы реализации OTP».
- Также много интересного пишет Шеннон Го в документе «Открытые системы».

Методы противодействия программам-шпионам

Для обнаружения и удаления мониторинговых программных продуктов, которые могут быть установлены без ведома пользователя ПК, в настоящее время используются программы различных типов, обеспечивающие более или менее эффективную защиту исключительно только против ИЗВЕСТНЫХ программ-шпионов с помощью сигнатурного анализа. Для эффективной работы программ данного типа необходимо получить образец программы-шпиона, выделить из нее сигнатуру и включить данную сигнатуру в свою базу. При обновлении сигнатурной базы пользователи персонального компьютера получают возможность бороться с данным вариантом программы-шпиона. По данному принципу работают многие известные фирмы производители антивирусного программного обеспечения.

Что же может противопоставить пользователь персонального компьютера программам-шпионам?

Решение данной проблемы возможно только в использовании комплекса программных продуктов:

- Программный продукт N1 - это продукт, который использует эвристические механизмы защиты против программ-шпионов, созданные специалистами, имеющими больший опыт борьбы с программами-шпионами. Он оказывает защиту непрерывно и не использует никакие сигнатурные базы.
- Программный продукт N2 - это Антивирусный программный продукт, использующий постоянно обновляемые сигнатурные базы.
- Программный продукт N3 - это персональный Firewall, контролирующий выход в сеть Интернет с персонального компьютера на основании политик, которые устанавливает сам пользователь.

Такая последовательность выбрана неспроста.

Методы противодействия аппаратным кейлоггерам

Никакие программные продукты не в состоянии определить наличие установленных аппаратных устройств, которые обеспечивают перехват нажатий клавиатуры пользователем персонального компьютера. Сегодня существует только два метода противодействия аппаратным кейлоггерам при работе на стандартном персональном компьютере:

- физический поиск и устранение аппаратного кейлоггера;
- использование виртуальных клавиатур для ввода особо важной информации (логины, пароли, коды доступа, PIN коды кредитных карт и т.д.).

ШИФРОВАНИЕ

Проблема защиты информации путем её преобразования, исключающего её прочтение посторонним лицом, волновала человеческий ум с давних времен.

История криптологии (kryptos — тайный, logos — наука) — ровесница истории человеческого языка. Более того, письменность сама по себе была вначале криптографической системой, так как в древних обществах ею владели только избранные. Священные книги Древнего Египта, Древней Индии тому примеры.

Криптология разделяется на два направления — криптографию и криптоанализ. Цели этих направлений прямо противоположны. Криптография занимается поиском и исследованием методов шифрования информации. Она даёт возможность преобразовывать информацию таким образом, что её прочтение (восстановление) возможно только при знании ключа. Сфера интересов криптоанализа — исследование возможностей расшифровки информации без знания ключей.

КЛЮЧ

Ключ — информация, необходимая для беспрепятственного шифрования и дешифрования текста.

Первые криптографические системы встречаются уже в начале нашей эры.

Так, Цезарь в своей переписке уже использовал шифр, получивший его имя. Бурное развитие криптографические системы получили в годы первой и второй мировых войн. Появление вычислительной техники ускорило разработку и совершенствование криптографических методов.

О шифровании и защите информации в сетях читайте здесь.

Полезные советы

- Установите пароли на BIOS и экранную заставку
- Исключите доступ посторонних лиц к вашему компьютеру
- Создайте аварийную загрузочную дискету
- Систематически делайте резервное копирование данных
- Регулярно очищайте Корзину с удаленными файлами
- Устанавливайте пароли на файлы с важной информацией
- При установке пароля не используйте ваше имя, фамилию, телефон
- Проводите архивацию файлов
- После удаления большого количества файлов производите дефрагментацию жёсткого диска

Ресурсы

- http://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D1%81%D0%B0%D0%BD%D0%BA%D1%86%D0%B8%D0%BE%D0%BD%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF – Несанкционированный доступ
- http://www.bezpeka.com/ru/lib/sec/art382 - Шпионские программы
- Жукова Е.Л., Бурда Е.Г. Информатика: Учебное пособие. – М.: Издательско-торговая корпорация «Дашков и К^0»; Ростов н/Д: Наука-Пресс, 2007, с.100-102.
- http://www.infobez.com/article.asp?ob_no=3922 Методы реализации OTP
- http://pmi.ulstu.ru/new_project/protect/inter.htm Основы защиты информации
- http://www.osp.ru/text/print/302/132783.html Открытые системы