ИТ в юриспруденции

Лекция 7. Проблемы информационной безопасности

Розина Ирина Николаевна
Д.п.н., профессор кафедры ЕНДиИТ

Информационная безопасность

- Состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в **информационной** сфере
- Процесс обеспечения конфиденциальности, целостности и доступности информации

«Кто владеет информацией, тот владеет миром»

Ст. 1 Закона о безопасности

Понятие безопасности – "состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз«

Федеральный закон от 28.12.2010 N 390-ФЗ (ред. от 05.10.2015) "О безопасности"

Стандартная модель безопасности

1) **Конфиденциальность** – доступность информации только определенному кругу лиц

2) **Целостность** – гарантия существования информации в исходном виде

3) **Доступность** – возможность получения информации авторизованным пользователем в нужное для него время

Характеристики безопасности информации

- Аутентичность – возможность установления автора информации
- Апеллируемость – возможность доказать, что автором является именно заявленный человек и никто другой
- Подотчётность — обеспечение идентификации субъекта доступа и регистрации его действий
- Достоверность — свойство соответствия предусмотренному поведению или результату

Государственные органы РФ, контролирующие деятельность в области защиты информации

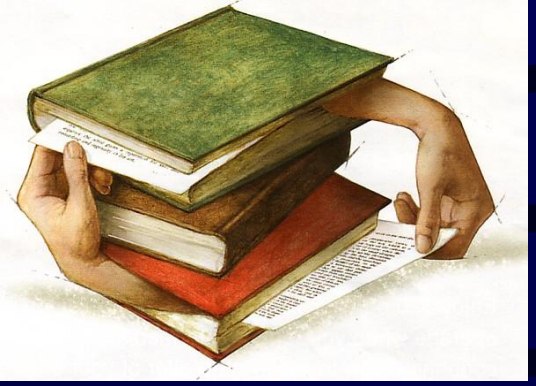
- Федеральная служба безопасности Российской Федерации (**ФСБ России**)
- Министерство внутренних дел Российской Федерации (**МВД России**)
- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (**Роскомнадзор**)

Методы обеспечения информационной безопасности

- Средства *идентификации* и *аутентификации* пользователей (ЗА -- аутентификация, авторизация, администрирование)
- средства *шифрования* информации, хранящейся на компьютерах и передаваемой по сетям
- *межсетевые экраны*

Компьютерная этика

- Компьютеры не отменяют **традиционные** моральные принципы и законодательные акты
  - копирование интеллектуальной собственности без разрешения
  - вход в секретную компьютерную систему без авторизации
- Появляются **специфичные** компьютерные проблемы, которые ставят пользователей перед моральной дилеммой и требуют особого подхода и урегулирования
  - плагиат (электронные архивы рефератов на веб-сайтах и CD-ROM)
  - пиратское программное обеспечение
  - непредусмотренное использование э-почты
  - эротика и непристойности
  - несанкционированный доступ в компьютерные системы



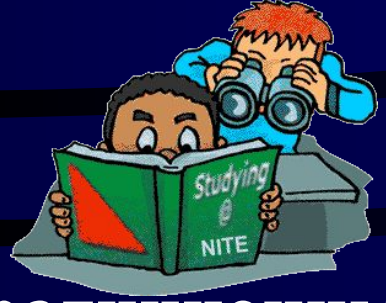
Плагиат (электронные архивы рефератов на веб-сайтах и CD, digital term-paper mills)

- Плагиат (лат. plagiatus - похищенный , как это понималось в XVIII веке) - умышленное присвоение чужого авторства, выдача чужого произведения или изобретения за собственное
- Соблазн плагиата возрос в связи с развитием Интернета
- Отсутствуют примечания о защите прав

На сколько серьезно это правонарушение?

Гражданская (закон РФ «Об авторском праве и смежных правах») и уголовная ответственность (ст. 146 УК РФ) за нарушение авторских прав (моральный и материальный ущерб)

Международное соглашение - автор имеет право на юридическую защиту своего авторского права в случае его нарушения даже без явного указания на него, например, на своем веб-сайте.



Авторские и смежные права

Традиционные объекты

- Произведения:
  - литературные
  - музыкальные
  - хореографические
  - аудиовизуальные
  - художественные, архитектурные
  - фотографические
  - декоративно-прикладные
- Программы и БД
- Географические карты и пр.

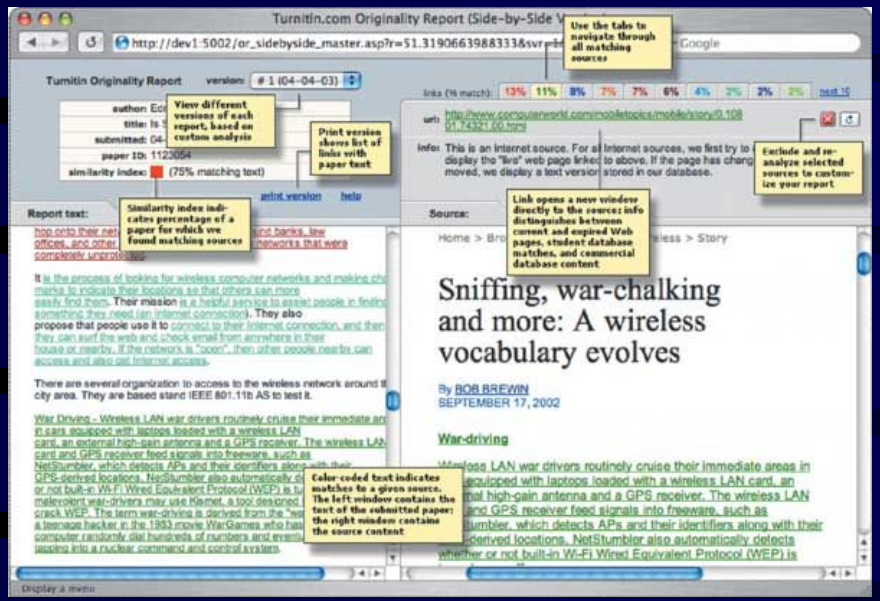
Объекты в Интернете

- материалы печатных СМИ, ТВ и др. э-СМИ
- архивы программного обеспечения
- предпринимательская деятельность юридических лиц только через Интернет
- текстовые, аудио, видео и графические файлы

Как избежать плагиата

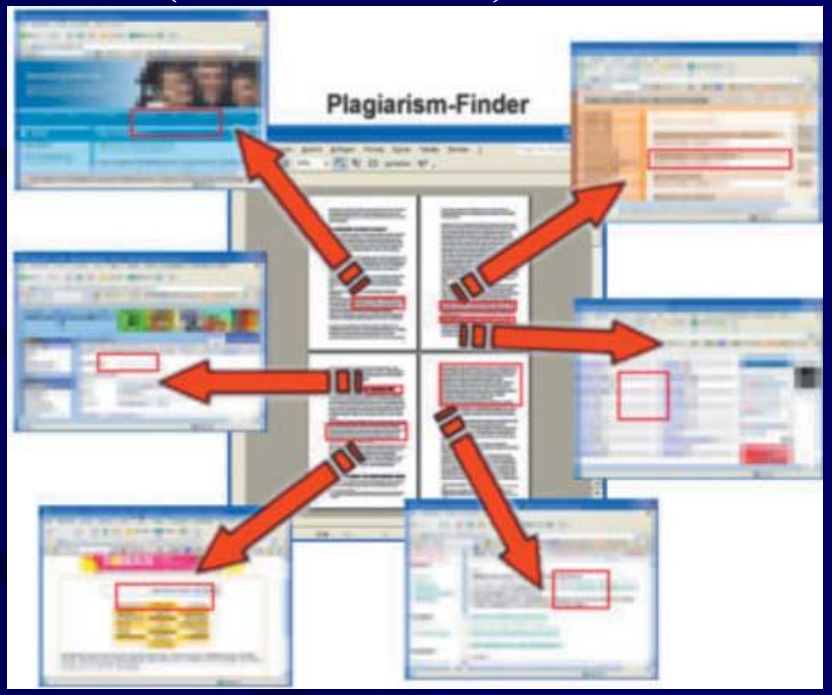
- *Ссылки на источники* информации (факты, мнения, теории, статистика, графики, рисунки), если они не являются общеизвестными (common knowledge)
- *Цитирование* высказываний или отрывков из произведений других авторов
- Избегать *недопустимого перефразирования* (unacceptable paraphrase) - скрытого использования чужого текста путем механической перестановки местами слов и фраз, замены слов синонимами при отсутствии новых мыслей
- Избегать *повторного использования* собственных работ, рециркуляции (recycling work)

Выявление плагиата



Turnitin tool - онлайновое средство проверки на плагиат (turnitin.com)

Plagiarism-Finder - приложение, проверяющее совпадения с интернет-документами



Антиплагиат.Ру /AntiPlagiat.ru - проверка текстовых документов на наличие заимствований из общедоступных сетевых источников

Виды компьютерного пиратства ПО

Уровень пиратства в странах

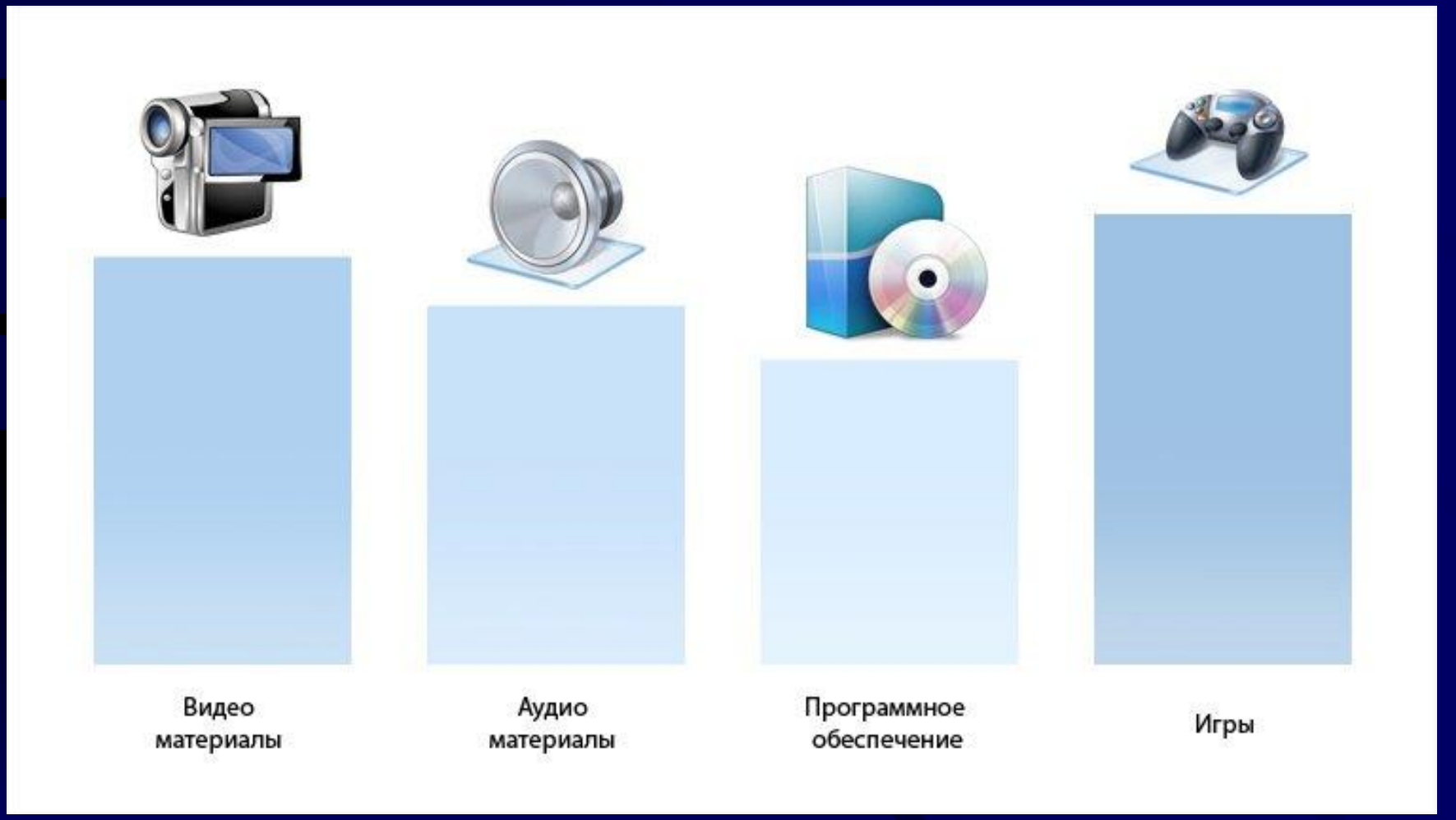
До 70%

- Бангладеш
- Зимбабве
- Молдавия
- Грузия
- Армения
- Китай
- Россия
- Украина
- Белоруссия

До 20%

- Япония
- Люксембург
- США
- Новая Зеландия

Цифровое пиратство -- копирование и распространение без соблюдения лицензии



Почему воруем?

Макропричины:

- несовершенство нормативно-правовой базы (осуждается не более 20% подследственных)
- общая криминногенная обстановка и заинтересованность в существовании пиратского сегмента организованных финансовых групп
- ментальные убеждения (9 из 10 не видят ничего зазорного в том, чтоб не покупать, а скачивать)

Микропричины:

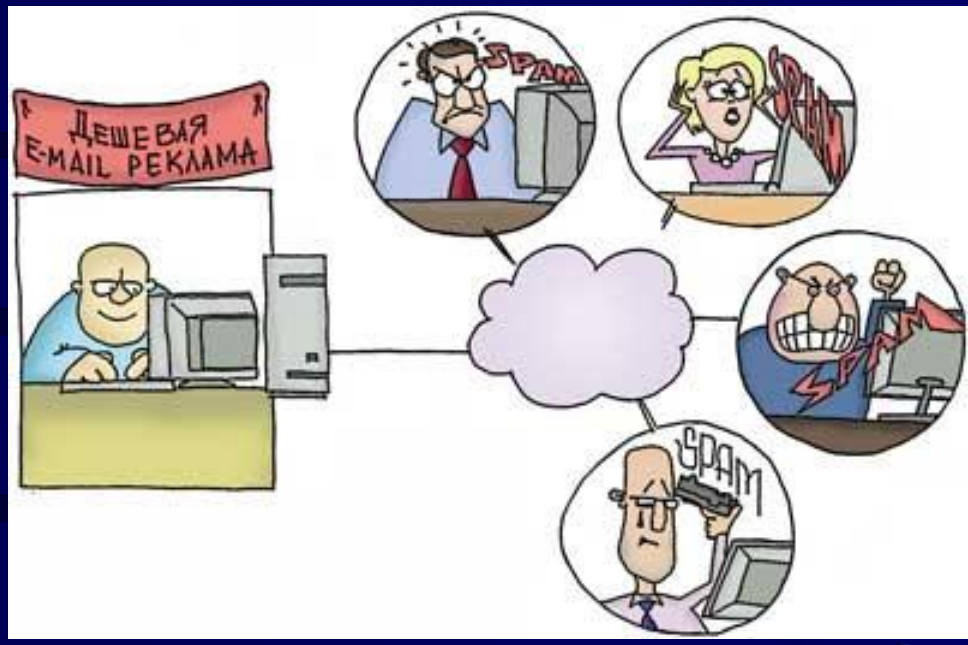
- неудобство совершения процедур оплаты
- более легкая доступность пиратских копий по сравнению с легальным контентом
- отсутствие визуальной и функциональной разницы между лицензионным и пиратским контентом
- несправедливое ценообразование

Непредусмотренное использование э-почты

- Доступность для прочтения содержимого посторонними (при пересылке, хранении) ≈ *почтовая открытка*
  - Спам - массово рассылаемые сообщения коммерческого или некоммерческого характера (реклама, письма с просьбами и предложениями)
- Язык вражды
- Неэтичное поведение (в переписке, в групповом списке рассылки)
- Вирусы (черви, троянские кони)
- Потеря корреспонденции
- Возможность имитации (автора, адреса)

Электронная подпись

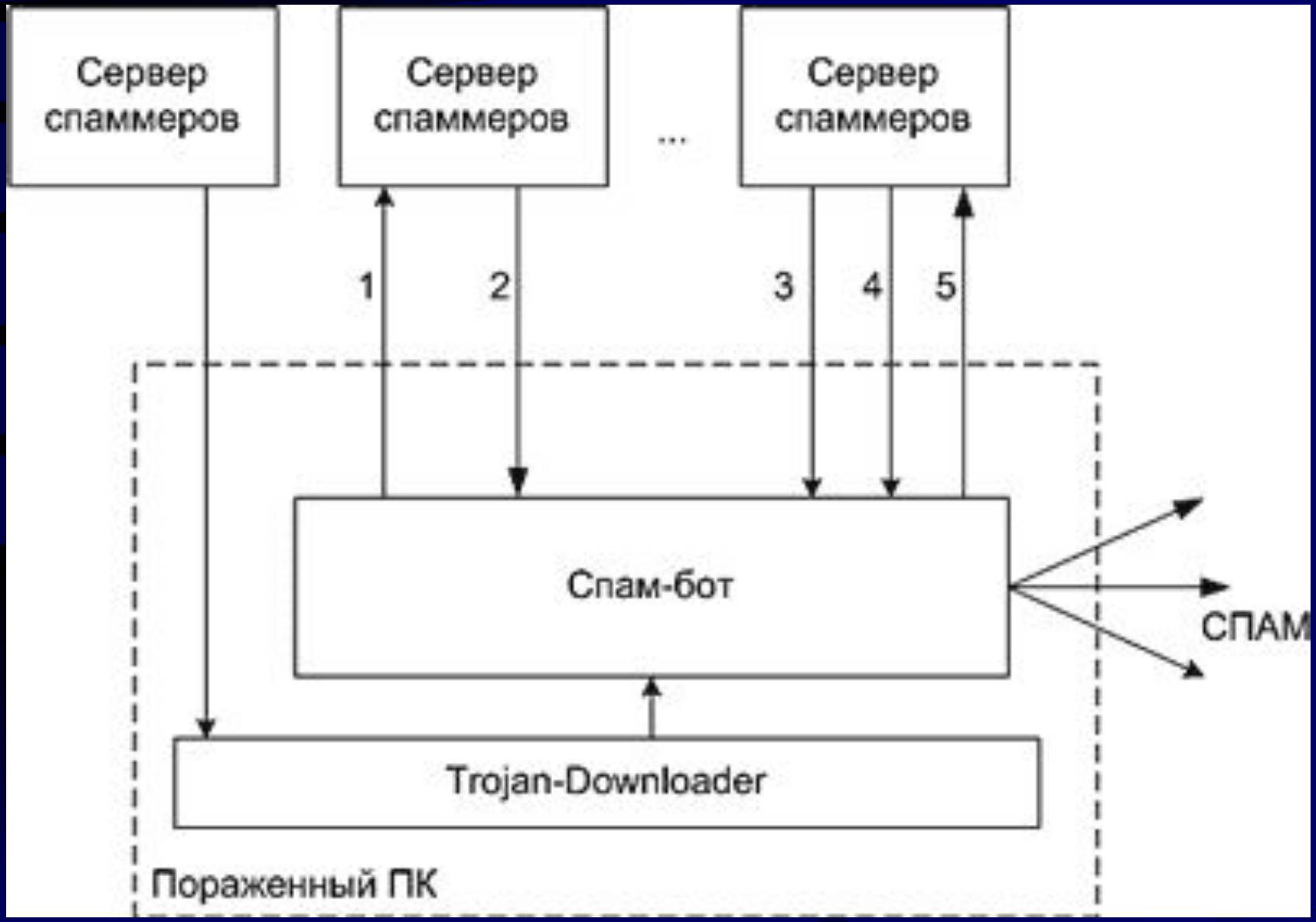
Возможность отправить письмо нескольким адресатам обернулась проблемой спама



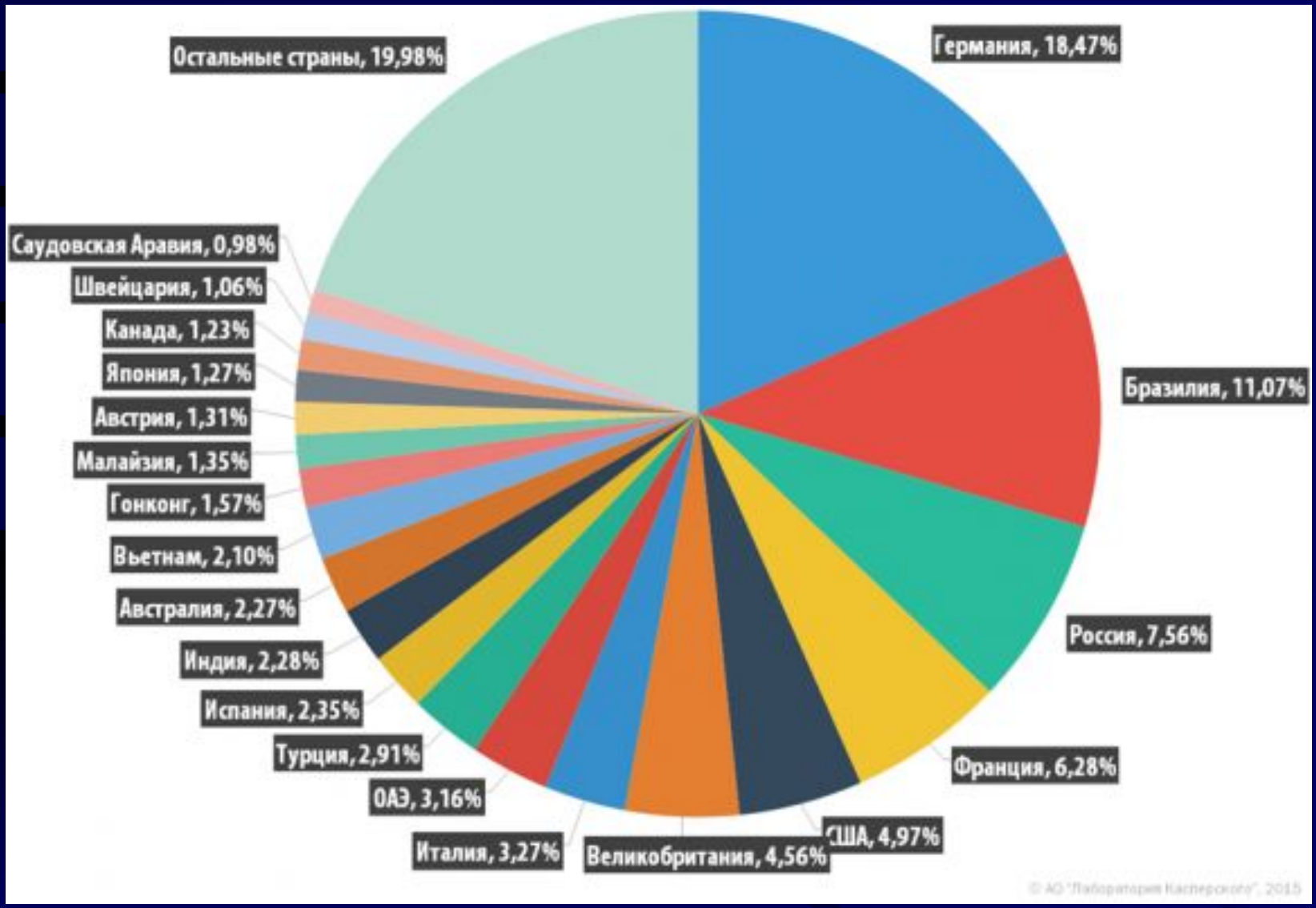
Дешевая email-реклама превратилась в доходный бизнес

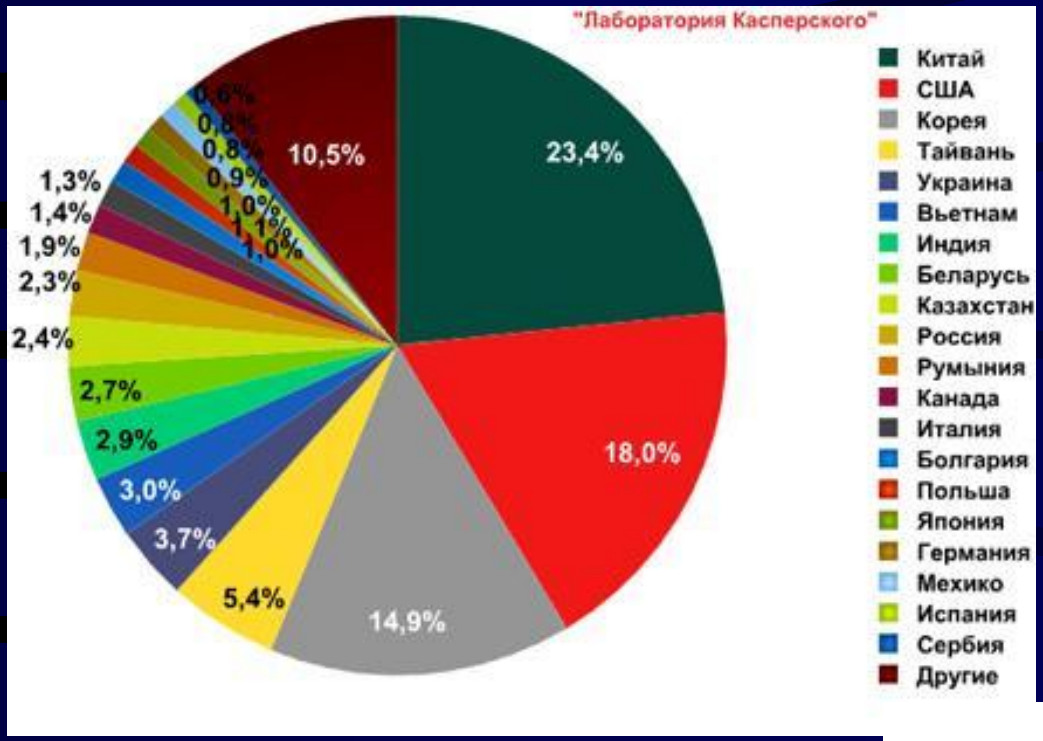
Наличие спама осложняет сортировку сообщений на нужные и ненужные

Схема работы спам-бота



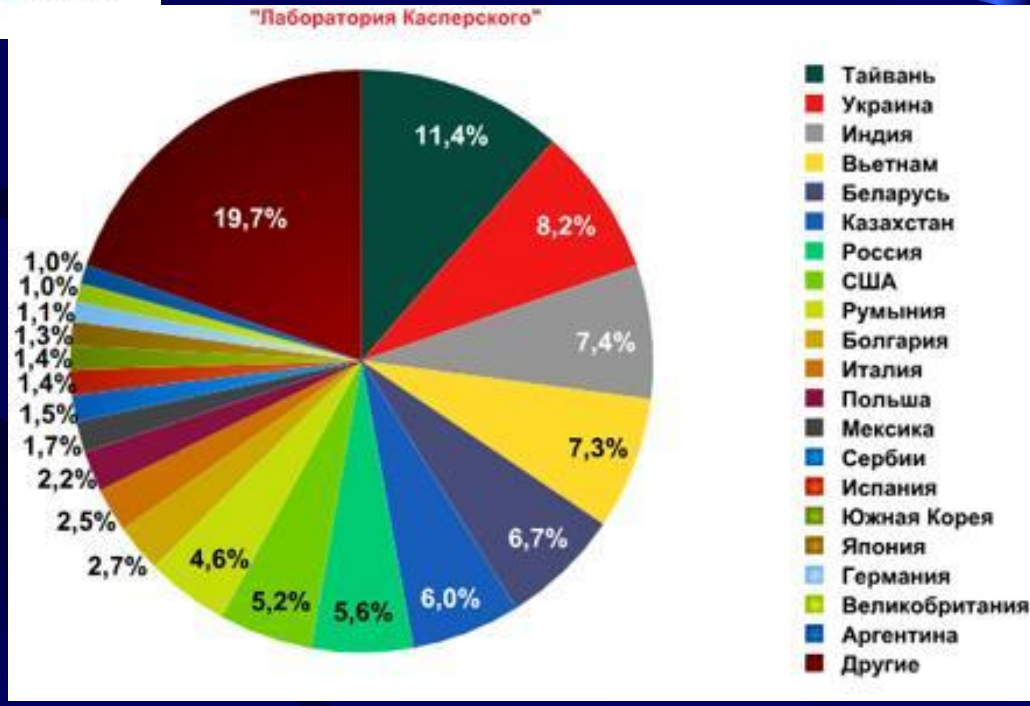
Спам в Рунете
(источник: «Лаборатория Касперского», 2015)





Страны — источники спама в мире

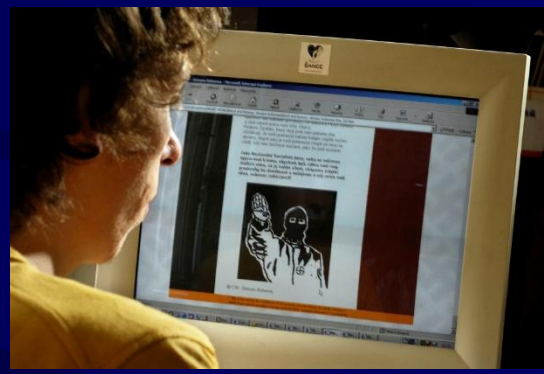
Страны — источники спама в России



Распределение топ-100 организаций, атакованных фишерами

Язык вражды (hate speech)

Проявления экстремистской деятельности, человеконенавистническое содержание веб-сайтов, нарушение политкорректности



Данные Центра Simon Wiesenthal:

- 1995 г. – 1 веб-са
- 1997 г. – > 500
- 1999 г. – 1426

Способы борьбы:

- Программы-фильтры (CyberPatrol, WebSense, CYBERSitter, Net Nanny, Surf Wath, Pure Sight - по принципу “черного списка”)
- Самоидентификация содержания сайтов контент-провайдерами (предложение международной организации ICRA – Internet Content Rating Association)
- Фильтрация на сервере провайдера или компании
- Ограничения на получение ссылок объектов неполиткорректности и ненормативной лексики через ИПС

Эротика и непристойности

- Посещение сайтов для взрослых в рабочее время, в библиотеке, в учебном учреждении, организации (сохранение посещаемых адресов в браузере, на административном сервере)
- Размещение рекламных баннеров сомнительного содержания на сайтах, предоставляющих хостинг
- Распространение вирусов через порносайты, как самые посещаемые
- Хакерские шалости с заменой содержимого, переключением на порносайты, рассылкой картинок с «обнаженкой»

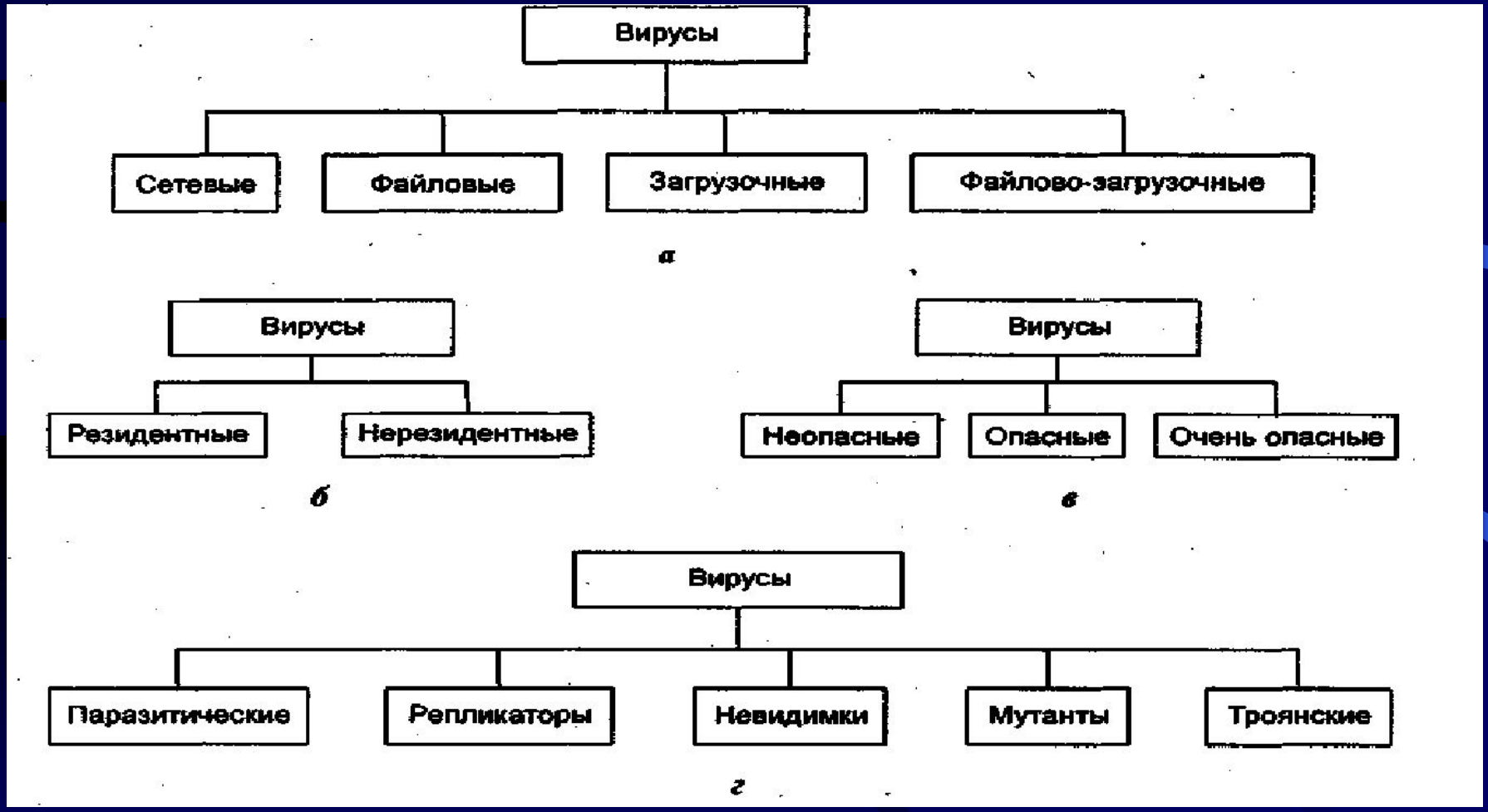
Основные признаки проявления вирусов

- Прекращение работы или неправильная работа ранее успешно функционировавших программ
- Медленная работа компьютера
- Невозможность загрузки операционной системы
- Исчезновение файлов и каталогов или искажение их содержимого
- Изменение даты и времени модификации файлов
- Изменение размеров файлов
- Неожиданное значительное увеличение количества файлов на диске
- Существенное уменьшение размера свободной оперативной памяти
- Вывод на экран непредусмотренных сообщений или изображений
- Подача непредусмотренных звуковых сигналов
- Частые зависания и сбои в работе компьютера

Классификация компьютерных вирусов

а - по способу заражения; б - по среде обитания;
в - по степени воздействия; г - по особенностям алгоритмов

«Вирусы - это первый удачный эксперимент по созданию искусственной жизни с неудачным выбором формы ее жизнедеятельности» ;-))



Вирусы по принципу действия

- *Собственно вирусы* (саморазмножающиеся программы:
  а) "черви" (worm), "ползающие" по Интернету или локальной сети и активизирующих определенные функции системы
  б) вирусы, заражающие компьютерную систему через какие-либо другие программы
- «*Троянские кони*» (маскирующиеся под что-либо полезное, но содержащие невидимые инструкции некоторых злоумышленных задач:
  а) разрушающие данные (например, при наступлении определенной даты)
  б) используемые для кражи конфиденциальной информации (логины, пароли, PIN-коды, номера счетов)
  в) используемые для получения доступа к системе (проникают незаметно, предоставляют back-door-доступ своему хозяину)
  2005 г. - все угрозы из первой десятки являлись Windows-червями, общее число *троянов* и *червей* соотносилось как 2:1

Несанкционированный доступ в компьютерные системы

Hacker – Cracker – Carder – Phreaking – *самурай*

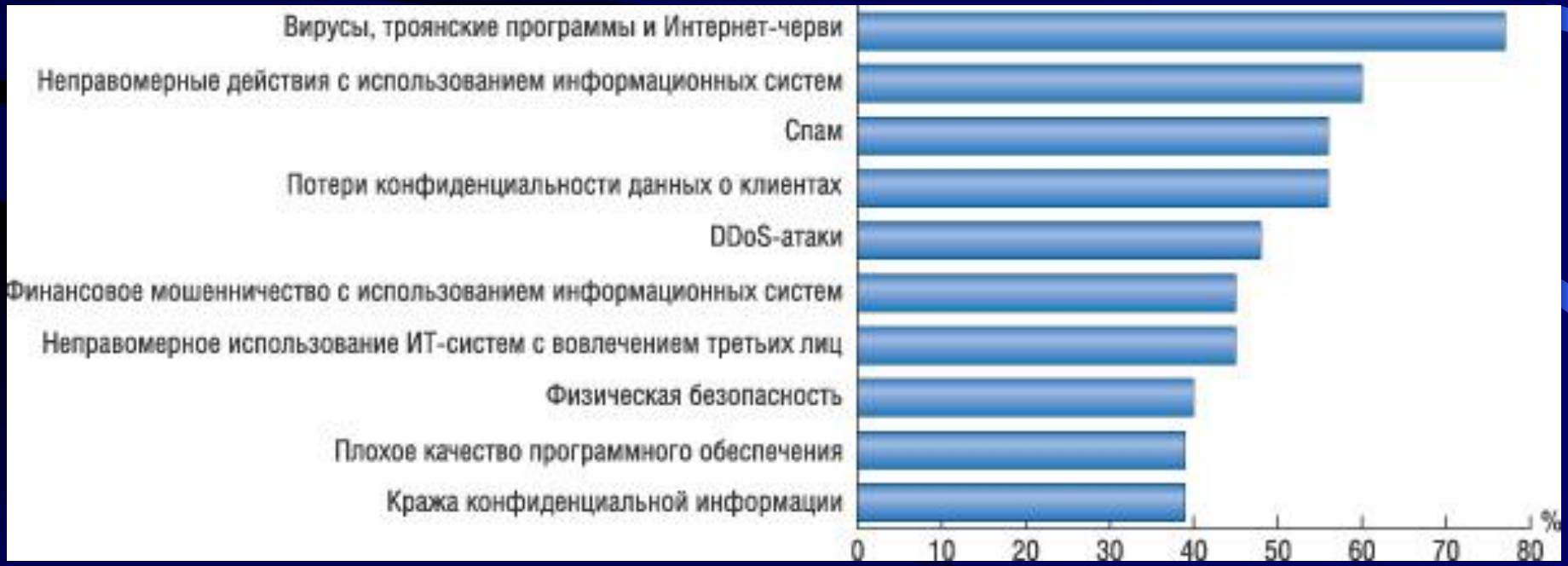
- Высококлассные программисты
- Взломщики лицензионного ПО, серверов с санкционированным доступом
- Взломщик банковских сетей
- Взлом банковских и телефонных сетей
- Исполнитель чужих заданий по проникновению в информационные массивы с целью хищения, искажения или уничтожения информации

Мотивы

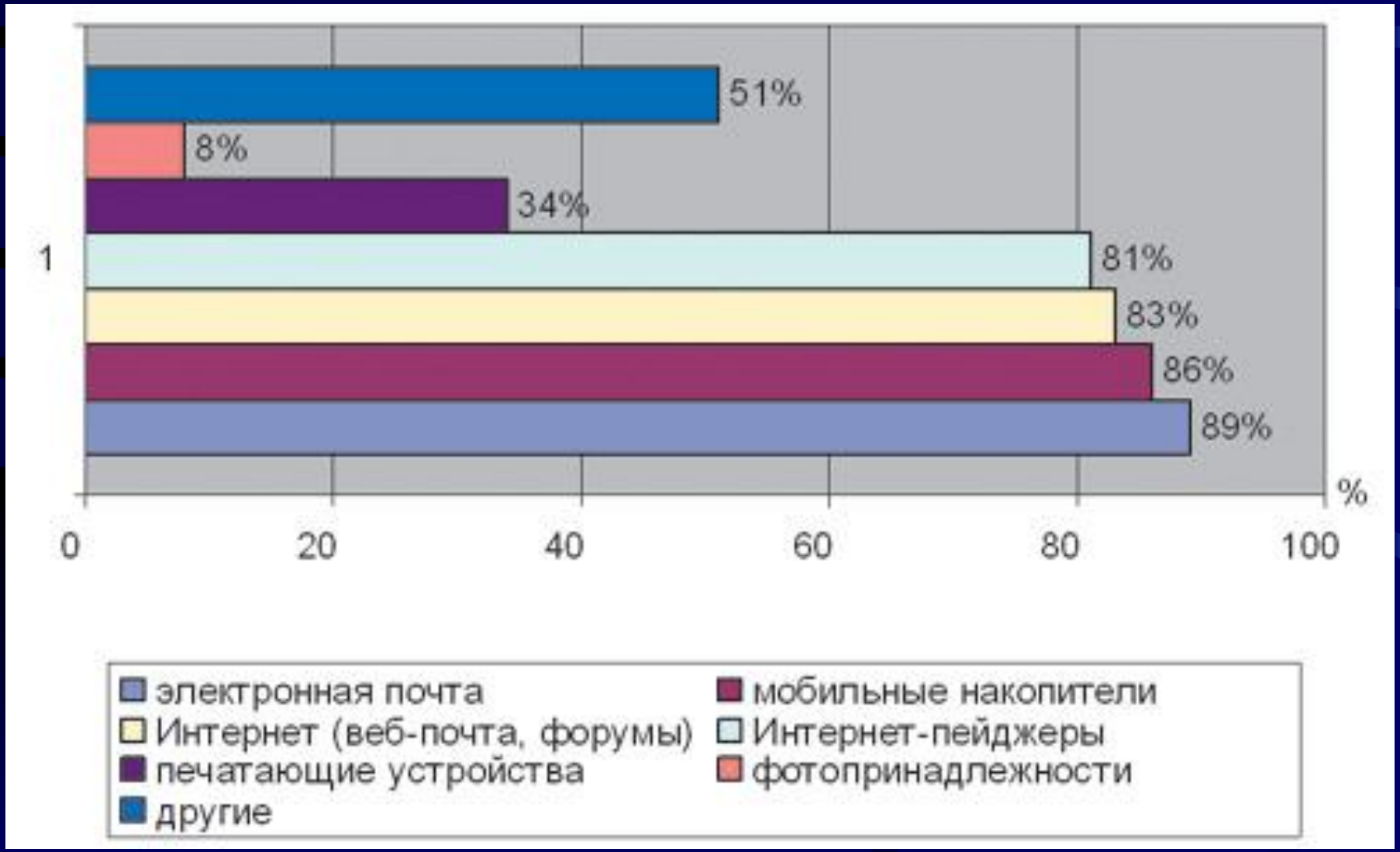
Ларошфуко: «Самая чистая форма радости – это злорадство»

- рассылка вирусов врагам
- любопытство, амбициозность
- наивные шутки, техновандализм - верят, что не причиняют вреда
- антисоциальные действия детей без внимания родителей
- выявление дыр и слабых мест в защите ПО (вирусописатели VXers ↔ создатели антивирусов AVers)
- борьба за чистоту сети (purists)
- возмутители спокойствия
- получение выгоды, шпионаж
- отсутствие этических и моральных границ, злобность, «Герострaты»
- информационная, электронная война, диверсии, кибертерроризм

10 главных угроз информационной безопасности (источник: Global Information Security Survey 2004, Ernst&Young)

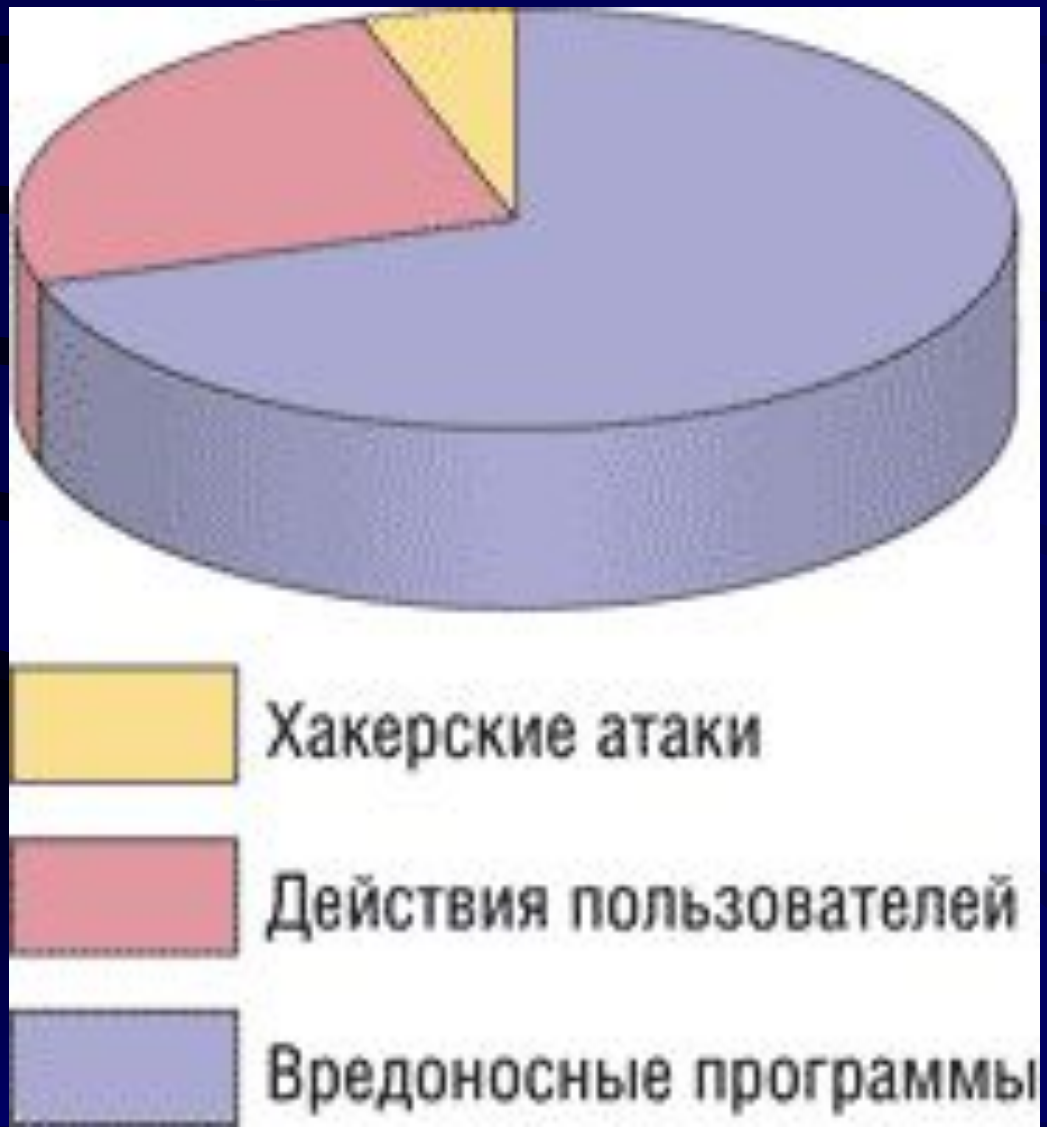


Пути утечки данных (источник: Внутренние ИТ-угрозы в России — 2004, InfoWatch)



Угрозы для корпоративной сети

Причины инцидентов



Технологии вторжения

- Самая уязвимая - электронная почта (вирус находится ≈ в каждом 44 письме, при эпидемии в каждом 12, SophosLabs, конец 2005 г.)
- Незащищенный компьютер в течение 10 мин нахождения в Интернете с вероятностью 40% будет заражен вирусом или червем (в начале 2005 г. ≈ 20 мин, SophosLabs)

Способы и результаты вторжения:

- Вычисление пароля (идущие подряд буквы, цифры, собственное имя, дата рождения)
- Использование психологических приемов - социальный инжиниринг (любопытство, жадность, неожиданность - “I love you”, “New Virus Alert!”, “Important Princess Diana Info”,“your password”, “darling”, “congratulations”, “look my beautiful girl friend”)
- “Фишинг-атаки” (сострадание, заманчивые предложения: вознаграждение за помощь иностранцу, заработок денег не выходя из дома и ничего не делая, отправка в путешествие за мизерную цену)
- Подглядывание, неосторожность в использовании личных данных
- Программный анализатор трафика
- Получение статуса администратора
- Взлом программ, использование программных ошибок и дырок
- Снятие небольших сумм со счетов
- Изменение данных

От: secur@phazen.net [mailto:secur@phazen.net]
Отправлено: Пн, 27.11.2006 11:10
Кому: Irina Rozina
Тема: Mail server report.

Mail server report. Update-KB5843-x86.zip

Our firewall determined the e-mails containing worm copies are being sent from your computer.

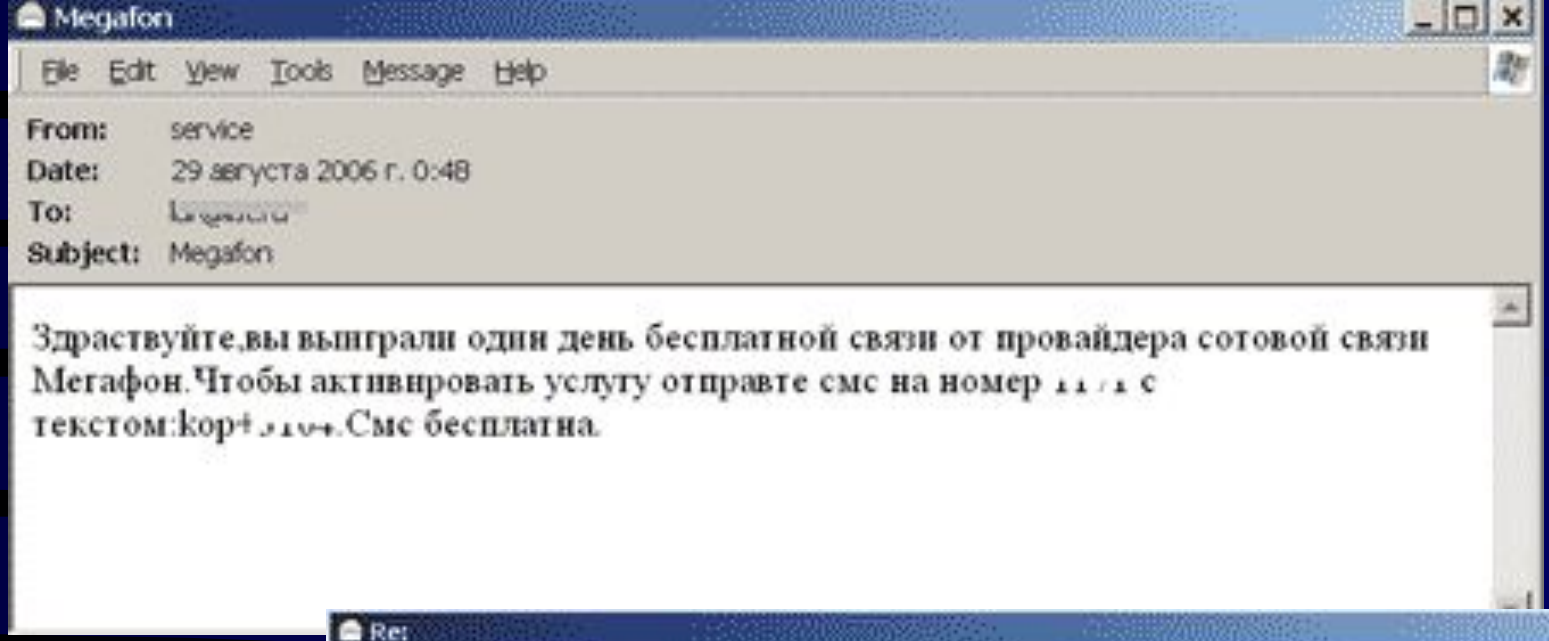
Nowadays it happens from many computers, because this is a new virus type (Network Worms).

Using the new bug in the Windows, these viruses infect the computer unnoticeably.

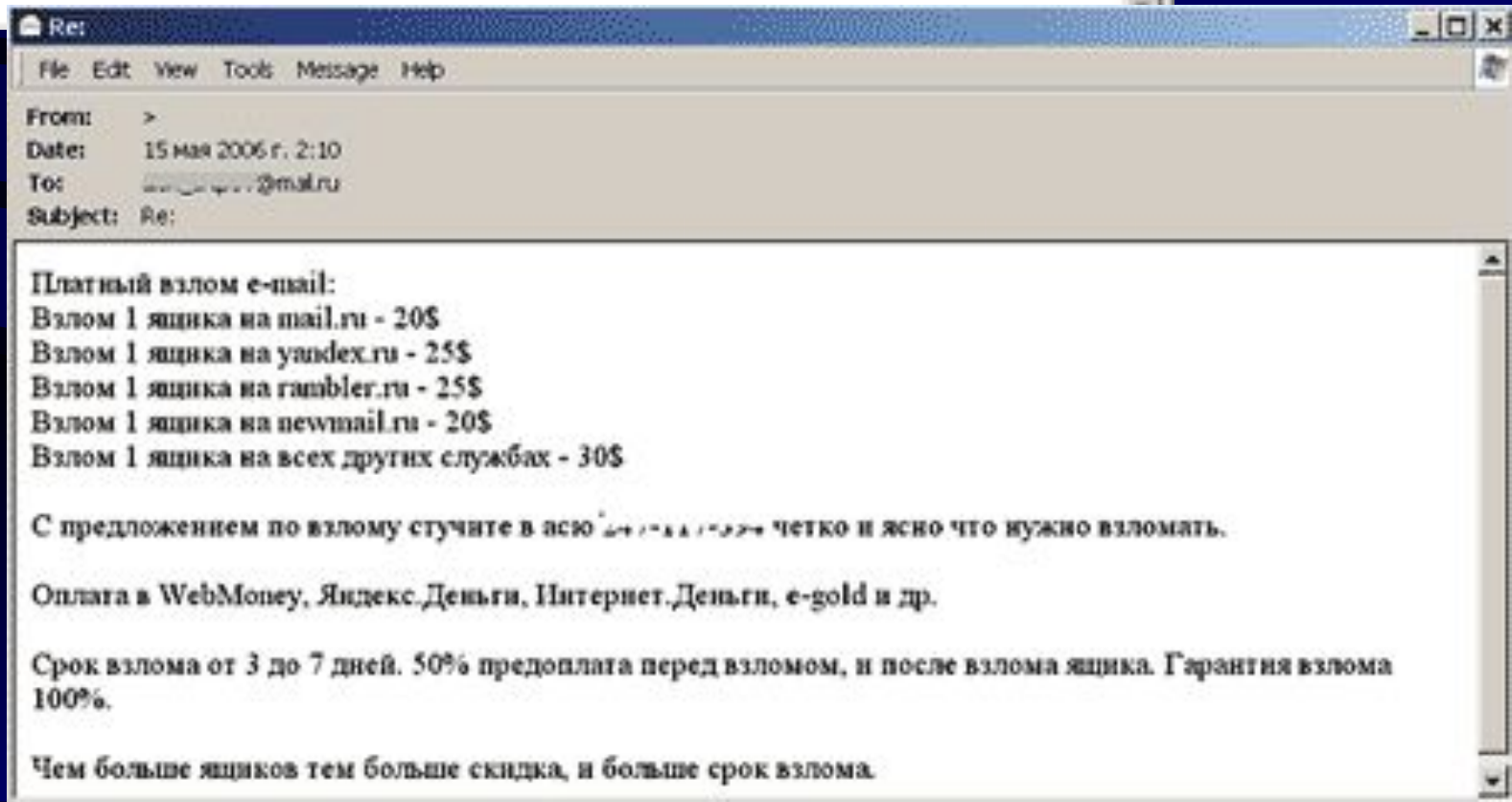
After the penetrating into the computer the virus harvests all the e-mail addresses and sends the copies of itself to these e-mail addresses

Please install updates for worm elimination and your computer restoring.

Best regards, Customers support service



Пример предложения отправить SMS для получения бесплатной услуги



Пример предложения взлома почтовых ящиков

Анти-спамовые (анти-вирусные) программы

Orange Box Mail

Kaspersky Anti-Spam

МНОГОФАКТОРНЫЙ АНАЛИЗ (ЗАГОЛОВОК, ТЕЛО, ПРИЛОЖЕНИЯ)

- По типу файла приложения (zip, html, doc)
- Характер содержания (текст, изображение, видео, аудио)
- Сочетание тела сообщения и приложения в комплексе
- Сверка адреса со списком Real-time Black Lists (RBL) - актуальные адреса спамеров (ведут провайдеры и различные общественные организации)
- Отсутствие адреса отправителя, большое число получателей и другие странности
- Содержание сообщения по эвристическому алгоритму (“Сходи на сайт”, “Для взрослых”, “Купи то или это”, “Горящие путевки”, “Снизь налоги”, “Заработок в Интернете” и т.п.)
- Наличие лексических сигнатур, составленных из известных словосочетаний спамописателей, кодов вирусов

Примеры

Организация DDoS-атак

- поиск слабо защищенных систем (edu, business)
- внедрение
- рассылка ping-запросов
- пересылка ответов на запросы на следующую жертву

Примеры

1988 - Роберт Моррис

1992 - «Микеланджело»

1995 - Кевин Митник

- Yahoo! ZDNet
- Buy.com E*Trade
- E-buy Datek
- CNN Excite
- Amazon.com

Правовые споры зарегистрированных доменных имен

Киберсквоттинг (*cybersquatting*) – от слова *cybersquatter* – киберпоселенец, поселившийся незаконно на незанятой земле. В отношении к Интернет – регистрация громкого доменного имени сайта с перспективой его последующей перепродажи заинтересованному лицу

Классический – недвусмысленная регистрация имени, идентичного известной торговой марке

MOSFILM.RU, KODAK.RU, NIVEA.RU, QUELLE.RU
KAMAZ.RU, COCA-COLA.RU, SPRITE.RU, MIELE.RU
NTV.RU, BAXTER.RU, MEGASHOP.RU, KAPEL.RU

Тайпсковттинг – захват имен, по своему написанию и звучанию воспринимаемые как известные, в том числе не для перепродажи, а с целью дезинформации, конкуренции

AYHOO.COM, YAFOO.COM, WHITEHOUSE.COM

«Интеллектуальный" – регистрация легко запоминающихся названий, тематически подходящих каким-либо компаниям либо частным лицам, но не содержащих имя

BUSINESS.COM, WINES.COM, CINEMA.COM, MEN.COM, CAR.COM, COMPUTERS.COM, SMOKING.COM

Примеры потери доменов

- Похищенные и невозвращенные:

  sex.com; hackers.com; wifi.com; commercials.com
- Вовремя не продленная регистрация:

  rocit.ru; dni.ru; lycos.ru; eweek.com, washpost.com

Фишинг (*phishing*)

- Методы, которые служат для незаконного получения и использования конфиденциальных данных (кража идентичности)
- В английском слове *fishing* намеренно сделана ошибка, иллюстрирующая один из приемов злоумышленников:
  - разработка вредоносного ПО
  - создание сетей фальшивых сайтов
  - регистрация доменов-подделок
  - целенаправленное заражение официальных корпоративных сайтов
- Фишинг-атака – отправка массовых рассылок с привлекательными или похожими на достоверные призывами: посетить сайт компании из числа известных брендов (фальшивый); от имени банка выслать данные с подтверждением номера кредитной карты и ее PIN-кода; помочь за большое вознаграждение иностранцу и т.п.

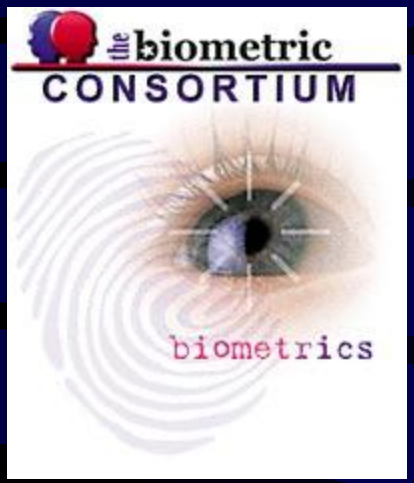
Принципы организации системы контроля, регистрации доступа в компьютерную систему, идентификации и аутентификации пользователя

1) *“Нечто такое, что вы знаете”* (пароль, ID, PIN, проговариваемая фраза - callback systems)
2) *“Нечто такое, чем Вы владеете”* (пластиковая смарт-карта, специальный знак, штрихкод, RFID-метка);
3) *“Нечто Ваше личное”* (биометрические – физиологические, поведенческие особенности)

Биометрические системы распознавания

- Развиваются с середины 1970-х гг.
- Применяются в *банковских системах*, *транспортной промышленности*, для идентификации личности при *пересечении границ государств*
- 1998 г. фирмы Mitsubishi, Япония, IBM в США и ее филиалы в Великобритании, NPI, США - подход к разработке биометрического программного интерфейса **BioAPI** (Application Program Interface):
  - *регистрация* (enroll)
  - *верификация* – сравнение “один к одному” (verify)
  - *идентификация* – сравнение “один ко многим” (identify)

Методы биометрического распознавания (19 определено)



Физиологические параметры человека:

- глаза – сетчатка (Iridian Autenticam фирмы Iridian Technologies), зрачок (BioID SOHO фирма D.C.S. AG)
- лицо – геометрия, подкожные сосуды, голос (программа Talk Direct, фирма Veritel), движение губ при разговоре
- рука – геометрия, отпечаток ладони, пальцев (AFIS, MS 3000 PC Card – сканер отпечатков пальцев фирмы Ethentica Ethenticator)
- форма уха и пр.

Поведенческие системы:

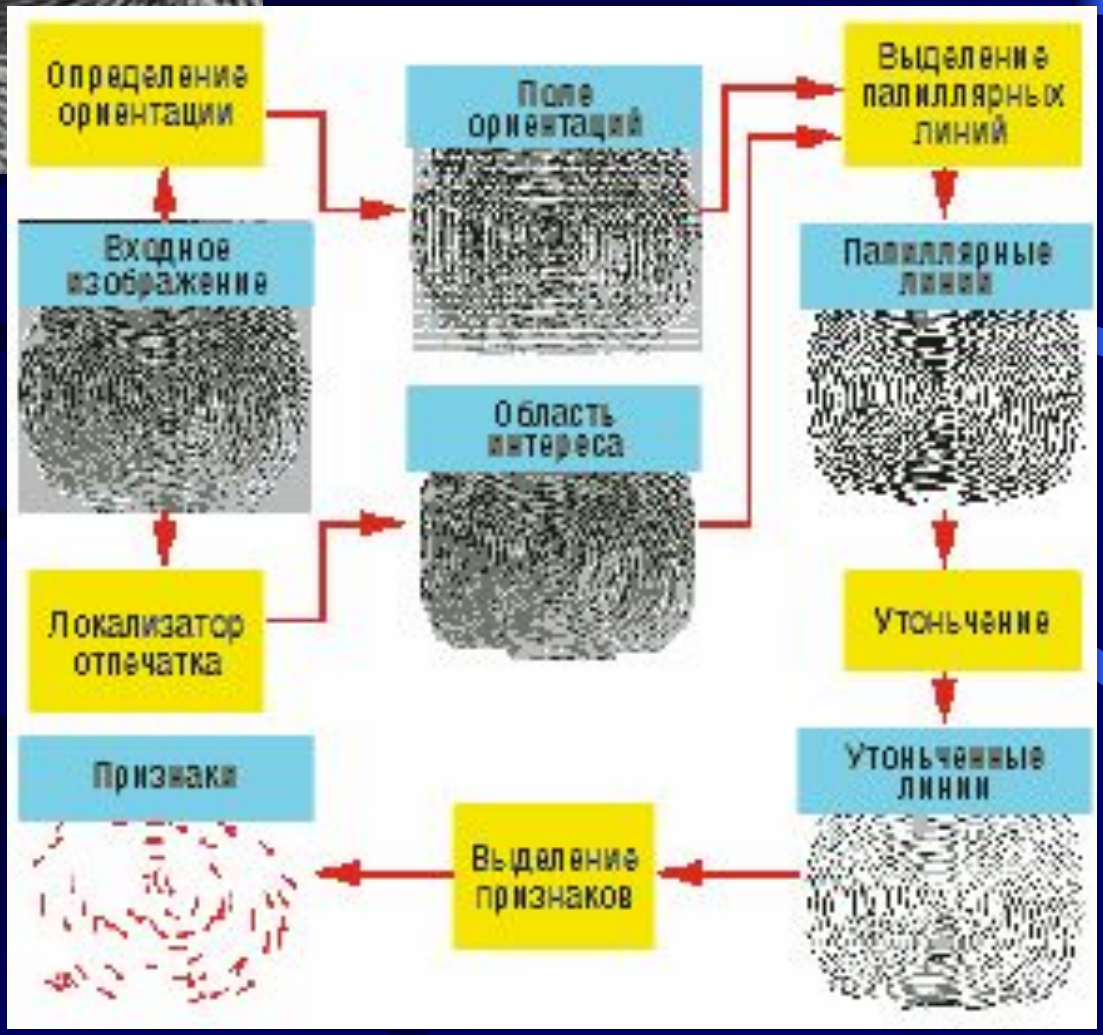
- подпись (например, Cyber-Sign Electronic Signature Verification для Adobe Acrobat)
- динамика подписи
- динамика клавиатурного набора

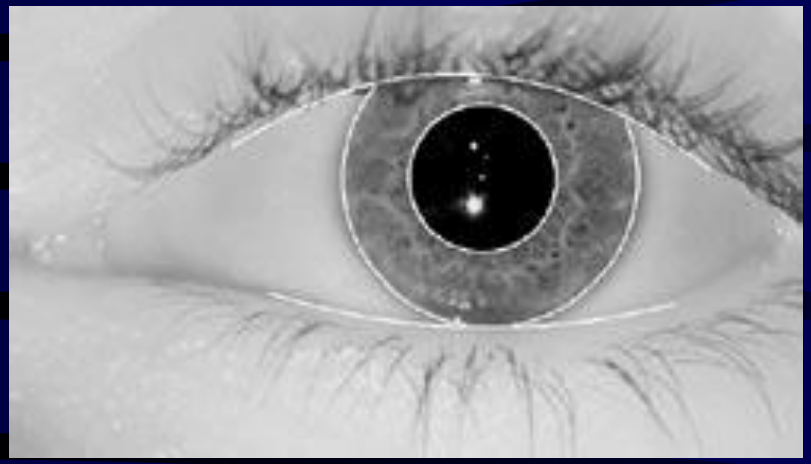
Применение биометрических технологий на горизонтальном и вертикальном рынках

Технология	Горизонтальный рынок	Вертикальный рынок
Распознавание отпечатков пальцев	Идентификация гражданского населения	Правительственный сектор
Распознавание лица	Наблюдение и проверка	Туризм и перевозка грузов
Распознавание радужной оболочки глаза	PC/сетевой доступ	Финансовый сектор
Сетевая защита	Розничная торговля/ATM/пункты продаж	Здравоохранение
AFIS*	Электронная коммерция/телефония	Правовой сектор
Распознавание голоса	Физический доступ/присутствие и время	
Распознавание геометрии руки	Идентификация преступников	
Верификация подписи		
Распознавание клавиатурного почерка		

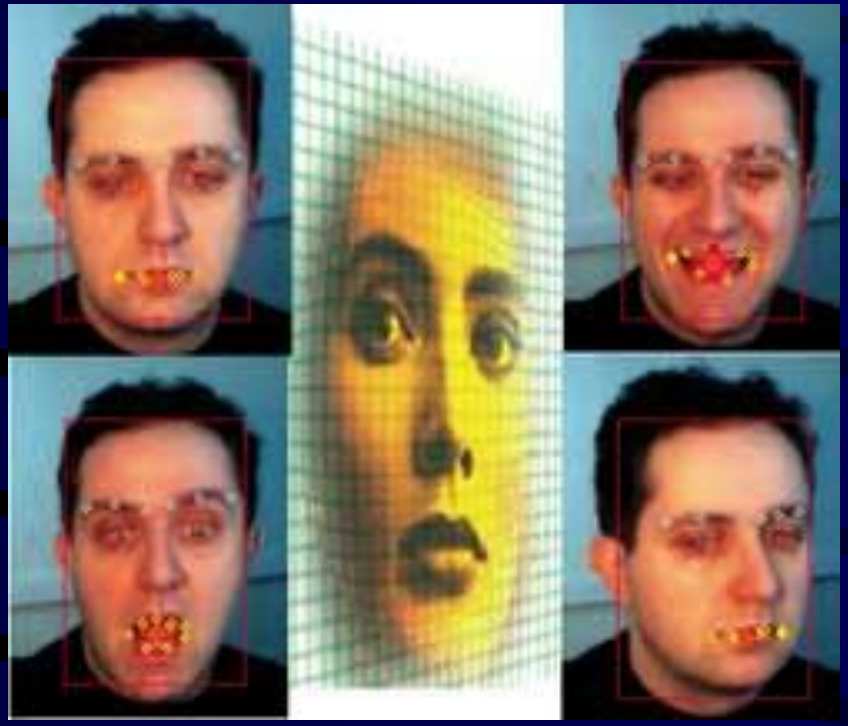
*AFIS — Automated Fingerprint Identification System — наиболее широко распространенное биометрическое приложение

Распознавание по отпечаткам пальцев





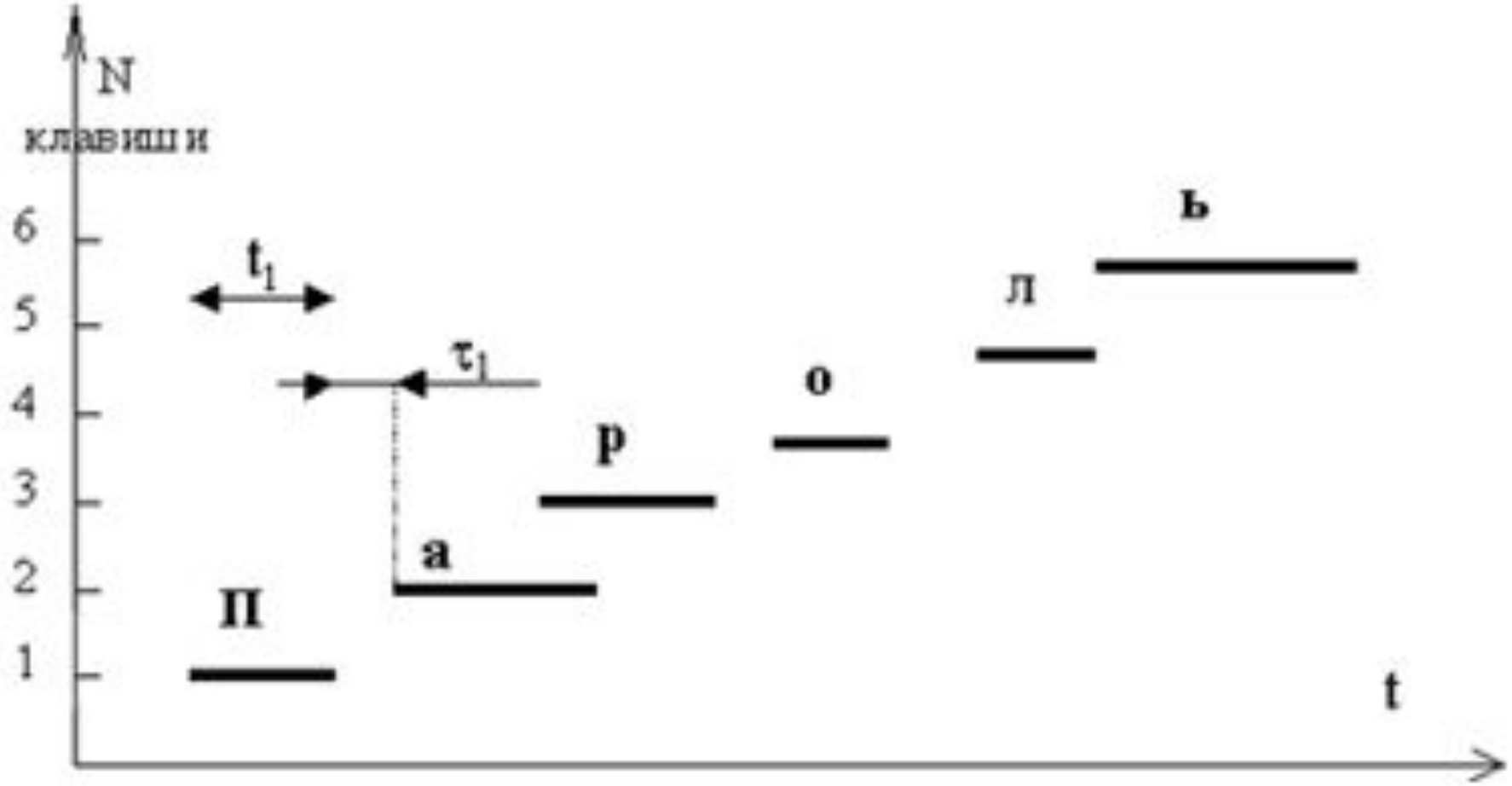
Распознавание по радужной оболочке глаза и по сетчатке глаза



Распознавание по геометрии лица

Электронный считыватель жестов

Временная диаграмма ввода слова «пароль»



Зрелость технологий защиты информации

Структура затрат на безопасность

САМАЯ СТРАШНАЯ

ФРАЗА ШКОЛЬНОГО ДЕТСТВА:

„ТАК, А ТЕПЕРЬ УБИРАЕМ УЧЕБНИКИ И ДОСТАЁМ ДВОЙНЫЕ ЛИСТОЧКИ..."

Вопросы по теме

1. Что понимается под информационной безопасностью? Каковы ее критерии?
2. В чем отличие традиционных и компьютерных этических правил? Приведите примеры нарушений авторского права. Как избежать плагиата?
3. Что представляет собой контрафактное (пиратское) ПО. Каково Ваше отношение к данной проблеме?

Что такое спам и спам-боты? Каковы их особенности в Рунете?

4. Что представляют собой вирусы и кто такие вирусописатели? Какие цели они преследуют?
5. Назовите и охарактеризуйте социально опасные этические нарушения в использовании электронной почты и веб-сайтов. Приведите примеры киберсквоттинга, атак, социального инжиниринга.
6. Что представляют собой биометрические системы распознавания пользователей? Как они используются в системах контроля доступа?