Защита информации и информационная безопасность при внедрении электронного документооборота. ЭЦП

ПОНЯТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УГРОЗА

Угроза - это потенциальная возможность определенным образом нарушить информационную безопасность

Попытка реализации угрозы называется атакой, а тот, кто предпринимает такую попытку - злоумышленником

Потенциальные злоумышленники называются источниками угрозы

УГРОЗЫ МОЖНО КЛАССИФИЦИРОВАТЬ ПО НЕСКОЛЬКИМ КРИТЕРИЯМ:

- по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура)
- по способу осуществления (случайные/преднамеренные, действия природного/техногенного характера)
- по расположению источника угроз (внутри/вне рассматриваемой ИС)

ВИДЫ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ОБЩЕГО ПЛАНА:

- организация утечки информации
- угроза искажений (дезинформация, подделка, повтор)
- угроза уничтожения информации
- угроза интеллектуальной собственности (незаконное копирование, воспроизведение)
- помехи функционирования информационных систем
- телекоммуникации (отказ от получения, отправления информации)

ЗАЩИТА ИНФОРМАЦИИ

Защита информации	это комплекс мероприятий, направленных на обеспечение информационной безопасности
Средства защиты информации	это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации

СТАНДАРТИЗОВАННОЕ ОПРЕДЕЛЕНИЕ

Информационная безопасность — защита конфиденциальности, целостности и доступности информации

- Конфиденциальность: обеспечение доступа к информации только авторизованным пользователям
- Целостность: обеспечение достоверности и полноты информации и методов её обработки
- Доступность: обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости

ОРГАНЫ, ОБЕСПЕЧИВАЮЩИЕ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

ГОСУДАРСТВЕННЫЕ ОРГАНЫ РФ, КОНТРОЛИРУЮЩИЕ ДЕЯТЕЛЬНОСТЬ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

- Комитет Государственной думы по безопасности
- Совет безопасности России
- Федеральная служба по техническому и экспортному контролю (ФСТЭК России)
- Федеральная служба безопасности Российской Федерации (ФСБ России)
- Министерство внутренних дел Российской Федерации (МВД России)
- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)

СЛУЖБЫ, ОРГАНИЗУЮЩИЕ ЗАЩИТУ ИНФОРМАЦИИ НА УРОВНЕ ПРЕДПРИЯТИЯ

- Служба экономической безопасности
- Служба безопасности персонала (Режимный отдел)
- Отдел кадров
- Служба информационной безопасности

НОРМАТИВНЫЕ ДОКУМЕНТЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

НОРМАТИВНО-ПРАВОВЫЕ АКТЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ

- Международные договоры РФ
- Конституция РФ
- Законы федерального уровня (включая федеральные конституционные законы, кодексы)
- Указы Президента РФ
- Постановления правительства РФ
- Нормативные правовые акты федеральных министерств и ведомств
- Нормативные правовые акты субъектов РФ, органов местного самоуправления и т. д.

К НОРМАТИВНО-МЕТОДИЧЕСКИМ ДОКУМЕНТАМ ОТНОСИТСЯ

Методические документы государственных органов России:

- Доктрина информационной безопасности РФ
- Руководящие документы ФСТЭК (Гостехкомиссии России)
- Приказы ФСБ

СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Международные стандарты
- Государственные (национальные) стандарты РФ
- Рекомендации по стандартизации
- Методические указания

ПРОГРАММНО-ТЕХНИЧЕСКИЕ СПОСОБЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СРЕДСТВА ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

- Средства авторизации
- Мандатное управление доступом
- Избирательное управление доступом
- Управление доступом на основе ролей
- Журналирование

АВТОРИЗАЦИЯ

Процесс предоставления определенному лицу прав на выполнение некоторых действий

Процесс подтверждения (проверки) прав пользователей на выполнение некоторых действий

ВИДЫ АВТОРИЗАЦИИ

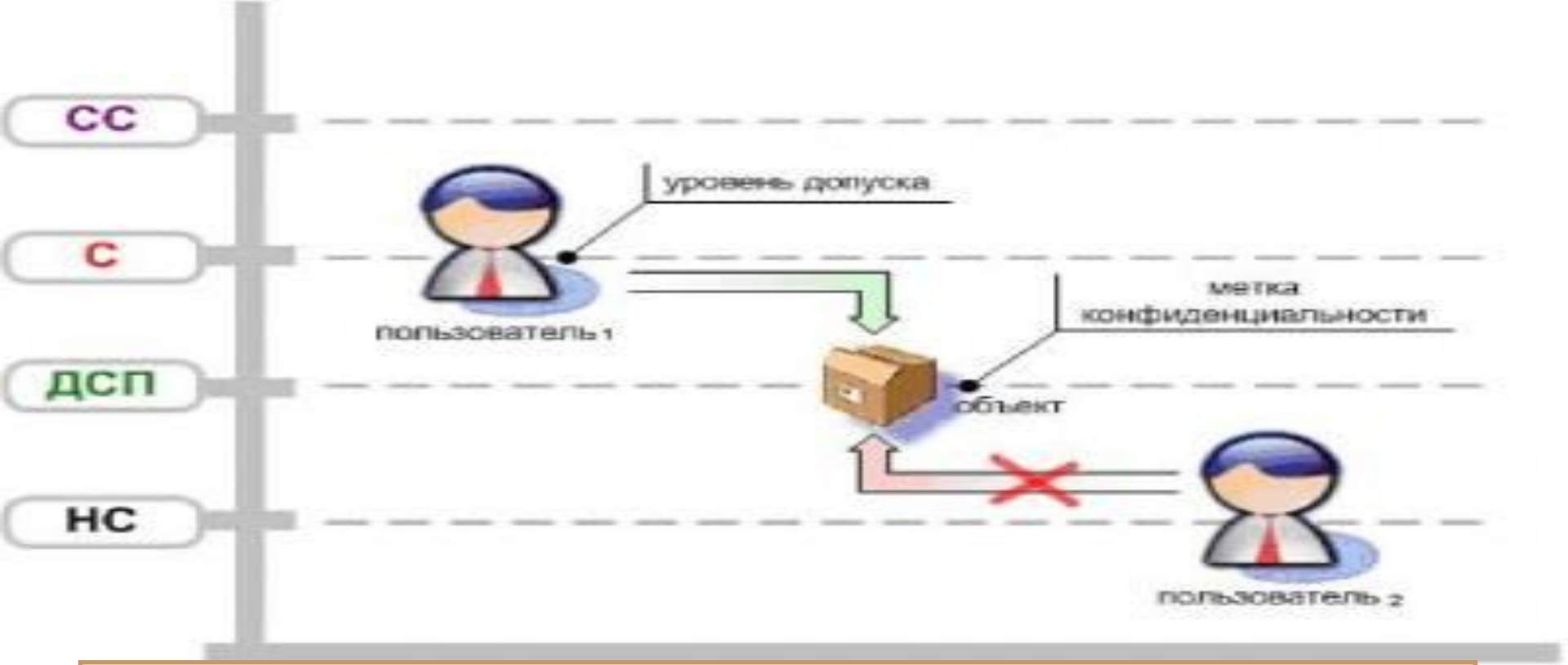
- В информационных технологиях посредством авторизации устанавливаются и реализуются права доступа к ресурсам и системам обработки данных

- В финансовой сфере авторизация проводится при использовании банковских платежных, кредитных и иных карт

МАНДАТНОЕ УПРАВЛЕНИЕ ДОСТУПОМ

Mandatory access control — разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности

Это способ, сочетающий защиту и ограничение прав, применяемый по отношению к компьютерным процессам, данным и системным устройствам и предназначенный для предотвращения их нежелательного использования



Мандатное управление доступом. СС — совершено секретно; С — секретно; ДСП — для служебного пользования; НС — не секретно.
В приведенном примере субъект «Пользователь № 2», имеющий допуск уровня «не секретно», не может получить доступ к объекту, имеющего метку «для служебного пользования». В то же время, субъект "Пользователь «№ 1» с допуском уровня «секретно», имеет право доступа к объекту с меткой «для служебного пользования».

ИЗБИРАТЕЛЬНОЕ УПРАВЛЕНИЕ ДОСТУПОМ

Discretionary access control — управление доступом субъектов к объектам на основе списков управления доступом или матрицы доступа.

Также называется Дискреционное управление доступом, Контролируемое управление доступом и Разграничительное управление доступом.

УПРАВЛЕНИЕ ДОСТУПОМ НА ОСНОВЕ РОЛЕЙ

Role Based Access Control — развитие политики избирательного управления доступом, при этом права доступа субъектов системы на объекты группируются с учетом специфики их применения, образуя роли

Формирование ролей призвано определить четкие и понятные для пользователей компьютерной системы правила разграничения доступа.

Ролевое разграничение доступа позволяет реализовать гибкие, изменяющиеся динамически в процессе функционирования компьютерной системы правила разграничения доступа

ЖУРНАЛИРОВАНИЕ

Журналирование — процесс записи информации о происходящих с каким-то объектом событиях в журнал (в файл)

Журнал это запись в хронологическом порядке операций обработки данных, которые могут быть использованы для того, чтобы воссоздать существовавшую или альтернативную версию компьютерного файла

В системах управления базами данных журнал — это записи обо всех данных, изменённых определённым процессом

КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА

Шифрование — способ преобразования открытой информации в закрытую и обратно

Применяется для хранения важной информации в ненадёжных источниках или передачи её по незащищённым каналам связи

Согласно ГОСТ 28147-89, шифрование подразделяется на процесс зашифровывания и расшифровывания

В зависимости от алгоритма преобразования данных, методы шифрования подразделяются на гарантированной или временной криптостойкости

В ЗАВИСИМОСТИ ОТ СТРУКТУРЫ ИСПОЛЬЗУЕМЫХ КЛЮЧЕЙ ПОДРАЗДЕЛЯЮТСЯ НА:

симметричное шифрование:

- посторонним лицам может быть известен алгоритм шифрования, но неизвестна небольшая порция секретной информации — ключа, одинакового для отправителя и получателя сообщения

асимметричное шифрование:

- посторонним лицам может быть известен алгоритм шифрования, и, возможно, открытый ключ, но неизвестен закрытый ключ, известный только получателю

ЭЛЕКТРОННАЯ ПОДПИСЬ

Электронная подпись (ЭП)

Реквизит электронного документа, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования ЭП и проверить принадлежность подписи владельцу сертификата ключа ЭП.

Значение реквизита получается в результате криптографического преобразования информации с использованием закрытого ключа ЭП.

О ПОДПИСИ

Любая подпись, будь-то обычная или цифровая, всегда выполняет, по крайней мере, три функции:

- первая – это удостоверение того, что подписавшийся является тем, за которого мы его принимаем (функция авторизации)
- вторая - это то, что подписавшийся не может отказаться от документа, который он подписал
- третья – подтверждение того, что отправитель подписал именно тот документ, который отправил, а не какой-либо иной

Во всех этих случаях “работает” свойство подписи, называемое аутентичность, т.е. подлинность

НАЗНАЧЕНИЕ И ПРИМЕНЕНИЕ ЭП

использование цифровой подписи позволяет осуществить:

- Контроль целостности передаваемого документа
- Защиту от изменений (подделки) документа
- Невозможность отказа от авторства
- Доказательное подтверждение авторства документа

ЭП КАК МЕТОД АУТЕНТИФИКАЦИИ

- Когда кто-то получает от вас сообщение, зашифрованное вашим частным ключом, он уверен в аутентичности послания. То есть в данном случае шифрование эквивалентно поставленной подписи.

- Таким образом, цифровая подпись или электронная подпись - это метод аутентификации отправителя или автора подписи, подтверждающий, что содержание документа не было изменено. Цифровая подпись может быть поставлена как в зашифрованном, так и в открытом послании.

АТАКА И ЕЕ РЕЗУЛЬТАТЫ

Полный взлом цифровой подписи.

- Получение закрытого ключа, что означает полный взлом алгоритма

Универсальная подделка цифровой подписи.

- Нахождение алгоритма, аналогичного алгоритму подписи, что позволяет подделывать подписи для любого электронного документа

Выборочная подделка цифровой подписи.

- Возможность подделывать подписи для документов, выбранных криптоаналитиком

Экзистенциальная подделка цифровой подписи.

- Возможность получения допустимой подписи для какого-то документа, не выбираемого криптоаналитиком

ЗАДАЧА ЗАЩИТЫ КЛЮЧЕЙ

Сертификат позволяет удостоверить заключённые в нём данные о владельце и его открытый ключ подписью какого-либо доверенного лица

Существуют системы сертификатов двух типов: централизованные и децентрализованные

В децентрализованных системах путём перекрёстного подписания сертификатов знакомых и доверенных людей каждым пользователем строится сеть доверия

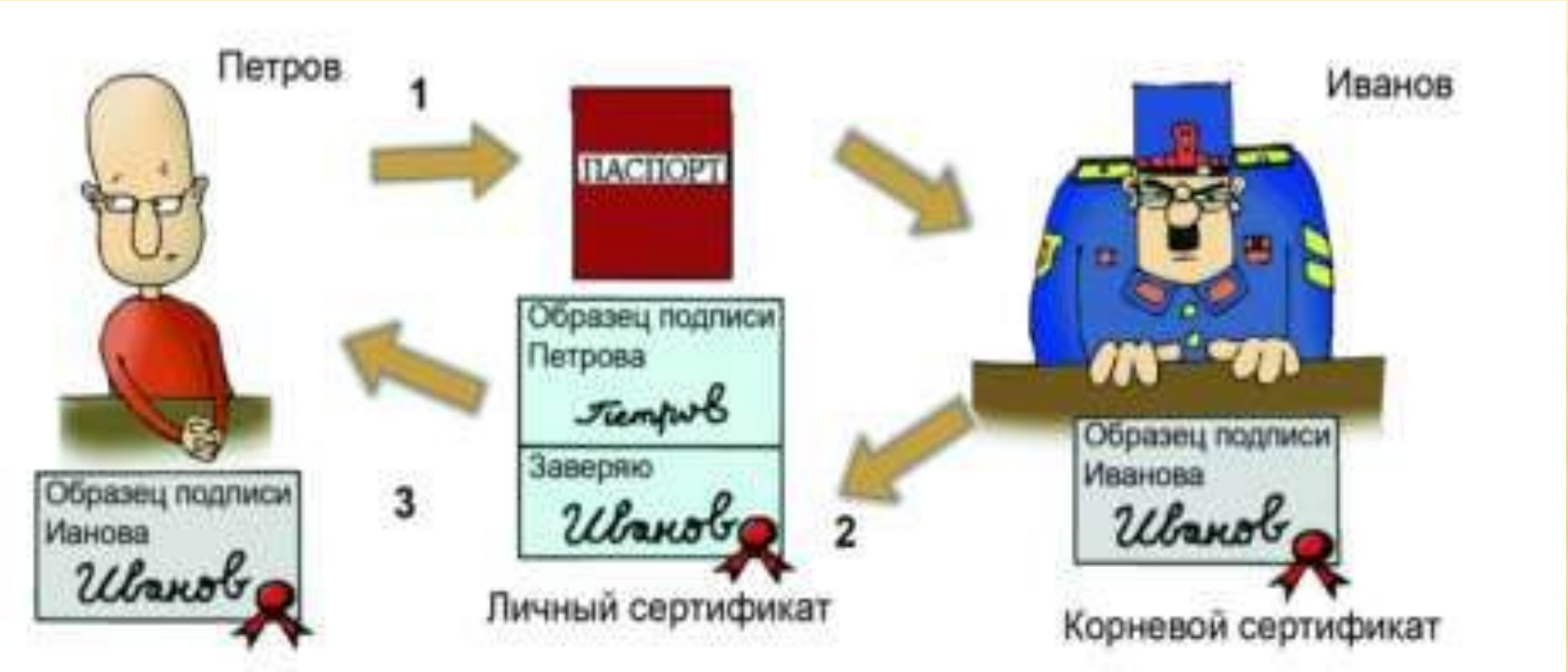
В централизованных системах сертификатов используются центры сертификации, поддерживаемые доверенными организациями

ЦЕНТРЫ СЕРТИФИКАЦИИ

- Для того чтобы определить, кто является истинным владельцем публичного ключа, нужна третья сторона, которой доверяют все корреспонденты.
- С этой задачей справляются центры сертификации CA (Certification Authority). Они выдают сертификаты - цифровые данные, подписанные цифровой подписью поручителя, подтверждающие соответствие открытого ключа и информации, идентифицирующей его владельца.
- Сертификат содержит публичный ключ, информацию о владельце ключа, название сертификационного центра, время, в течение которого сертификат действителен, и т.д. Каждая копия сертификата имеет цифровую подпись организации, выдавшей сертификат, так что

КЛАССЫ СЕРТИФИКАТОВ

- Личные сертификаты могут быть разных классов. Для получения сертификата низшего уровня требуется минимальный уровень проверки владельца публичного ключа. При выдаче сертификата высшего уровня проверяются не только личные данные владельца, но и уровень его кредитоспособности. В этом случае сертификат может выступать аналогом "кредитной карты", подтверждающей кредитоспособность при сделках в Web.
- Для получения личного сертификата пользователь обязан внести плату, которая тем больше, чем выше класс сертификата.



Изначально у всех должен храниться корневой сертификат, в котором имеется образец подписи Иванова.

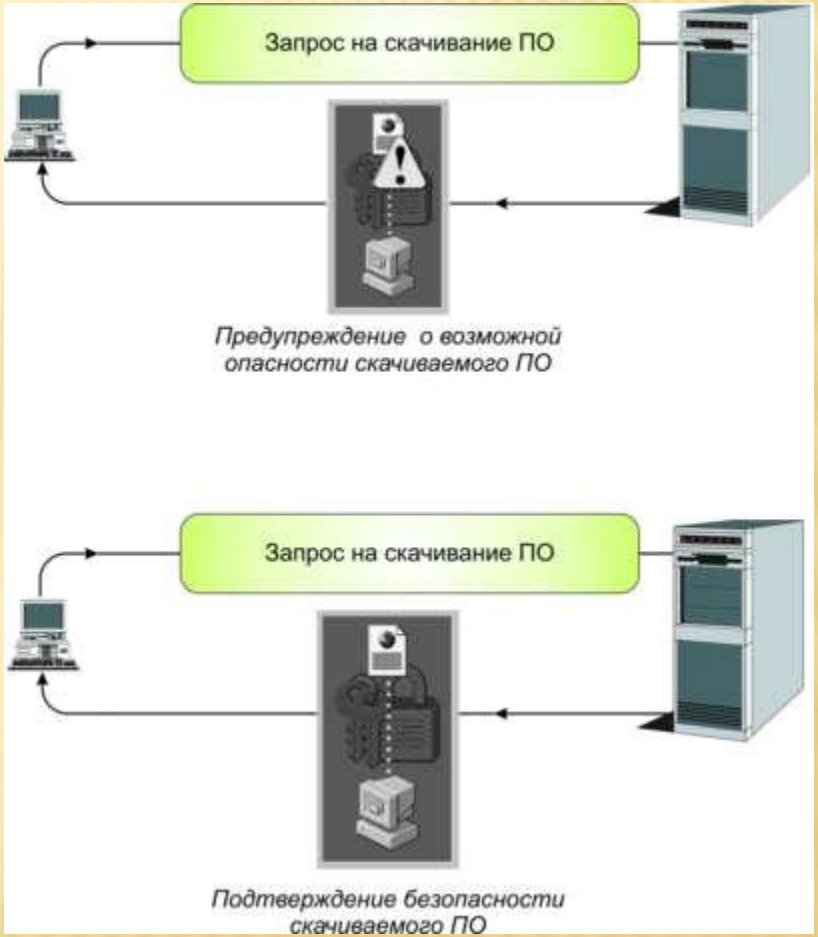
Если некто Петров (пункт 1) хочет получить личный сертификат, он направляет в центр сертификации свой паспорт и в ответ получает личный сертификат, заверенный подписью Иванова (пункт 2-3). У Петрова имеется образец подписи Иванова, поэтому он верит, что сертификат пришел именно от Иванова.

Петров сохраняет этот сертификат и рассылает его копии своим корреспондентам (пункт 4), одним из которых является некто Сидоров. Сидоров получает сертификат, заверенный подписью Иванова, и поэтому не сомневается, что сертификат действительный (пункт 5).

После того как Сидоров получил сертификат Петрова, тот может написать Сидорову, в полной уверенности, что его не примут за кого-то еще (пункт 6). Сидоров получает письмо с подписью Петрова (пункт 7), сравнивает ее с подписью в личном сертификате Петрова и убеждается, что письмо от Петрова.

ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Когда вы скачиваете продукт из Сети, нет гарантии, что поставщик данного ПО является именно тем, за кого себя выдает, а скачиваемое ПО не содержит вирусов.
Данная проблема решается путем внедрения в распространяемый продукт кода аутентификации (Authenticode), позволяющего включать информацию о разработчике посредством использования цифровой подписи.



ПРИМЕНЕНИЕ

- В Internet Explorer для импорта и экспорта сертификатов предусмотрен менеджер импорта и экспорта сертификатов - Internet Explorer Certificate Manager, который позволяет инсталлировать и удалять сертификаты клиентские и сертификаты центров сертификации.
- В пакете Office2010 технология цифровых подписей применяется для подписывания файлов, документов и макросов. Если подписан весь файл, цифровая подпись гарантирует, что этот файл не изменялся с момента подписывания.

ХРАНЕНИЕ ЗАКРЫТОГО КЛЮЧА

В настоящее время существуют следующие устройства хранения закрытого ключа:

- Дискеты
- Смарт-карты
- USB-брелоки
- Таблетки Touch-Memory

СРАВНИТЕЛЬНАЯ ОЦЕНКА ОБЫЧНОЙ ПОДПИСИ С ЦИФРОВОЙ

Защита целостности документа

- В случае применения обычной подписи и печати после подписания документ может быть изменён (например, допечатано пару нулей). Изменить же электронный документ, подписанный цифровой подписью невозможно, поскольку содержание документа через его дайджест “включается” в саму подпись.

Подделка подписи

- Чтобы подделать обычную подпись достаточно иметь компьютер, цветные сканер и принтер, а также образец подписи и печати. Стоимость перечисленного оборудования в настоящее время не превышает $2000. Далее дело техники.

Конфиденциальность

- Документ, подписанный обычной подписью, может быть прочитан любым лицом, к которому он попал в руки. В случае цифровой подписи предусматривается режим, когда документ может быть прочитан только лицом, которому он адресован.

- Защита информации с помощью паролей

ПАРОЛЬ

Пароль это секретное слово или набор символов, предназначенный для подтверждения личности или полномочий.

Пароли часто используются для защиты информации от несанкционированного доступа.

В большинстве вычислительных систем комбинация «имя пользователя — пароль» используется для удостоверения пользователя.

ПАРОЛИ, КОТОРЫЕ ЛЕГКО ВЗЛОМАТЬ:

- дата рождения
- 111, 333, 777 или что вроде этого
- 12345 или qwert - буквы клавиатуры идущие подряд
- простые имена - sergey, vovan, lena ...
- русское слово набранное в английской кодировке, напр. Сергей получится Cthutq

ЗАЩИЩЕННЫЙ ПАРОЛЬ:

длинный (8-12-15 символов)

сложно взломать пароль в котором присутствуют ЗАГЛАВНЫЕ БУКВЫ, малые буквы и цифры (не дата рождения!)

не из словаря, то есть не слово, не имя ...

отдельный пароль для каждого отдельного сервиса

не связанный с вами (адрес. номер сотового ...).

ИНСАЙДЕРЫ

Инсайдеры - это люди, которые имеют прямой доступ к вашим данным, например сотрудники Mail.ru, где находится ваша почта или сайтов Одноклассники, Вконтакте

Недобросовестный сотрудник просто может взять ваш пароль. Поэтому не пользуемся сомнительными сервисами

В продаже паролей был уличен Mail.ru. Надежными являются сервисы Google, Яндекс

ВАЖНО!

Не должно быть одинаковых паролей:

- для доступа эл.почты,
- эл. платежные системы (WebMoney, RBK Money, Яндекс.Деньги …)

алфавит	6 символов	8 символов	10 символов	12 символов
Время полного перебора всех возможных паролей заданного алфавита при скорости перебора 10,000,000 паролей в секунду				
26 (латиница в одном регистре)	31 сек	5 часов 50 мин	163.5 суток	303 года
52 (латиница с переменным регистром)	33 мин	62 суток	458 лет	1,239,463 года
62 (латиница разного регистра плюс цифры)	95 мин	252 суток 17 часов	2,661 год	10,230,425 лет
68 (латиница разного регистра плюс цифры плюс знаки препинания .,;:!?)	2 часа 45 мин	529 суток	6,703 года	30,995,621 год
80 (латиница разного регистра плюс цифры плюс знаки препинания .,;:!? плюс скобки ()[]{} плюс #$%&*~) не везде пойдет	7 часов 30 мин	5 лет 4 месяца	34,048 лет	217,908,031 год

ПРОГРАММЫ ПО ВЗЛОМУ ПАРОЛЕЙ

В настоящее время существует множество всевозможных программ предназначенных для подбора паролей операционной системы Windows.

- Например: LCP (распространяется бесплатно)

LCP

LCP - Программа предназначена для подбора паролей операционной системы Windows (старое название - LC+4).

Основные возможности:

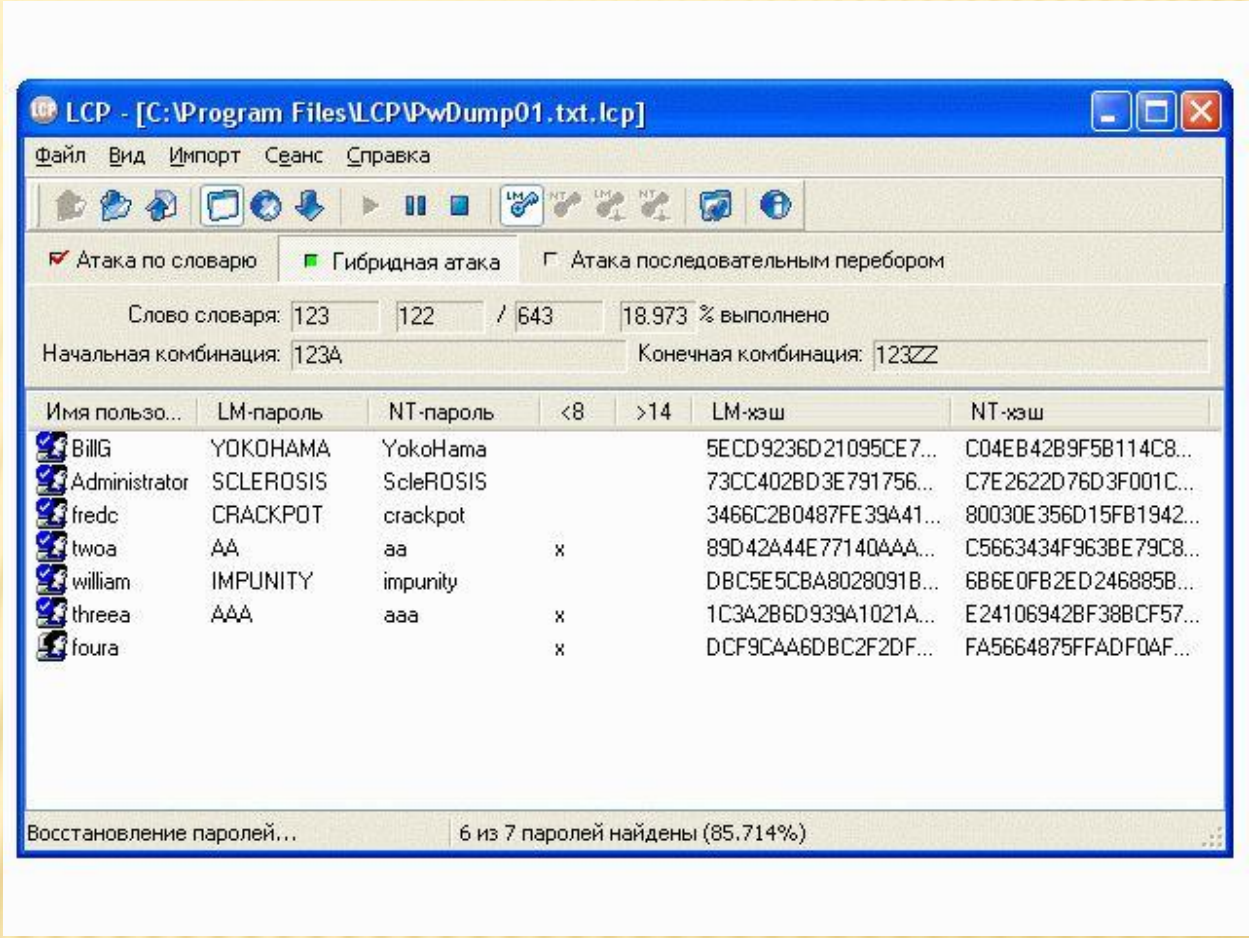
импорт информации об учетных записях пользователей	создание дампа паролей (методом pwdump; pwdump2)	подбор паролей с применением словаря	подбор паролей гибридом атаки по словарю и последовательного перебора	подбор пароля последовательным перебором комбинаций

LCP

Подбор пароль вида:

- 12345
- 87654
- Aaaaaa
- Qwerty
- Admin

Займет около 1 минуты и менее



ОСНОВНЫЕ РЕКОМЕНДАЦИИ ПО СОСТАВЛЕНИЮ ПАРОЛЕЙ

- минимальная длина пароля должна быть не менее 8 символов;
- кроме букв и цифр желательно включать в пароль другие символы, имеющиеся на клавиатуре (например, символы / ? ! < > [ ] { } и т.д.);
- пароль являющийся словарным словом очень уязвим перед автоматическими программами-взломщиками, которые используют частотные словари для перебора наиболее употребимых слов;
- пароль составленный из набора букв, находящихся на клавиатуре по-соседству также уязвим, все популярные комбинации давно включены в базы данных программ подбора паролей;
- нельзя использовать в качестве пароля даты и телефоны - именно такие пароли взламываются чаще всего.

ОСНОВНЫЕ РЕКОМЕНДАЦИИ ПО СОСТАВЛЕНИЮ ПАРОЛЕЙ

- Все пароли необходимо менять с определенной периодичностью, оптимальный срок - от трех месяцев до года.
  Хороший пароль должен состоять из бессмысленной комбинации букв и цифр, которую можно составить известным только Вам хитрым образом.

- **НАПРИМЕР**: Вспоминаете строчку стихотворения, из каждого слова берёте три первые буквы (при включенной латинской раскладке вводите символы соответствующие русским буквам), в начале ставите восклицательный знак, а в конце день рождения своей матери. Такой пароль легко запомнить, а подобрать его практически невозможно. Из строчки стихотворения: "*Белеет парус одинокий*" и даты 29.05.XXXX получается такой пароль:**!,tkgfhjlb29**.

КОМПЬЮТЕРНЫЕ ВИРУСЫ

УГРОЗЫ БЕЗОПАСНОСТИ

- Конкретные действия вредоносного кода на компьютере зависят от вида и назначения программы злоумышленника.
- Она может быть разработана лишь с целью вызвать раздражение пользователя или может нанести реальный вред компьютеру путем удаления файлов и программ.

ЧТО ТАКОЕ ВИРУС?

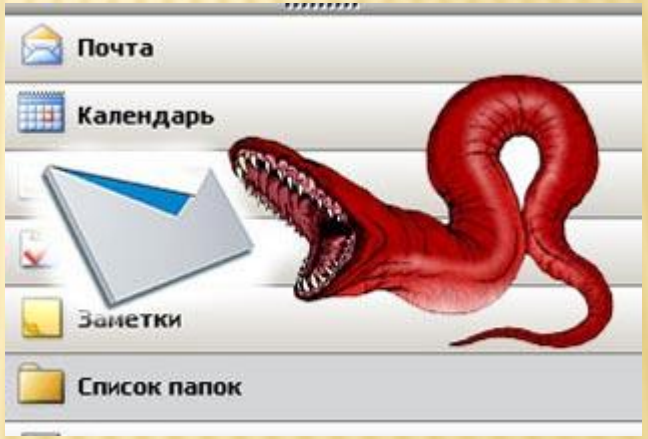
Вирусы - Программы (или программный код), написанные с целью копирования самих себя.

Вирусы пытаются распространиться на компьютеры путем прикрепления себя к другим файлам и программам.

КЛАССИФИКАЦИЯ ФАЙЛОВЫХ ВИРУСОВ ПО СПОСОБУ ЗАРАЖЕНИЯ

1. **Вирусы – черви**

Программы, которые пытаются самостоятельно отправить себя на другие компьютеры через сетевые подключения.



КЛАССИФИКАЦИЯ ФАЙЛОВЫХ ВИРУСОВ ПО СПОСОБУ ЗАРАЖЕНИЯ

2. **Троянские кони**

Программы, которые выглядят полезными или безвредными, но содержат скрытый код, предназначенный для использования или повреждения компьютера.

ТРОЯНЫ

- Троянские программы, "троянские кони" и просто "трояны" - это вредоносные программы, которые сами не размножаются. Подобно знаменитому Троянскому коню из "Илиады" Гомера, программа-троянец выдает себя за что-то полезное. Чаще всего троянский конь маскируется под новую версию бесплатной утилиты, какую-то популярную прикладную программу или игру.

- Таким способом "троян" пытается заинтересовать пользователя и побудить его переписать и установить на свой компьютер вредителя самостоятельно.

ВИДЫ ТРОЯНОВ

По выполняемым вредоносным действиям троянские программы можно условно разделить на следующие виды:

- утилиты несанкционированного удаленного администрирования (позволяют злоумышленнику удаленно управлять зараженным компьютером);
- утилиты для проведения DDoS-атак (Distributed Denial of Service - распределенные атаки типа отказ в обслуживании);
- шпионские и рекламные программы, а также программы дозвона;
- серверы рассылки спама;
- многокомпонентные "троянцы"-загрузчики (переписывают из Интернета и внедряют в систему другие вредоносные коды или вредоносные дополнительные компоненты).

КЛАССИФИКАЦИЯ ФАЙЛОВЫХ ВИРУСОВ ПО СПОСОБУ ЗАРАЖЕНИЯ

3. **Перезаписывающие вирусы**

Вирусы данного типа записывают своё тело вместо кода программы, не изменяя названия исполняемого файла, вследствие чего исходная программа перестаёт запускаться.

При запуске программы выполняется код вируса, а не сама программа.

Классификация файловых вирусов по способу заражения

4. **Шпионские программы.**

Программы, которые могут отображать рекламные объявления (например, всплывающую рекламу), собирать сведения о пользователях или изменять настройки на их компьютерах, обычно без согласия самих пользователей.

Шпионские программы обычно загружаются при посещении ненадежных веб-узлов.

SPYWARE

- Существует класс программ - клавиатурные шпионы. Эти вредители следят за пользователем и записывают каждое нажатие клавиши. По команде хакера или через определенное время клавиатурный шпион отсылает собранные сведения на компьютер злоумышленника.
- Существуют также "трояны"-шпионы, которые отсылают на удаленный компьютер пароли и другую личную информацию пользователя.

- За последние несколько лет получили распространение шпионские программы, которые собирают сведения о предпочтениях пользователя, часто посещающего Интернет.
- Такие вредители записывают адреса посещенных сайтов и имена загруженных файлов, а потом передают эти данные на чужой компьютер.
- Эта информация представляет большую ценность для компаний, проводящих маркетинговые, аналитические и статистические исследования.

Классификация файловых вирусов по способу заражения

5. **Фишинг**

Способ извлечения личных сведений, таких как данные банковских или кредитных карточек, реализуемый обычно через электронную почту.

Существуют также схемы фишинга данных посредством записи на компьютер шпионских программ.

ИСТОЧНИКИ ЗАРАЖЕНИЯ

Будь это вирус, червь, троянский конь или шпионская программа, вредоносный код пытается скрытно попасть на компьютер пользователя, чтобы не вызвать подозрений.

Например, вредоносный код может находиться во вложении в электронную почту, в некоторых программах, загружаемых из Интернета, на посещаемом веб-узле, в общем или сетевом файле, на дискете, совместно используемой с другими пользователями, или даже внутри документа Microsoft Office.

По существу любые данные, поступающие с другого компьютера, могут представлять потенциальную угрозу.

ИСТОЧНИКИ ЗАРАЖЕНИЯ

Контролируя данные, поступающие на компьютер, следует также быть осторожным при посещении веб-узлов, запрашивающих сведения, и необходимо убедиться в подлинности веб-узла, прежде чем вводить какие-либо личные сведения

Например, следует убедиться, что посещаемый веб-узел принадлежит финансовой организации, а не является поддельным веб-узлом, сфабрикованным злоумышленниками

Также учтите, что при посещении любого веб-узла происходит неявная загрузка файлов, поэтому посещать следует только веб-узлы, заслуживающие доверия

АДМИНИСТРАТИВНЫЕ МЕРЫ БОРЬБЫ С ВИРУСАМИ

Говоря о степени ответственности антивирусной защиты, требуется разделять корпоративные и частные системы.

Если речь идет об информационной безопасности организации, то необходимо позаботиться не только о технических (программных и аппаратных) средствах, но и об административных.

- Нельзя давать пользователям возможности самостоятельно считывать носители информации, такие как CD-диски, USB-флэш или выходящие из употребления дискеты
- При нормальной организации безопасности в офисе именно администратор контролирует установку любого ПО; там же, где сотрудники бесконтрольно устанавливают софт, в сети рано или поздно появляются вирусы.
- Большинство случаев проникновения вирусов в корпоративную сеть связано с выходом в Интернет с рабочей станции. Существуют режимные организации, где доступ к Интернету имеют только неподключенные к корпоративной сети станции. В коммерческих организациях такая система неоправданна. Там Интернет-канал защищается межсетевым экраном и прокси-сервером

- Помимо антивирусной защиты важно не забывать о таком важном средстве защиты данных, как система резервного копирования.
- Резервное копирование является стратегическим компонентом защиты данных.
- Если данные уничтожены вирусом, но у администратора есть вовремя сделанная резервная копия, потери будут минимальными.

РЕЗЕРВНОЕ КОПИРОВАНИЕ

Резервное копирование backup

— процесс создания копии данных на носителе , предназначенном для восстановления данных в оригинальном месте их расположения в случае их повреждения или разрушения

ХРАНЕНИЕ РЕЗЕРВНОЙ КОПИИ

Лента стримера	запись резервных данных на магнитную ленту стримера
DVD или CD	запись резервных данных на компактные диски
HDD	запись резервных данных на жёсткий диск компьютера
LAN	запись резервных данных на любую машину внутри локальной сети
FTP	запись резервных данных на FTP-серверы
USB	запись резервных данных на любое USB-совместимое устройство (такое, как флэш-карта или внешний жёсткий диск)
ZIP, JAZ	Резервное копирование на дискеты ZIP, JAZ

СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Средства предотвращения взлома корпусов и краж оборудования.
- Средства контроля доступа в помещения.
- Инструментальные средства анализа систем защиты
- Системы бесперебойного питания
- Системы анализа и моделирования информационных потоков (CASE-системы).
- Системы мониторинга сетей

ЦЕНТР ОБНОВЛЕНИЯ МАЙКРОСОФТ — НЕОБХОДИМАЯ МЕРА БЕЗОПАСНОСТИ

В качестве первоначального шага по обеспечению безопасности компьютера следует убедиться, что установлены последние версии программного обеспечения.

Корпорация Майкрософт регулярно выпускает обновления — в новостях они упоминаются как «исправления» — для борьбы с новыми угрозами по мере их возникновения.

Эти обновления доступны для Microsoft Windows и Microsoft Office.

ЦЕНТР ОБНОВЛЕНИЯ МАЙКРОСОФТ — НЕОБХОДИМАЯ МЕРА БЕЗОПАСНОСТИ

Опытные пользователи регулярно проверяют наличие обновлений и устанавливают их.

Все обновления для операционных систем Windows и пакетов Office находятся на веб-узле Центр обновления Майкрософт

Можно даже настроить службу «Центр обновления Майкрософт» на автоматическую загрузку и установку новых обновлений по мере их доступности.

Таким образом, после того как служба настроена, она работает без вмешательства пользователя.

АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Наиболее важной защитой от вирусов является антивирусное программное обеспечение

Установите его и постоянно обновляйте

Если компьютер подключен к сети, то эти действия, возможно, выполняются администратором сети

Антивирусное программное обеспечение необходимо в качестве защиты от вирусов

АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Антивирусные программы разрабатываются для обнаружения известных вирусов

Так как новые вирусы пишутся постоянно, требуется регулярно обновлять антивирусные программы

Когда появляется новый вирус, производители антивирусных программ обычно готовят обновление и выкладывают его для загрузки на свои веб-узлы спустя несколько часов после появления вредоносного кода

КЛАССИФИКАЦИЯ АНТИВИРУСОВ

- Определяют наличие вируса по БД, хранящей сигнатуры (или их контрольные суммы) вирусов.

Сканеры

- Запоминают состояние файловой системы, что делает в дальнейшем возможным анализ изменений.

Ревизоры

- Отслеживают потенциально опасные операции, выдавая пользователю соответствующий запрос на разрешение/запрещение операции.

Сторожа (мониторы)

- Изменяют прививаемый файл таким образом, чтобы вирус, против которого делается прививка, уже считал файл заражённым. В современных условиях, когда количество возможных вирусов измеряется десятками тысяч, этот подход неприменим.

Вакцины

АНТИВИРУСНЫЕ КОМПАНИИ И ПРОГРАММЫ

- ALWIL Software (avast!) из Чехии
- AVZ из России
- Dr.Web из России
- Eset NOD32 из Словакии
- Антивирус Касперского из России
- Sophos из Великобритании
- Computer Associates из США

МЕРЫ БЕЗОПАСНОСТИ

Существует огромное множество других мер безопасности, о которых следует знать. Здесь приводится их краткая сводка.

Установка антишпионского программного обеспечения.

Постоянное использование надежных паролей.

Применение брандмауэра для повышения уровня безопасности.

Регулярное создание резервных копий важных документов.

БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ

Никогда **не следует** открывать подозрительное сообщение электронной почты, полученное от неизвестного лица, или отвечать на такое сообщение:

выполнение этих действий только подтвердит, что ваш адрес электронной почты активен и действителен.

МЕЖСЕТЕВОЙ ЭКРАН

- Межсетевые экраны, называют также брандмауэрами или файерволами (от англ. firewall).
- Первые компьютерные брандмауэры были созданы для того, чтобы препятствовать распространению сетевого программного обеспечения, содержащего множество ошибок, на всю сеть с одного ее участка.
- Сегодня брандмауэры выступают в роли защитников границ между локальными сетями и Интернетом. Персональные брандмауэры выполняют те же функции, но на границе между домашним компьютером и Интернетом.

ВИДЫ БРАНДМАУЭРОВ

- Брандмауэр, или межсетевой экран,- это система, предотвращающая несанкционированный доступ извне во внутреннюю сеть.
- Брандмауэры бывают аппаратными или программными.
- Аппаратный брандмауэр - это устройство, которое подключается к сети физически, фильтрует входящий и исходящий трафик и защищает от нежелательных проникновений во внутреннюю сеть или на персональный компьютер.
- Программный брандмауэр выполняет те же функции, но является не внешним аппаратным устройством, а программой, установленной на компьютере.

Несанкционированный пользователь не сможет получить доступ в локальную сеть, если ее защищает брандмауэр.

ИЗВЕСТНЫЕ БРАНДМАУЭРЫ

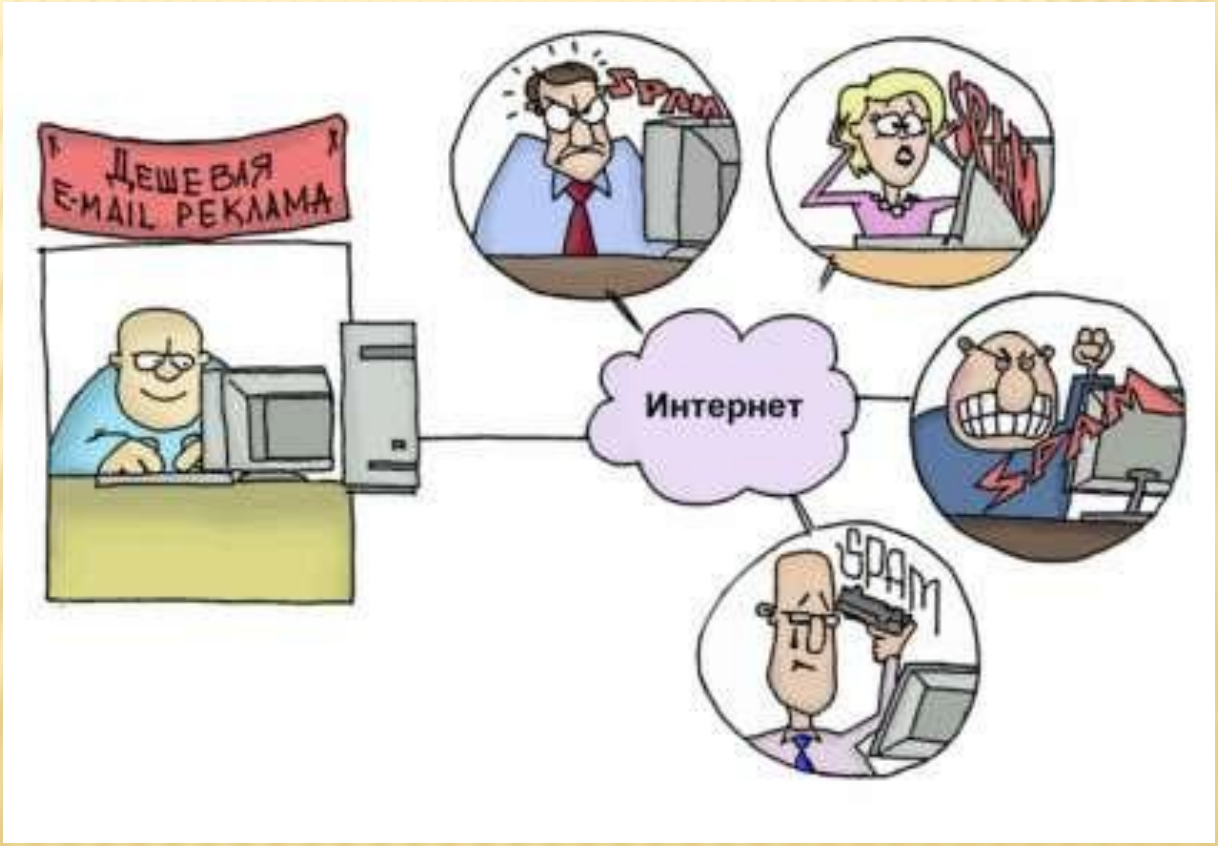
- Kaspersky Anti-Hacker
- Outpost Firewall Pro
- ZoneAlarm Pro

КОНТЕНТ-СЕКЬЮРИТИ

- Понятие "контент-секьюрити" охватывает вопросы безопасности содержания информации и включает широкий спектр тем - опасность утечки конфиденциального контента (содержания), риск попадания нежелательного контента в корпоративную сеть и т.д.
- Если речь идет о корпоративных пользователях, то в понятие "контент-секьюрити" включаются также вопросы ограничений на личную почту, личный доступ к Интернету из организации и т.п.

ОСНОВНАЯ ПРОБЛЕМА

Одной из проблем контент секьюрити является проблема нежелательных писем или спама.



ЛИЧНАЯ ПЕРЕПИСКА

- Проблема усугубляется еще и тем, что 30% сотрудников в своих частных письмах вольно или невольно отсылают информацию конфиденциального характера.
- Выявление личной переписки на рабочем месте - довольно тонкий момент. В России право на тайну переписки гарантируется любому гражданину РФ в соответствии с п. 2 ст. 23 Конституции и подтверждается ст. 138 УК РФ ("Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений граждан").

ОРГАНИЗАЦИОННЫЕ МЕРЫ

- Организационные меры борьбы со спамом применяются в рамках крупных и средних компаний и помогают несколько сократить поток нежелательных писем, попадающих в корпоративную сеть.
- Организационные меры представляют собой четкую политику, устанавливающую правила пользования почтой на рабочем месте. Только следование таким оговоренным заранее правилам позволит избежать конфликта между работодателем и сотрудником. При этом существуют общепринятые нормы поведения, снижающие риск попадания корпоративных электронных адресов в листы рассылки спама. Вот некоторые из них.

НОРМЫ ПОВЕДЕНИЯ

- Нежелательно отвечать на письма спамеров. Ответ пользователя подтверждает факт наличия данного почтового адреса.
- Имя почтового ящика не должно быть коротким или общепринятым. Иначе программа рассылки спама сможет подобрать почтовый адрес по словарю.
- Нежелательно оставлять свой основной адрес электронной почты в качестве контактных данных в Интернете, в анкетах и на форумах. Следует завести дополнительные почтовые ящики на бесплатных почтовых серверах (например, Mail.ru, Yandex.ru, Hotmail.com) и оставлять именно эти адреса.

ТЕХНИЧЕСКИЕ СРЕДСТВА БОРЬБЫ СО СПАМОМ

- К техническим средствам борьбы с нежелательной почтой относятся специальные программные фильтры, которые на основании заданной политики (набора правил) способны отсеивать нежелательную корреспонденцию.
- Следует отметить, что в фильтрах реализованы высокоинтеллектуальные технологии, принимающие решения "спам" или "не спам" на основе не только формальных признаков и ключевых слов, но и с помощью лингвистического анализа тела письма.

- Спасибо за внимание!