лекция 5

Долговечность электронных ресурсов, некоторые виды правонарушений, типичных для информационной деятельности, информационная безопасность

январь 2010 г.

Девиз лекции - Abusus non tollit usum

(возможность неправильного пользования не отменяет использование)

План лекции :

1) Долговечность носителей информации
2) Меры по обеспечению сохранности ресурсов
3) Нецелевое использование
4) Вирусы
5) Спам
6) Хакерство и фишинг
7) Судебные случаи
6) Информационная безопасность.

Сравнение долговечности различных видов ресурсов

Печатные ресурсы;

жалобы на недостаточную прочность бумаги, изготовленной начиная со второй половины 19-го века.

Повышение хрупкости под влиянием остатков кислот, используемых при производстве бумажной массы из древесных щепок.

Разработаны специальные технологии деацидификации (устранения излишней кислотности). Обсуждая проблемы архивации, библиотечные работники ссылаются на долговечность бумажных документов. «Что написано пером, не вырубишь топором».

Электронные ресурсы;

носители разрабатывались с учетом их массового использования и меры по обеспечению их физической сохранности были заложены в спецификации технологии производства.

Можно сравнить CD-ROM с книгой, каждая страница которой защищена слоем прозрачной и очень прочной пластмассы. Такие ламинированные страницы обеспечивают надежное сохранение информации.

Но в целом нужно помнить, что одновременное соблюдение всех технологических требований (долговечность в сочетании с удобством перезаписи) нереально, поэтому приходится оптимизировать, искать баланс.

По гибкости, простоте внесения изменений, цифровая запись ближе к устной речи, чем к традиционным печатным публикациям; заметим еще раз, что речь идет не о физической сохранности материального носителя информации.

Устные ресурсы

Несмотря на кажущуюся изменчивость отдельно взятого высказывания, своеобразным гарантом сохранности устной речи является коллективная память слушателей.

Правда эта память неустойчива и способна допускать произвольные дополнения и украшения, тем не менее, «слово не воробей, вылетит – не поймаешь».

Угрозы надежности хранения информации:

1) Физическая порча или гибель (срыв электропитания, поломка сервера, пожар, наводнение и т.п)

2) Внутренние нарушения (воровство, нарушение технологии);

3) Вмешательство извне (взлом сайта хакерами, проникновение вирусов, обычное воровство);

4) Миграция, то есть изменения в аппаратно - программных средствах хранения и обеспечения доступности ресурсов.

Меры защиты от физической порчи или гибели (срыв электропитания, поломка сервера, пожар, наводнение и т.п):

- бесперебойное питание;
- “горячее резервирование”;
- разумное содержание библиотечных серверов;
- создание технологических и страховых резервных копий.

Обеспечение долговременной (на срок порядка нескольких столетий) сохранности электронных материалов.

1. Принцип сохранения электронных документов в виде их печатных копий (принцип «распечатывать все») не может приниматься всерьез ввиду нереальности.

Неразумным было бы пытаться сохранить в библиотеке все физически ощутимые носители (будь это дискеты 5,25 дюймов или 3,5 дюйма или CD-ROM или другие) и соответственно старые компьютеры и устройства ввода-вывода. Это означало бы превращение библиотеки в музей технических древностей, да и откуда возьмутся специалисты по их обслуживанию?

Перезапись («освежение», refreshing), - периодическое многократное перенесение электронных ресурсов на современные носители. С технической стороны этот метод выглядит безупречно, поскольку полностью сохраняется первичная информация. Сложность в том, что никогда не узнаешь заранее, пора ли приступать к перезаписи или можно еще подождать. Кроме того, некоторые документы могут быть изначально защищены от перезаписи по соображениям авторского права. Конечно, следует обновлять и копии соответствующего прикладного программного обеспечения – иначе все окажется напрасным, документы утратят читаемость.

Миграция, в данном случае – конверсия электронных ресурсов в новую аппаратно-программную среду. Данная технология выглядит жизнеспособной и широко применяется, например конверсия документов, записанных с помощью текстового редактора Word Perfect 9, в формат Word 2000 XML. Легко и без потерь качества осуществляется конверсия из простого формата в более высокоразвитый.

Обратный переход (например из формата, используемого для записи математических формул LaTex в простой текстовый формат) может оказаться очень трудоемким, требующим массу ручной работы.

В некоторых случаях вообще невозможно говорить о конверсии ввиду трудоемкости или дороговизны процесса, например для документов, представляющих собой записанные в бинарном коде компьютерные программы. Столь же нелегким делом может оказаться конверсия баз данных, их необходимо будет конвертировать сначала в текстовый файл, а уж затем загружать в новую оболочку. При этом, например, для библиографических данных обменный формат ISO 2709 не полностью передает все детали записи формата MARC и приходится делать небольшие доработки, которые при огромном количестве записей выливаются в довольно большие затраты ручного труда.

Эмуляция. В 1995 году консультант европейского отделения компании RAND Джеф Розенберг опубликовал в журнале Scientific American предложение обеспечивать долговременную сохранность электронных документов методом эмуляции, то есть разработки программ, которые воспроизводят копии старого программно-аппаратного обеспечения в новых условиях, на новых технических средствах.

В памяти нового мощного компьютера хранятся сами ресурсы и подробная информация, описывающая те средства, на которых они в свое время воспроизводились.

Для эмуляции требуются очень точные описания оборудования и программ (спецификации), но в ряде случаев все это имеется и, например, процессор Transmeta вполне успешно воспроизводит процессор Intel, а эмуляторы системы MAC воспроизводят систему Windows. Цифровой архив на базе эмуляторов будет довольно неудобным в пользовании, поскольку придется надстраивать их «один над другим» по мере внедрения новых видов оборудования и программ.

Считается, что объем хранимых в мире данных удваивается каждый год.

Соответственно сложность администрирования хранилищ растет экспоненциально.

Тем более что уже высказывается мнение: хранить нужно все, имеющее хоть малейший шанс когда-нибудь пригодиться.

Следовательно, одной из основных задач новой технологии является упрощение администрирования больших объемов данных.

Меры защиты от внутренних нарушений (воровство, нарушение технологии);

- Создание технологических и страховых резервных копий (служебная копия и страховая копия);
- Авторизации в предоставлении доступа к системам хранения документов и данных в ЭБ, а также доступа к архивам.

Виртуализация

Создание хранилищ данных, изолированных от пользователя, который может отправлять данные на хранение и получать их по мере надобности, не вникая, где именно данные находятся и что с ними в процессе хранения происходит.

Можно сравнить виртуализацию с электричеством, которое добывается путем включения прибора в розетку, а не вращением педалей динамо-машины, а также с финансовыми институтами, куда можно сдать деньги, а затем получить их обратно.

Несмотря на то что свет иногда отключается, а банки разоряются, никто не планирует полностью отказаться от коммунальных услуг и перейти на более надежную керосиновую лампу и примус, да и финансовые институты тоже не демонстрируют признаков всеобщего упадка.

Некоторые примеры злонамеренных действий :

- - Вредительство сотрудников компании («своих»);
- - Несанкционированный доступ и порча со стороны «чужих» (хакерство)
- - Зловредные программы (вирусы, троянские кони, черви), быть может, направленные не специально вам во вред, но тем не менее наносящие ущерб.

Неблаговидные действия администраторов сети (например, изменения конфигурации сетевого оборудования и т.п.), обиженных на руководство компании или подкупленных конкурентами(врагами).

Организация внутреннего цифрового телевидения для контроля доступа к компьютерам; контроль содержимого и адресов.

Нецелевое использование сетевых компьютеров сотрудниками библиотеки или пользователями библиотеки (80% сотрудников передают личные сообщения с рабочего места).

Посещение серверов, не нужных для работы в офисе :

33% Интернет-пользователей не имеют четких целей;

28 % совершают покупки в Интернет не покидая рабочего места;

объем порно трафика в рабочее время (с 9-00 до 17-00) составляет 70%.

Валерий Кодачигов Интернет на работе временно недоступен Коммерсант № 193/П 22.10.2007 с. 19

Самым быстрорастущим сегментом рынка информационной безопасности в 2007 году стали системы блокировки корпоративных каналов связи — их продажи выросли на 136%, до $26 млн.

В стремлении повысить производительность и не допустить утечек работодатели все чаще ограничивают коммуникационные возможности своих сотрудников, внедряя специальные системы.

Их не останавливает даже то, что до 50% внедрений таких систем проходит неудачно

Компания LETA опубликовала прогноз развития российского рынка информационной безопасности, (основанный на исследованиях IDC, PricewaterhouseCoopers, Gartner и ряда других) По итогам 2006 г весь российский рынок защитных систем составил $700 млн. Самым быстрорастущим сегментом рынка стал ILDP (Information Leakage Detection and Prevention) — система защиты от утечек инсайдерской информации.

Такие системы позволяют автоматически контролировать и блокировать переписку сотрудников компаний по e-mail и через интернет-мессенджеры, запрещать доступ к интернет-ресурсам и определенным устройствам (например, сетевым принтерам и пишущим CD-ROM).

Внедряя ILDP-системы, работодатели зачастую стремятся не столько ограничить утечки, сколько повысить производительность труда. «В рунете возникло отдельное направление сайтов, целевая аудитория которых—сотрудники офисов. Это такие ресурсы, как, например, „Одноклассники.ру", anekdot.ru,— рассказывает зам. генерального директора NVision Group Сергей Головин.— Они, как и ICQ, отвлекают сотрудников. Естественно, при этом через различные форумы часто сливается конфиденциальная информация».«Как показывает опыт, только блокирование у отдельных групп сотрудников ICQ. и доступа на нежелательные ресурсы повышает производительность труда на 40-50%».

Опрошенные сотрудники российских компаний и банков подтвердили, что их работодатели в той или иной мере ограничивают их доступ к средствам связи и информационным ресурсам. О том, что на их рабочих местах блокируется ICQ рассказали в консалтинговых компаниях «Вимм-Билль-Данн», KPMG и Ernst&Young. При этом блокируется доступ ко всем некорпоративным почтовым ящикам». На компьютерах большинства сотрудников компании установлена блокировка доступа к сайтам, которые не требуются им для работы, таким, к примеру, как mamba.ru. «Наша система безопасности гибкая и позволяет дать тем или иным сотрудникам доступ к ICQ или отдельным сетевым ресурсам. Но для этого требуется согласие руководства.

Горсовет Лос-Анджелеса озаботился следующей проблемой: враждующие кланы игроков в Counter Strike (многопользовательская игра, имитирующая боевые действия) перешли от выяснения отношений на виртуальном поле боя к вполне реальному насилию. Стычки между посетителями киберкафе стали обычным делом. Выяснилось, что 86% драчунов — подростки и 93% арестов нарушителей порядка произведены в то время, когда хулиганам полагалось находиться в школе. Вследствие чего муниципалитет и принял закон. Контролю подлежат 30 городских киберкафе, полиции разрешено там проводить проверки, а хозяева заведений вправе требовать у посетителей доказательств того, что им уже исполнилось восемнадцать

Внешние угрозы.

Несанкционированное проникновение в систему (хакерство, взлом сетей государственных и финансовых учреждений); воровство номеров кредитных карт; нарушение конфиденциальности массивов персональных данных.

Создание системы «Социальной обработки» Social Engineering по выпытыванию из людей закрытой информации, действия в духе Остапа Бендера.

Наличие в сети Интернет бесплатных программ для организации хакерских атак.

Вирус компьютерный.

Программа, без ведома пользователя внедряющаяся в компьютеры и производящая там различные несанкционированные действия, создание дубликатов или новых видов вирусов. Вирусы портят файлы, проигрывают мелодии, уничтожают данные на микросхемах. Известно более 55 тысяч вирусов. Классификация вирусов по : среде обитания; операционной системе; особенностям алгоритма.

Например, вирус «Чернобыль» - файловый резидентный неполиморфный Windows вирус.

Черви и кони не могут размножаться.

Червь распространяется по сетям, не прибегая к размножению. Вместо этого зловредная программа рассылает свой оригинал, например по электронной почте.

Троянские кони лишены функции распространения; они попадают в компьютер с помощью своих авторов или лиц, незаконно их использующих. Троянские программы имеют полезный или завлекательный вид; после запуска файла эти программы незаметно активируют нежелательные действия, например, могут следить за посещениями «хозяина» и отсылать полученную информацию автору коня.

Мутанты: мелисса (Melissa) – макровирус, шел по сетям как червь. Вирус часто прячется под внешне приветливой и безобидной оболочкой :

“I love you” - автоматическая рассылка признания в любви по всем имеющимся адресам заразил 3,1 млн. компьютеров и нанес ущерб в 2000 г. 15 млрд. долларов.

Вирус Navidad, - С новым Годом ! желающий всем счастливого Нового Года;

Вирус, спрятанный в фотографию Анны Курниковой;

Вирус Code Red; Борьба с терроризмом (Мир между Америкой и исламом, - вирус w32.vote).

Парадоксом является лавинообразная рассылка писем – предупреждений об вирусах (например, самых новых - California IBM, Girl Thing).

Евгений Касперский, руководитель известной антивирусной лаборатории, считает, что возможна мистификация в этих вопросах.

Сотовым телефонам угрожают новые вирусы, обнуляющие счета абонентов, «инфекцию» может подхватить любой мобильник, работающий на платформе Java. Чтобы вредоносная программа не «пробралась» в телефон, ее просто не нужно запускать.

Обычно «заражение» происходит следующим образом: пользователь скачивает из Интернета вирус, «прикидывающийся» какой-нибудь программой для телефона (чаще всего игрой), и устанавливает его на свою «трубку». После этого «больной» телефон начинает рассылать SMS-сообщения на платные номера, и счет абонента моментально обнуляется. Или — в случае кредитной системы оплаты—уходит в глубокий минус. Причем настолько глубокий, что практически разоряет абонента. Ведь стоимость платных SMS-сообщений может достигать $ 5—6, а отправляются они непрерывно. Вот и представьте, сколько денег может «сожрать» вирус, пока пользователь не заметит.

Главная проблема — обычные телефоны (в отличие от смартфонов) невозможно оснастить антивирусной защитой. Поэтому такой аппарат просто не может самостоятельно идентифицировать и удалить вредоносный софт.

Обнаружить его можно лишь на компьютере, куда первоначально закачивается «вредитель», — с помощью антивируса.

Но пользователи часто беспечно относятся к «телефонным» файлам и не проверяют их.

Вылечить «зараженную» трубку, как правило, не удается. Вирус «перепрошивает» мобильник, делая его непригодным для дальнейшего использования.

Заметим, что «вредители» попадают в телефон не только через компьютер.

Иногда они приходят «по воздуху» — через MMS или Bluetooth. Причем последний вариант более распространен, так как не требует от злоумышленника расходов — достаточно установить на телефоне (или переносном компьютере) программу, рассылающую «вредителя» всем мобильникам в радиусе 100 метров (иногда до 1 км).

Но просто отправить вирус через Bluetooth недостаточно. Нужно, чтобы пользователь его запустил, а добиться этого гораздо сложнее.

Отдадим должное креативности киберпреступников — иногда им удается убедить человека добровольно загрузить «вредителя».

Приведем пример. Человеку на стадионе приходит сообщение на телефон: «Вы выиграли билет на следующий матч. Установить приложение?»

В другой— более спокойной—ситуации пользователь наверняка бы заподозрил подвох и просто стер послание. Но разгоряченный зрелищем болельщик может запросто нажать «ОК» и загрузить зловредную программу.

Как обезопасить свой телефон? Во-первых, не следует держать Bluetooth постоянно включенным. Особенно в местах массового скопления людей (в метро, на стадионах, на улице). Во-вторых, категорически нельзя настраивать телефон на автоматическое открытие пришедших сообщений — в этом случае «инфекция» попадет в мобильник со стопроцентной гарантией.

Что же касается MMS-сообщений (в России не распространены), то открывать их можно только в том случае, если отправитель вам знаком и вы ему доверяете.

Коммерсант среда 29 марта 2006 №54 , с. 20 Дмитрий Попович директор по маркетингу российского представительства Esef «Технологии становятся опаснее» Интервью взял Валерий Кодачигов

Количество новых вирусов не увеличивается и не уменьшается — опаснее или безопаснее информационная среда не становится. Большие опасения вызывает другое. Мировая ГГ-инфраструктура постоянно растет. В нее интегрируются все новые устройства — мобильные телефоны, бытовая техника и электроника, корпоративные информационные системы. Во всем постиндустриальном мире развиваются сети беспроводного доступа Wi-Fi и WiMAX. Соответственно, растет количество достойных мишеней для хакеров и вирусописателей. Самое неприятное, что об уязвимых местах в относительно новых информационных системах пока ничего не известно.

Ситуация усложняется тем, что характер потенциальной опасности неизвестен. Тут антивирусным компаниям приходится, что называется, играть на опережение. Это оказывает прямое влияние на рынок антивирусного ПО. Чтобы застраховаться, корпоративные пользователи теперь все чаще стремятся устанавливать софт не одного производителя, а нескольких. Естественно, это ведет к росту объемов продаж.

В чем специфика российского рынка антивирусных программ? Существуют ли у российских потребителей какие-либо специфические проблемы и запросы?

Специфических угроз для российских пользователей нет, поскольку нет программного обеспечения, созданного специально для России Российские информационные системы атакуют вредоносные программы, распространенные во всем мире. Специфичны не вирусы, а рынок антивирусных средств. Основная его особенность — присутствие сразу многих игроков местных, европейских, американских. Этим ситуация отличается от той, которая складывается, допустим, в Европе. В каждом крупном государстве Евросоюза есть производитель, который контролирует львиную долю рынка. В России же между антивирусными компаниями идет конкуренция.

Тем не менее одна характерная черта у российского софтверного рынка есть —это пиратство. Насколько сильно оно влияет на развитие бизнеса антивирусных компаний в России?

Пиратство действительно негативно влияет на софтверный рынок. Но в случае с антивирусными компаниями его уровень не очень велик. Мы, как и конкуренты, стараемся защищать свою продукцию специальными ключами, кодами и другими средствами. Кроме того, покупать пиратскую версию антивирусной программы не всегда целесообразно. Главное в таких системах — постоянные обновления, а пираты зачастую их обеспечить не могут.

Как меняется круг пользователей антивирусного ПО в России? Какие ниши рынка наиболее перспективны с точки зрения такого софта?

В ближайшее время спрос на антивирусы и другие средства информационной безопасности будет формировать не только коммерческий сектор — традиционный потребитель, но и государство. Масштабные IT-проекты, под которые из бюджета выделяются десятки миллиардов рублей — такие, к примеру, как введение в России биометрических паспортов. Для использования в госпроектах ПО иностранных производителей должно проходить сертификацию в Гостехкомиссии. Как правило, западные компании испытывают при этом сложности.

Нам выгоднее сейчас просто продавать наши продукты на российском рынке. Конечно, высокая квалификация российских программистов известна давно.

Однако в России сейчас растут зарплаты ИТ-специалистов.

В крупных городах России услуги программистов уже сейчас стоят дороже, чем услуги индийских, китайских, а порой и европейских коллег.

антивирусные программы, используемые российскими предприятиями* источник: romir monitoring. *(некоторые компании используют сразу несколько антивирусных программ.)*

Dr. Web 35%

Symantec/Norton Antivirus 33%

McAfee 9%

Eset Nod32 9%

Panda Antivirus 7%

Trend Micro 7%

«Антивирус Касперского» 60%

Правила безопасного поведения в сети и правила реагирования на опасность.

Полезно:

- применять средства активной защиты (динамический мониторинг и подавление подозрительной активности); вести и регулярно анализировать протоколы работы серверов;
- не утаивать факты нападения и максимально активно противодействовать компьютерным атакам, всегда пытаясь выявить нападающего и привлечь его к административной или уголовной ответственности.

Правила безопасного поведения в сети и правила реагирования на опасность.

Полезно: сотрудничать с юридическими фирмами и международными организациями, занимающимися безопасностью (хакер может физически располагаться в любой стране мира);

Полезные адреса сайтов, содержащих предупреждения об уязвимых точках программного обеспечения и о новых вирусах и способах их устранения :

securityfocus.com xforce.iss.net cert.org

На сайте некоммерческой организации MITRE (www.mitre.org) ведется так называемый CVE-список (Common Vulnerabilities and Exposures) названий общеизвестных системных уязвимостей и недостатков в различных ОС и ПО. Хакеры пытаются проникнуть в систему, пользуясь прежде всего этими лазейками.

Компания “Диалог наука” (www.virusbtn.com) предоставляет в аренду за 1 долл в месяц антивирусные программы Doctor web и Adinf;

программа Doctor web 4.27 (автор – Игорь Данилов, СПб) завоевала медаль журнала Virus Bulletin VB100%.

на тех же примерно условиях предоставляется и облегченная версия антивируса AVP Lite компанией “Лаборатория Касперского”.

Сравнение антивирусных программ :

Корпорация Symantec, программа Norton Antivirus - нет русской версии, сложности с обновлением через Интернет и нужно платить

- Лаборатория Касперского, программа AVP, - сложная в настройке
- Компания "Диалог - Наука», программа Doctor Web, - медленный запуск из-за полномасштабного сканирования системной памяти

Внутренняя система обнаружения атак - мониторинг системных и сетевых ресурсов на предмет некорректной, неуместной или аномальной деятельности и уведомление администраторов сети. Антивирусная обработка компьютера в автоматизированном режиме или по заказу.

Убедиться в принципиальной доступности компьютера для вторжения извне очень легко:
достаточно, к примеру, посетить Web-сайт корпорации Symantec и протестировать уязвимость своей системы (бесплатная услуга).

Контроль уровня защиты через систему автоматических агентов, устанавливаемых на каждом хосте и собирающих информацию по 1500 параметрам.

Искусственная имитация хакерских атак с целью нахождения уязвимых мест.

В качестве профилактической меры можно воспользоваться прокси-серверами (серверы, которые хранят актуальные копии данных, принадлежащих другим узлам, — в локальных сетях таким образом можно существенно уменьшить нагрузку на внешний канал передачи данных) или даже цепочкой прокси-серверов. В этом случае реальный iP-адрес вашего компьютера уже никакая программа-взломщик не увидит.

Второй вариант — установить программный межсетевой экран, эффективно блокирующий попытки доступа к памяти вашего компьютера.

Специалисты высоко отзываются о серии Personal Firewall корпорации Symantec и BlackICE Defender компании network ICE.

Бесплатно распространяемый межсетевой защитный экран Zone Alarm на сайте (www.zonelabs.com) блокирует утечку конфиденциальной информации и поступление распространенных видов мусора – спам

Спам - это рекламные письма с предложением купить "горящую" турпутевку или зайти на ""бесплатный" семинар, в худшем случае - огромное количество мусорного трафика, в котором нередко скрываются вирусы. Каждый день спамеры отправляют около 30 млрд. сообщений - эта проблема представляет собой крупномасштабную угрозу функционированию электронной почты и безопасности компьютеров.

Доля спама в общем объеме корреспонденции неуклонно растет. Если в 2003 году она составляла 50%, то в 2004-м достигла 60%. В 2005-2006 годах спамеры создавали уже 70-80% почтового трафика.

По данным калифорнийского исследовательского института Ferris Research Institute, мировой убыток от спама в 2005 году составил $51,1 млрд. В эту сумму входит стоимость трафика, а также рабочего времени сотрудников, потраченного на ознакомление со спамом либо устранение последствий спама.

Всего за год издержки, связанные со спамом, во всем мире возросли более чем на 500%.

По мнению российских специалистов, в нашей стране проблема спама имеет примерно те же масштабы, что и в странах ЕС.

В 2005 г. более 90% писем российского сектора Интернет содержали спам.

«Размеры спама в России сопоставимы с европейскими, 70-80% писем, которые получают россияне,— спам,— отметил директор по маркетингу компании InfoWatch Денис Зенкин.— Эту проблему надо решать на государственном уровне, в первую очередь необходимо обязать провайдеров внедрить систему защиты.». По оценкам г-на Зенкина, спам ежегодно наносит российской экономике ущерб в размере не менее $100 млн.

Спам – гораздо более массовый и доступный бизнес по сравнению с вирусописательством.

Спамер управляет своими рассылками лишь с одного компьютера, с помощью которого он контролирует множество других, зараженных троянами – рассыльщиками.

Массовые рассылки по электронной почте:
905 000 email адресов "Фирмы Москвы" 3500 руб.
5 937 000 email адресов "Физические лица Москвы" 10 000 руб/всё; 3 500руб/1 млн.
6 842 000 email адресов "Вся Москва" 12 000 руб.
6 101 000 email адресов "Фирмы России" 10 000 руб. /всё; 3 500руб /1 млн.
9 840 000 email адресов "Физические лица России" 18 000руб /всё; 3 500руб /1 млн.
15 941 000 email адресов "Вся Россия" 25 000 руб.
350 000 email адресов "фирмы Санкт-Петербурга" 3500 руб.
1 240 000 "физические лица Санкт-Петербурга" 5500 руб.

Переезд для Всех

Наша компания рада предложить Вам услуги по: квартирным, офисным и складским переездам. В нашей компании работают исключительно квалифицированные грузчики-славяне!

Обращаясь к нам, Вы получаете качественный переезд по разумной цене! На данный момент действуют сезонные скидки!

Также у нас Вы можете заказать различный вид транспорта для перевозки вашего груза. Мы работаем по Москве, МО и другим регионам России! Заключаем договора на постоянное сотрудничество.

Звоните и мы будем рады Вам помочь!

518-58-47, 517-25-04

Массовые рассылки очень эффективны по соотношению цена/качество, цены 2005 г. – 100 долларов за два миллиона сообщений.

Несмотря на то что 99,9% получателей сразу же удаляют рекламное сообщение, всегда остается 0,1% - 0,2% людей, которые внимательно прочитают и "клюнут" на предложенное. Этот процент окупает все расходы, потраченные на рассылку При базе в 1 млн адресов среагируют 1 - 2 тыс пользователей. Крупные российские спамеры зарабатывают до 2 млн долларов в год.

По данным компании Sophos, российские спамеры по количеству рассылок заняли второе место в мире, уступая только ~~американцам. Сейчас с российских адресов~~ исходит 8,3% несанкционированной e-mail-рекламы.

В 2007 г. российские спамеры заработали $13-15 млн, при этом, по оценкам компании «Ашманов и партнеры», они нанесли российской экономике ущерб в размере $500 млн (в первую очередь эти убытки связаны с вынужденным простоем персонала компаний, читающего и удаляющего спам, а также с оплатой интернет-трафика).

Термин SPAM появился в 1937 г. — так назывались свиные консервы компании Horne Foods (Shoulder of Pork and Нам — "свиные лопатки и окорока"). Консервы рекламировались в Америке крайне назойливо.

В 1986 г. в конференциях Usenet появилось множество одинаковых сообщений от Дэйва Родеса, который рекламировал новую финансовую пирамиду.

Современный спам ведет свое начало от direct mail — массовой рассылки обычных, бумажных писем, в которых отправляли адресную рекламу в Европе и США до середине 90-х.

Популярным термин "спам" стал в 1993 г., когда Ричард Депью написал программу для автоматического моделирования конференций Usenet и из-за ошибки в коде она вместо удаления одного сообщения продублировала его 200 раз. Свалившиеся в больших количествах письма окрестили спамом, и через несколько лет. когда это явление стало частым, слово прочно заняло свое место в компьютерном лексиконе. В 1995 г. Сэнфорд Уоллэс, самопровозглашенный король спама, вместе со своим партнером Уолтом Райнсом основал компанию Cyber Promotions, специализирующуюся на рассылке рекламы по e-mail. Компания быстро заняла лидирующие позиции в этой области, став заодно главным поставщиком адресов для остальных спамеров.

Уоллэс не просто зарабатывал на спаме деньги, он создавал новые приемы обхода фильтров и технологии, позволяющие повысить эффективность рассылок. Фальшивые обратные адреса, ретрансляция, множественная адресация —были изобретены в его компании и впоследствии использовались ведущими спамерскими конторами.

В конце 90-х широкую известность получил Алан Ральский — сетевые аналитики считают его самым плодовитым спамером в истории. Начав с незаконного страхования (на чем в 80-х он зарабатывал 500 тыс. долл. в год), он попался на фальсификации банковских документов и начал новый "бизнес" в Сети.

С ним получатели спама расквитались — один пользователь вычислил почтовый адрес Ральского и распространил его в Интернете. Тысячи компьютерщиков отправились искать в сети фирмы, рассылающие бумажные рекламные проспекты, бесплатные каталоги и прочую макулатуру. В графе "кому" они вводили адрес Алана, и все это добро свалилось на спамера. История закончилась в 2005 г., когда агенты ФБР нанесли визит в дом 60-летнего спамера и по решению суда конфисковали всю компьютерную технику, включая несколько мощных серверов и его финансовые документы. Ральский контролировал около 200 mail-серверов, каждый из которых мог отправлять 650 тыс. рекламных писем в час.

В 2000-х годах борьба со спамом перешла на качественно иной уровень — важно было не только предотвратить массовую рассылку почты, но и сделать это максимально оперативно. К примеру, одна спам-рассылка могла быть доставлена миллионам пользователей по всему миру за 20—50 мин. Объектами скоростных атак чаше всего являлись серверы бесплатных почтовых служб.
Классическое построение обороны:

на первом месте определение спама по IP-адресам отправителя,

далее — контроль массовости рассылки повторяющегося сообщения,

на последнем месте — многочисленные фильтры.

Основная сложность борьбы состоит в том, что спамеры защищают свои письма, маскируя их содержание, к примеру, с помощью технологии внесения случайных текстов, "шума", невидимых текстов. Для этого в начало или конец письма спамер может поместить отрывок из классического текста или просто случайный набор слов, а в HTML-сообщение можно внести "невидимый" текст (очень мелким шрифтом или цветом, совпадающим с цветом фона). Эти добавления затрудняют распознавание спама методом нечетких сигнатур и статистическими методами. В качестве ответной меры появился поиск цитат, устойчивый к дополнениям текстов, детальный разбор HTML и другие методы углубленного анализа содержания письма.

Есть графические письма — рекламное сообщение можно прислать пользователю в виде графического файла, что крайне затруднит автоматический анализ. В качестве ответной меры появляются способы анализа изображений, выделяющие из них текст. Изменяющиеся графические письма — более продвинутая технология, в графическое сообщение можно внести "шум", что затруднит его анализ фильтром. Есть и перефразировка текстов — одно и то же рекламное сообщение составляется во множестве вариантов. То есть каждое отдельное письмо выглядит как обычный связный текст, и только имея много копий сообщения, можно установить факт перефразировки. Таким образом, эффективно настроить фильтры можно только после получения существенной части рассылки.

Одним из наиболее одиозных в 2003—2004 гг. стал Вардан Кушнир — автор известного в Рунете спама от "Центра изучения Американского английского". За год предложение изучить язык получили более 25 млн. человек в России, на Украине, в Израиле и даже США. Рекламируемый центр языкознания настолько вывел из себя рунетчиков, что на борьбу со спамером вышли тысячи людей. Одни названивали по оставленному в письмах телефону и бранили операторов или интересовались одними и теми же подробностями, другие проводили DDoS-атаки на сайт конторы.

В 2005 г Вардан Кушнир был найден с многочисленными ранами на голове, одна из которых оказалась смертельной.

Был ли Кушнир убит доведенными до бешенства пользователями Рунета, осталось неизвестным, но рассылка спама от «Центра американского английского» прекратилась.

Из-за действий главного спамера России некоторые зарубежные mail-серверы блокировали поступление любых писем из домена .ru, что сделало невозможным переписку людей, живущих в разных странах.

Против Центра выступили власти — записанное обращение тогдашнего первого заместителя министра связи Андрея Короткова с требованием прекратить рассылку провайдер Golden Telecom непрерывно прокручивал по телефонным линиям Центра.

Развитые в технологическом плане страны стали понимать, что спам представляет собой явление, не менее опасное, чем вирусы. Во многих из них массовые рассылки электронных писем были признаны вредоносным явлением и караются весьма сурово: от громадных штрафов до реального тюремного заключения.

К примеру, в США с декабря 2003-го действует CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act) , в котором прописаны стандарты и ограничения на рассылку коммерческих сообщений. Именно этот документ является в настоящее время базой, с помощью которой власти сражаются с отправителями массовых рассылок

4 ноября 2004 г. за многочисленные нарушения этого документа суд приговорил Джереми Джеймса, одного из самых влиятельных спамеров в Интернете, к девяти годам тюремного заключения. А самым первым спамером, которого отправили в тюрьму, стал Говард Кармак, который в 2003-м разослал 25 млн. рекламных сообщений. Так как американский закон о нелегальности спама в то время еще не вступил в силу, Кармака судили за фальсификацию документов и назначили максимально возможный срок — семь лет

Новая редакция закона российского закона "О рекламе" определяет порядок распространения рекламы по сетям электронной связи.

Управление Федеральной антимонопольной службы (УФАС) по Пермскому краю оштрафовало предпринимателя Кирилла Гуреева на 5 тыс. руб. за не санкционированную рассылку e-mail. В действиях Гуреева пермский УФАС усмотрел нарушение части 1 статьи 18 закона «О рекламе», которая запрещает рассылку рекламы по сетям электросвязи без предварительного согласия адресата или абонента на ее получение. За нарушение этого пункта закона полагается штраф в размере 4-20 тыс. руб.

Дело было возбуждено по заявлению директора пермской web-студии «Жанр» Кошина. Он пожаловался на то, что на его фирму стали приходить несанкционированные e-mail с рекламой багетной мастерской и некоей «Фабрики e-mail». «Фабрика», предлагала организацию рекламной спам-рассылки по предприятиям Перми и Пермского края.

Несколько дней господин Кошин писал спамерам ответные письма с просьбой прекратить рассылки, но отправители рекламы никак на них не отреагировали. Тогда он обратился в УФАС, и после трехмесячного расследования привлекло спамера к административной ответственности.

Сам Гуреев утверждает, что разослал рекламные объявления только один раз «по незнанию». Представители УФАС утверждают, что рассылки носили массовый характер: было установлено, что спам рассылался по 7,5 тыс. адресам.

То, что государство в лице ФАС начало борьбу со спамом, сейчас показательно: Россия вошла в число мировых лидеров по спам-рассылкам

Некоторые компании (Microsoft) для истребления спама предлагают вводить плату за отправление каждого сообщения. Символическую для частных лиц, но внушительную для спамеров, которые отправляют письма миллионами, — что-то вроде почтовых марок. Но спамеры используют для рассылки писем компьютеры конечных пользователей, а потому ничто не помешает им в будущем возложить на них и плату за отправление сообщений.

Наибольшее количество писем со спамом посвящено компьютерному мошенничеству.

Доля спама стабилизировалась на достаточно высоких показателях (до 80% от всего почтового трафика), и показатели эти уже слабо подвержены влиянию внешних факторов, например региональных праздников. Однако есть шанс снизить долю криминализированного спама — рассылок, которые могут содержать вирусы и другие вредоносные программы (в том числе троянцы), опасные для клиентских компьютеров и сетей компаний. В этой связи встает вопрос об усилении антивирусной профилактики и внедрении в антивирусные пакеты специальных модулей для защиты от спама.

Согласно информации компании Sophos, компьютеры, зарегистрированные на территории США, распространяют 22% всего мирового электронного мусора, за ними следует Китай (16%) и Южная Корея (7%). При этом девять из десяти спамерских сообщений рассылаются так называемыми взломанными компьютерами, которые контролируются извне.США лидируют и по количеству вредоносного ПО, содержащегося в компьютерах: 34,2% всего опасного кода в Интернете находится на серверах, расположенных в Штатах. Китай занимает второе место - 31%.

Только в одной важной категории США не попали в первую "пятерку вредителей". 30% всего зараженного ПО в 2006 году было написано в Китае. Большая часть этого "веб-зла" предназначена для кражи регистрационных данных и паролей для он-лайновых игр. Бразилия стала родиной 14,2% мирового вредоносного кода - главным образом "троянских коней", цель которых - банковский сектор. Далее следуют Россия, Швеция и Украина, которые произвели соответственно 4,1%, 3,8% и 3,4% вредоносного ПО.

Распределение спама по тематике в Рунете, 2006 г.:

Компьютерное мошенничество	18,2%
Образование	1 4,7%
Медикаменты, товары и услуги для населения	12,1%
Отдых и путешествия	8,7%
Компьютеры и Интернет	7,5%
Личные финансы	5,0%
Услуги по электронной рекламе	4,6%
Спам для взрослых	2,0%
Другие товары и услуги	27,2%

(источник – лаборатория Касперского, объем анализируемых сообщений – 250 – 600 тыс. в день)

Основная сложность борьбы состоит в том, что спамеры защищают свои письма, маскируя их содержание, к примеру, с помощью технологии внесения случайных текстов, "шума", невидимых текстов. Для этого в начало или конец письма спамер может поместить отрывок из классического текста или просто случайный набор слов, а в HTML-сообщение можно внести "невидимый" текст (очень мелким шрифтом или цветом, совпадающим с цветом фона). Эти добавления затрудняют распознавание спама методом нечетких сигнатур и статистическими методами

Есть графические письма — рекламное сообщение можно прислать пользователю в виде графического файла, что крайне затруднит автоматический анализ. В качестве ответной меры появляются способы анализа изображений, выделяющие из них текст. Изменяющиеся графические письма — более продвинутая технология, в графическое сообщение можно внести "шум", что затруднит его анализ фильтром. Есть и перефразировка текстов — одно и то же рекламное сообщение составляется во множестве вариантов. То есть каждое отдельное письмо выглядит как обычный связный текст, и только имея много копий сообщения, можно установить факт перефразировки.

Со спамом можно бороться — в странах, где антиспамерские мероприятия стали приоритетными для администраций связи .

В Нидерландах и Финляндии, где с 2006 года за рассылку спама предусмотрено тюремное заключение и штрафы в размере нескольких десятков тысяч евро, за три года его количество сократилось на 85%. Спецслужбы Финляндии и Великобритании взяли под стражу трех членов известной спамерской группы. В штате Индиана пять фирм оштрафованы, восемь находятся под следствием, 185 получили официальные предупреждения.Согласно законам Индианы и некоторых других штатов за каждое «деловое предложение» нерадивым бизнес-партнерам придется заплатить $1500.

Причем e-mail-спамом дело не ограничивается. Любые популярные публичные сервисы могут стать жертвой спамеров, начиная с интернет-пейджеров типа ICQ и заканчивая веб-блогами.

Уже не редкость спам на мобильных телефонах, когда высылаются SMS-сообщения с рекламой через интернет-шлюзы, ожидается спам по VoIP-сетям (IP-телефония).В 2005 г. были зафиксированы первые вирусы (Cabir, Gavno), поражающие мобильные телефоны продвинутого типа, работающие на ОС Symbian и использующие технологию Bluetooth.

С 2007 г. провайдеры обязаны отчитываться перед пользователями о том, как они борются со спамом. Документ также защитит провайдеров от пользователей, которые отказываются платить за трафик, сгенерированный вирусами.это не первая попытка борьбы со спамом: «Первая была предпринята в 2006 году с принятием новой редакции закона „О рекламе", который запретил рассылать рекламу по электронной почте без согласия получателя. Правда, спама от закона меньше не стало». Недостатком новых правил является не совсем точное определение спама: «В документе написано, что спам направлен неопределенному кругу лиц, в то время как на практике может быть наоборот. Спам зачастую рассылается определенному кругу лиц: работникам определенной отрасли, компании...»

7 мифов о спаме:

ходят слухи, что спам - это плохо и что плохо пользоваться услугами спамеров. *мы опровергнем их в этом письме!*

1 миф: спам дает маленький результат

Массовая рассылка, сделанная на миллионы пользователей, дает десятки звонков, по теории вероятности один из ста тысяч человек заинтересуется предложением.

2 миф: спам вне закона

В законодательстве нет четкого определения спам, поэтому вам каждый день приходят различные рекламные письма. если данный закон будет действовать, то сотни тысяч предприятий потерпят банкротство!

3 миф: спам заказывают безнадежные маленькие фирмы

Услугами массовых рассылок пользуются банки, крупнейшие торговые компании, интернет-провайдеры и просто частные лица которые хотят быстро продать свой дом или автомобиль. не говоря о фирмах, которые проводят семинары!

4 миф: спам - это плохо

Массовая рассылка - это помощь любой развивающейся компании в поиске клиентов. рассылка - это такая же обычная реклама, которую вы видите на сайтах, по телевизору, на улице, в журналах и т.п.

5 миф: от спама много негатива

Если вы закажите рекламу на крупном телевизионном канале, то к вам обратятся множество людей и обязательно найдется 2-4 человека которым не понравится ваш рекламный ролик и выскажут свое мнение в силу разных причин. также и в массовой рассылке, всегда найдется человек которому не понравится ваша реклама.

6 миф: спамеры обманывают

Все в жизни относительно, есть серьезные фирмы, которые оказывают качественные услуги и есть начинающие. к кому обращаться это ваш выбор. всегда трудно распознать!

7 миф: спам - это не этично:

Расклеивать объявления возле подъездов, рассылать коммерческие предложения почтой или производить массовую рассылку по электронной почте - это нормально! Любому бизнесу нужны клиенты, но не каждый себе позволит заказать рекламу на радио или телевидении.

Некоторые виды криминального спама распространены во всем мире — фишинг и "'нигерийский" спам, фальшивые уведомления о выигрыше в лотерею, предложения организовать вирусную рассылку.

Участие в замаскированных схемах по отмыванию денег предлагают пользователям Интернета на Западе.

Лондонская общеобразовательная сеть для обслуживания средних школ города. Доступ имеют 1, 1 млн. школьников и 65 тысяч учителей. 75% электронной почты этой сети - спам, в том числе пропаганда наркотиков (50%), порнография (20%)

А вот рунетчики получают рассылки с предложениями купить варианты билетов выпускных экзаменов в школах и вступительных в

Наибольший "вред" нанесли вирусописатели, которые стали использовать технологии массовой рассылки писем для распространения сотен тысяч копий своих вредоносных творений, а также невоздержанность многих спамеров, сделавших это бизнесом, так как от их рассылок простому пользователю просто невозможно отписаться.

Основная проблема — блокировка нежелательной корреспонденции и блокировка спам-машин, т. е. компьютеров, которые являются источниками такой активности. Однако в этом есть сложность — многие спамеры отправляют почту от имени обычных клиентских компьютеров, подключенных к Интернет

Такие компьютеры заражены вирусом и являются зомби-машинами, послушно выполняющими приказы новых "хозяев". Вряд ли в ближайшее время удастся снизить процент спама, находящегося в общем трафике электронной почты. Как отмечает Анна Власова, аналитик "Лаборатории Кас-перского", складывается впечатление, что к настоящему моменту произошло своеобразное "насыщение" спамом почтовых потоков во всем мире

Интернет-холдинг Mail.Ru совместно с «Лабораторией Касперского» объявляет об открытии информационного проекта Защита (http://protect.mail.ru/), пользователям предоставляется исчерпывающая информация о вирусах и спаме. Статистическая информация представлена в виде графиков; они отображают ежедневную ситуацию по данным почтового сервиса Mail.Ru, где установлена система фильтрации «Лаборатории Касперского». Поскольку Mail.Ru является крупнейшим почтовым сервисом в России (через его сервера в сутки проходит около 80 млн. писем), данные о % вирусов и спама в почтовом потоке могут использоваться как среднестатистические для всего Рунета.

В разделе «О вирусах» публикуются аналитические статьи о наиболее активных и новых вирусах, вирусных эпидемиях и других значимых событиях в области компьютерной безопасности. Раздел «О спаме» содержит обзор наиболее популярных видов спама. «Этот проект призван донести до пользователя необходимую информацию об обеспечении безопасности работы в сети. Вирусы и спам являются серьезной проблемой почты и Интернета. Мы уверены, что с появлением нового информационного ресурса пользователи смогут понять всю важность работы по борьбе с ними», — говорит Анна Артамонова, директор по маркетингу и PR холдинга Mail.Ru.

Холдинг Mail.Ru один из лидеров российского Интернет-рынка. Ежемесячная аудитория проектов холдинга составляет более 14 млн. пользователей или 80% от всей аудитории русскоязычного Интернета.
«Лаборатория Касперского» международная компания-разработчик программного обеспечения для защиты от вирусов, хакеров и спама. Продукты компании предназначены для широкого круга клиентов - от домашних пользователей до крупных корпораций

Захаров, Дмитрий Хакеры становятся частью мировой экономики. Коммерсантъ, четверг, 4 августа 2005 г. № 143

Как сообщается в отчете IBM 2005 года «Широкое распространение получают целенаправленные атаки против конкретных организаций и отраслей. Такие атаки предпринимаются с единственной целью - завладеть критически важными данными и идентификационной информацией пользователей либо получить от них деньги». По статистике IBM, чаще всего киберпреступники атакуют

госструктуры (23 % всех атак),

производственные предприятия (15 %),

финансовые организации (14 %) и

организации сферы здравоохранения (7 %).

В 2005 году около четверти всех киберпреступлений совершалось с целью наживы. Эту же тенденцию отмечают и российские эксперты по информационной безопасности.

«Хакер - это больше не мальчик, который ищет в Интернете дырявый сервер и запускает туда своего червя,— говорит заместитель директора по маркетингу компании „Информзащита" Михаил Савельев.— Прошло время, когда вирусы создавались в соревновательных целях, лишь бы только попасть в верхние строчки рейтинга. На кибератаках и проникновениях в компьютерные системы люди начали вполне профессионально делать деньги».

Как сообщает газета «Известия» №209 от 12.112009 с. 5, Минюст США предъявил обвинения хакерам из России, Эстонии и Молдавии во взломе компьютерной мети компании RBS World Pay (г. Атланта, США). С помощью 44 фальшивых дебетовых карт они обналичили через банкоматы более 9 млн. долларов. Трем главным обвиняемым грозит до 20 лет тюрьмы.

В 2005 году набрали популярность фишинговые атаки. Фишинг — термин, образованный от английского слова fishing («рыбалка») и обозначающий выуживание информации у доверчивых пользователей с помощью поддельных электронных писем. Выуживаются в основном данные о кредитных картах и счетах в электронных платежных системах. Фишинговых писем, по данным IBM, в мире в 2006 году стало в десять раз больше. Похожие темпы роста отмечается и в России. «Если в середине 2004 года в общем количестве спама мы даже не могли выделить хоть сколько-нибудь заметную долю фишинговых писем, то уже сейчас их доля составляет 4-5 % и постоянно растет,— говорит руководитель группы спам-аналитиков „Лаборатории Касперского" Анна Власова

В целом же доля мошеннических рассылок, целью которых является получение денег от пользователей, сейчас в России составляет уже 10-12 %».

С 2005 году фишинговые письма все чаще рассылались уже не простым пользователям в виде массовой рассылки, а адресно — работникам конкретных организаций. «Изменяется направленность атак с массовых пользователей на конкретные организации, комментирует старший вирусный аналитик Александр Гостев. Злоумышленники стараются атаковать конкретные базы данных, потому что гораздо удобнее украсть 40 млн. номеров кредитных карточек у одного банка, чему 40 млн. его клиентов».

Господин Гостев отмечает, что стремительное развитие экономического аспекта киберпреступности привело к резкому снижению числа громких вирусных атак, которые за считанные дни поражали персональные компьютеры по всему миру. «Злоумышленники находят более тихие и более эффективные методы добычи данных,— рассказывает Александр Гостев.— Например, уже два месяца мы наблюдаем интересную эпидемию вредоносной программы Win32.Opcode, которая при попадании на компьютер шифрует все документы и базы данных и оставляет сообщение пользователю, в котором предлагается расшифровать информацию за конкретную сумму—от $ 50 до $ 3 тыс.

Фактически хакеры берут ценные данные в заложники. Причем 90 % людей, которые пострадали от них,— сотрудники крупных организаций: агентств недвижимости, банков, заводов». Эксперты в области информационной безопасности прогнозируют, что доля экономических преступлений в киберпространстве к концу этого года превысит 35-40 %, а в 2006 году уже каждая вторая вредоносная программа будет создаваться с единственной целью — выбить деньги у незадачливых пользователей.

Троянские программы, получившие название ransomware (от английского ransom — выкуп), действуют следующим образом. Попадая в компьютер, они зашифровывают некоторые файлы. При попытке их открыть пользователь получает сообщение, что ему необходимо перевести определенную сумму на указанный счет. Размер «откупа» бывает разный и зависит исключительно от наглости злоумышленника. Потребовать могут и $ 10, и $ 1000. При этом преступники угрожают, что если деньги не будут переведены в назначенное время, то другие файлы тоже будут зашифрованы.

В нашей стране программы-вымогатели появились пару лет назад. Первыми жертвами вымогателей стали учреждения — в основном банки и офисы крупных компаний с большим документооборотом. Причем не только российские, но и западные. Но связываться с корпоративными пользователями, часто имеющими в своем арсенале специальные отделы, ведущие борьбу с хакерами, оказалось себе дороже. Ведь гораздо проще выманивать деньги у обычных граждан.

Охотники за мобильными телефонами научились вычислять обладателей дорогих аппаратов и, дождавшись удобного момента, крадут их. Кроме того, Bluetooth освоили хакеры — «проникнув» в телефон, взломщик может скопировать все содержащиеся в нем данные и даже войти в Интернет или позвонить за счет владельца.

Если в метро вы получаете текстовое сообщение SMS, это может быть сигналом об опасности. Текст может выглядеть необычно, к примеру: «Когда отдашь долг, редиска?». Любой нормальный человек, прочитав сообщение, только пожмет плечами, даже не подозревая, что цель отправителя SMS уже выполнена. Как правило, это неприметный паренек в 5—10 метрах, который с помощью технологии Bluetooth вычисляет, какие телефоны есть рядом. Найдя дорогую модель, он с помощью все той же технологии посылает сообщение без участия сотового оператора. Получатель читает сообщение, а паренек засекает, кто и в какой карман кладет дорогой аппарат, который потом либо крадут из кармана, либо отбирают, выследив жертву.

Кроме опасности стать жертвой карманников имеется опасность подвергнуться хакерской атаке. К примеру, сидя в кафе, человек и не заметит, что на экране телефона появилась маленькая иконка. А это может означать, что за соседним столиком опять же сидит неприметный паренек с карманным персональным компьютером (КПК) или ноутбуком. За несколько минут он может через Bluetooth проникнуть в телефон, скачать оттуда всю интересующую его информацию, ежедневник, телефонную книжку, личные фото. А попутно войти в Интернет, позвонить друзьям на другой конец света. Хозяин телефона узнает об этом, только когда получит счет от провайдера.

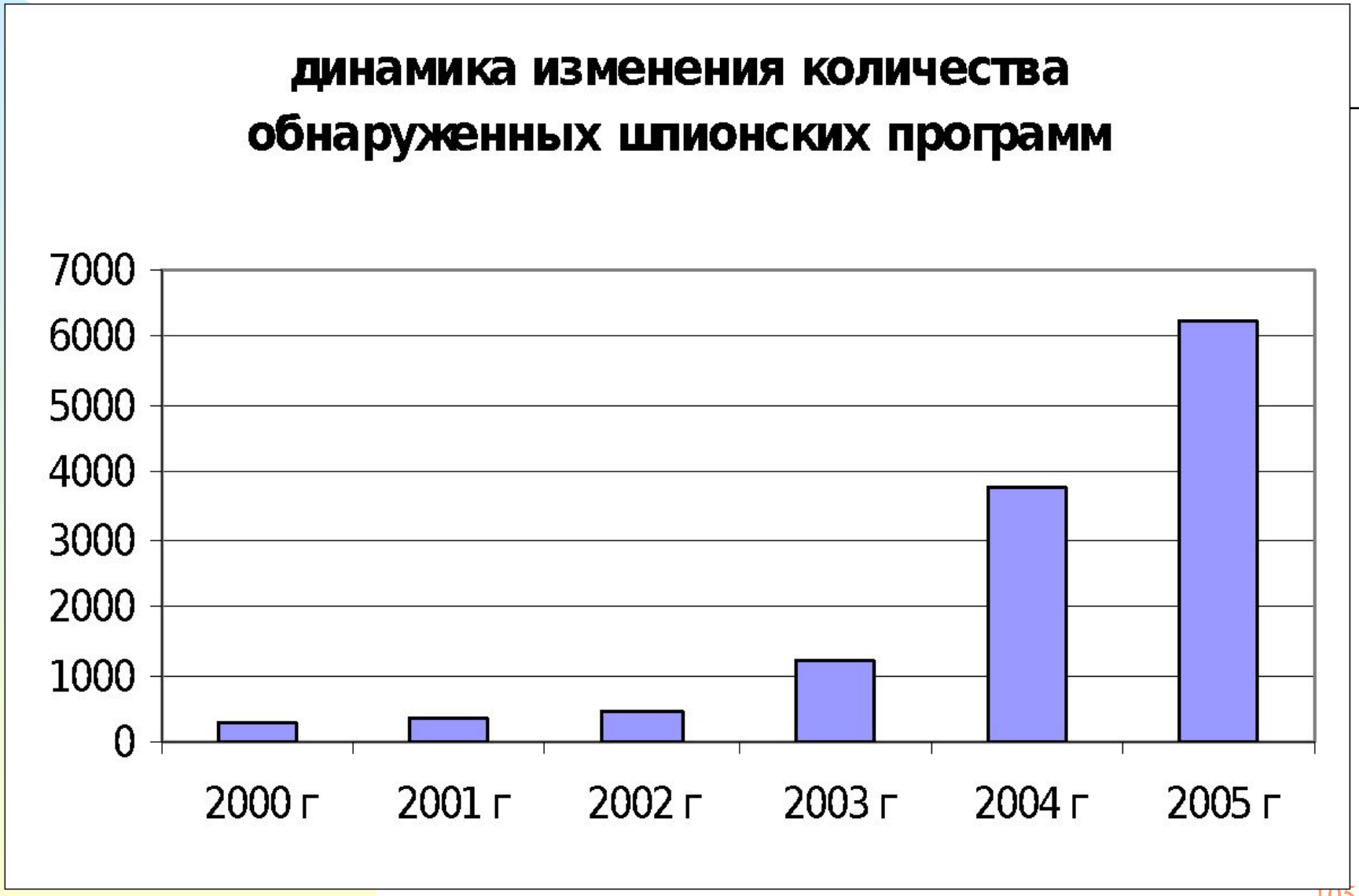
Известно около десяти видов различных атак, - они используют уязвимость либо самого протокола Bluetooth, либо его реализации на конкретных телефонах. Защититься от воров, присылающих странные SMS-послания, можно, только отключив саму функцию Bluetooth. Но делает это один из десяти пользователей. Что касается атак хакеров—для предотвращения атак технология Bluetooth предусматривает использование пароля. Далеко не все знают, как его установить. Но даже при установленном пароле, который в большинстве телефонов содержит 4 цифры, хакерская программа может подобрать код за несколько секунд. Поэтому надежнее всего функцию Bluetooth отключать, когда она не нужна.

Многие молодые люди сами устанавливают на своих телефонах пароль «0000». К этому их призывают сторонники нового модного увлечения, которое получило название Bluejacking. В его основе — отправка шутливых сообщений на телефоны незнакомых людей посредством того же Bluetooth.

Блюджекинг подается как способ завести новые знакомства, обменяться файлами и музыкой. Для того чтобы принять участие в общении, всех желающих просят установить на свой Bluetooth единый пароль. Как правило, «0000». На Западе опасности беспроводной технологии известны уже довольно давно. В здании английского парламента во избежание хакерских атак вообще запрещено пользоваться Bluetooth-устройствами. В Госдуме мобильными телефонами запрещено пользоваться, только входя в кабинеты первых лиц—спикера и вице-спикеров. Государственная комиссия по радиочастотам при Минсвязи РФ ввела ограничение на максимальную мощность передатчика, которое позволяет устройствам Bluetooth действовать только на расстоянии до 10 метров. В Европе такие устройства «бьют» до 100 метров, обнаружить их можно даже через стены.

Воровство мобильных телефонов можно сделать бессмысленным. Для этого каждый владелец телефона должен запомнить его уникальный, не зависящий от вставленной СИМ-карты идентификационный IMEI-код. Он состоит из 15 цифр и появляется на дисплее после набора комбинации *#06#. Если телефон похитят, нужно связаться с оператором и заблокировать телефон—им невозможно будет воспользоваться вне зависимости от того, какая СИМ-карта в нем стоит. Кроме того, похищенный телефон могут отследить правоохранительные органы. При широком распространении этой практики воровство мобильных станет слишком опасным и не оправдывающим себя делом.

Количество обнаруженных шпионских (keylogging) программ, данные iDefence The New York Times, march 6 2006 p/ 4



Российские хакеры испугали Европу на $4 миллиона Приговор российским хакерам, получившим более $4 миллионов с европейских игорных Интернет-компаний, вынес суд в Балакове.

Иван Максаков, Александр Петров и Денис Степанов получили по восемь лет строгого режима.

Больше года они атаковали букмекерские интернет-конторы Великобритании с требованием заплатить им десятки тысяч долларов. В случае отказа хакеры блокировали интернет-сайты компаний, что оборачивалось гигантскими убытками.

Бесплатный обмен музыкальными файлами через центральный сервер, - компания Napster, 60 млн пользователей; протесты гигантов музыкальных записи, выплата многомиллиардных отступных, банкротство;

одноранговый обмен (без центрального сервера - равный с равным, P2P) - Gnutella.

Весной 2009 г. администраторы крупнейшего в мире торрент-трекера The Pirate Bay были при говорены к году тюрьмы и к штрафу 900 тыс евро. Суд признал администраторов»пособниками пиратов», хотя формально на серверах The Pirate Bay ничего не хранилось, они только были «наводчиками».

Крупные компании постоянно ведут несколько дел, отбиваясь от обвинений в монополизме (Майкрософт) или в нарушении авторских прав (Гугл)

Компания Гугл может столкнуться с возрастающим сопротивлением во всем мире своим планам оцифровки всех книг мира. Суд г. Париж в декабре 2009 г. постановил, что оцифровка французских книг, хранящихся в американских библиотеках, без разрешения правообладателей, является нарушением авторских прав и наложил на Гугл штраф 300 тыс евро за нанесенный моральный и материальный ущерб. В суд обратилась компания Matiniere. Стремление Гугла оцифровать книги, находящиеся под защитой, но вышедшие из торгового оборота (out of prints), оказалось под угрозой.

В китайском суде находится на рассмотрении аналогичная жалоба.

В прошлом году Гугл сумел договориться с американскими издателями.

Победа французских издателей может оказаться пирровой – если Гугл прекратит сканирование и уничтожит созданные файлы: работы французских писателей просто окажутся вне зоны доступности пользователей величайшей поисковой машины мира. Французские издатели хотели бы начать переговоры с Гуглом.

По такому же пути могут пойти и другие европейские страны, в которых (как во Франции) нет концепции «честного пользования», принятой в американском законодательстве.

Французское правительство недавно выделило на оцифровку культурных ценностей (в том числе и французских книг) 750 млн евро.

Гугл стремится найти мирное решение своих споров с издателями и авторами. Примером может быть опубликованное в «Известиях» *№114 от 30.06.2009, с. 4* «Предусмотренное законом уведомление» о мировом соглашении по урегулированию коллективного иска в отношении осуществляемого Google сканирования и использования книг и других литературных произведений. В случае одобрения судом мирового соглашения Google сможет сканировать охраняемые авторским правом книги и поддерживать базу данных книг. В случае получения разрешения от владельцев прав Google сможет за плату предоставлять к ним, продавать подписку на базу данных, размещать рекламу, а также использовать книги иным коммерческим способом. Владельцы могут в любой момент изменить указания Google в отношении такого использования.

Создается Реестр прав на книги (на его создание выделяется 34,5 млн долларов). С помощью Реестра перечисляется владельцам прав 63% всех доходов от такого использования. Кроме того, выделяется 45 млн. долларов для выплаты владельцам прав.

В России в 2008 г. московский арбитраж признал провайдера «Мастерхост» виновным в размещении на сайте Zaycev.net нелицензионной музыки, но затем Высший арбитражный суд отменил это решение.

Поэтому 40 млн пользователей самой популярной социальной сети Рунета «В контакте» могут обмениваться файлами через сервис VKTracker, который дает ссылки на владельцев файлов.

Аудитория торрент трекеров в России – около 7 млн человек.

Прокуратура Сыктывкара (Республика Коми) передала в суд уголовное дело местного жителя Саввы Терентьева, которое было открыто по статье «Возбуждение ненависти либо вражды» за то, что тот нелестно отозвался о местной милиции в интернет-блоге.

Это первое в России уголовное дело, заведенное за комментарий в сетевом дневнике.

За него господин Терентьев, чье высказывание в блоге прокуроры приравняли к публикации в СМИ, может получить два года лишения свободы

Шестнадцатилетний школьник из города Гамильтон снял своих одноклассников на видео, в то время когда они бесились в классе, швырялись ручками и разрисовывали доску. Региональная газета Hamilton Advertiser не только напечатала статью, рассказывающую об «акции неповиновения», но и загрузила видео, снятое мальчиком, себе на сайт.

Две другие газеты The Scottish Sun и The Scottish Daily Mirror использовали картинки из видео для того, чтобы иллюстрировать материалы о проблемах в шотландских школах.: «Информация, опубликованная в СМИ, в наше время в любом случае будет рассмотрена комиссией точно так же, как и любой другой журналистский текст».

Но Британская комиссия по СМИ принимает к рассмотрению жалобы на сайты, которые являются интернет-версиями печатных изданий.

Пресс-секретарь комиссии сообщил, что их ведомство уже подвергалось критике за столь однобокий алгоритм принятия решений — фактически под их юрисдикцию не попадают все самостоятельные интернет-порталы.

Майкопский горсуд приговорил к году исправительных работ студента Виктора Милькова, распространившего в интернете видеоролик казни двух человек.

Видеозапись казни двух человек, стоящих в лесу на коленях со связанными руками под полотнищем с изображением свастики, появилась в интернете в 2007 г. Вскоре сотрудники правоохранительных органов задержали 24-летнего студента-заочника Адыгейского технологического университета Виктора Милькова, который на допросе признался, что получил скандальную видеозапись по электронной почте от неизвестных и выложил ее в интернете. Студенту оформили явку с повинной

Прокуратура предъявила обвинение по ч. 1 ст. 282 УК РФ («Возбуждение национальной, расовой или религиозной вражды»).

Судья Герасимов посчитал, что исправление Виктора Милькова возможно без его изоляции от общества, и назначил ему год исправительных работ с удержанием 10% заработка «в доход государства».

Калининский районный суд города Чебоксары приговорил студента Чувашского государственного педагогического университета им. И. Я. Яковлева Станислава Кузьмина к 14 месяцам заключения условно. Осужденный поменял пароль почтового ящика своего знакомого, который находится на сервере «Яндекса».

Эту процедуру удалось осуществить благодаря системе напоминания паролей: злоумышленнику понадобилось лишь ответить на контрольный вопрос о фамилии родственника жертвы

Получив доступ к почтовому ящику, студент Кузьмин скопировал логин и пароль для доступа к системе «ЯндексДеньги», перевел со счета один рубль и вернул его обратно, о чем и сообщил потерпевшему.

Потерпевший шутку не оценил и подал заявление в милицию. В результате суд признал Станислава Кузьмина виновным по ст. 138 УК РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» и ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» и приговорил к 14 месяцам условного заключения с испытательным сроком в течение года.

Самые крупные киберограбления

1994 г. - российский программист Владимир Левин, взломав систему Нью-йоркского отделения Ситибанка, попытался перевести ~~на свои счета $10 млн.~~

2004 г. - команда из 7 отечественных хакеров украла у 8 тыс. владельцев банковских карт около $21 млн. и была обезврежена МВД РФ.

2006 г. - более $1 млн, хакеры «списали» со счетов клиентов шведского банка Nordea.

2007 г.- кражей века названо похищение хакерами данных о 94 млн. кредитных карт, которыми расплачивались клиенты крупной американской сети магазинов товаров для дома. Ущерб от этой кражи оценён в более чем $100 млн.

В компьютерных сетях межсетевой защитный экран представляет собой специальную программу, защищающую от попыток внешнего вторжения в сеть с целью хищения, искажения, уничтожения конфиденциальной информации, несанкционированного доступа к вычислительным ресурсам подсоединенного к сети компьютера или каналам связи. В большинстве случаев сохранение индивидуальных данных с помощью экрана вполне реально.

Ни один межсетевой экран не обеспечивает 100%-ной гарантии — точно так же, как автомобильная сигнализация не гарантирует от угона.

Совокупность протоколов TCP/IP, лежащая в основе Интернет-технологий, изначально разрабатывалась (60-е годы) для обмена данными между удаленными компьютерами и не предназначена для защиты передаваемых данных.

Ошибочно мнение, что чем мощнее экраны, тем лучше защита.

Ведь нападающий не боится ответного удара и уверен в безнаказанности.

Но если в ответ на хакерское нападение система защиты сотрет у злоумышленника с жестких дисков всю информацию, это послужит ему прекрасным уроком.

Можно сослаться на техническую сложность такого ответного удара и вероятность ошибки (хакеры обычно подменяют IP-адреса своей машины), но ее вполне можно решить совместными усилиями (опираясь прежде всего на поддержку провайдеров). Да и квалификация хакеров-любителей крайне низка, и почти всегда их можно вычислить.

Согласно гл. 2 ст. 45 ч. 2 Конституции РФ, "каждый вправе защищать свои права и свободы всеми способами, не запрещенными законом”.

По российскому законодательству не является преступлением причинение вреда лицу, от которого исходит опасность, непосредственно угрожающая личности и ее правам или правам иных лиц (независимо от возможности избежать посягательства или обратиться за помощью к другим лицам или органам власти).

Можно считать самозащитой уничтожение информации на ПК хакера при попытке его проникновения в корпоративную сеть, где хранятся данные, имеющие высокую материальную ценность.

Подобный адекватный ответ не входит в противоречие со статьей 272 УК РФ "Неправомерный доступ к компьютерной информации", по которой любое деяние, влекущее за собой уничтожение, блокирование, модификацию либо копирование информации на ЭВМ, наказуемо. Ведь причинение физического вреда, запрещенное законом в обычных случаях, допускается этим же законом при самозащите.

Бесплатная утилита La Brea (www.trinux.org) создает приманки - ложные сетевые ресурсы и когда хакер начинает контактировать с ними, выманивает информацию о нападающем и блокирует работу программы злоумышленника так, что ее надо стирать из ОЗУ или перезагружать ОС.

Закон КНР о недопустимости нарушения работы информационных сетей, распространение через Интернет антиправительственных сведений и создание компьютерных вирусов.

Несколько «компьютерных гениев», вторгшихся в финансовую систему страны, были казнены.

Советник президента США по науке Ричард Кларк : « Мы оставляем за собой право дать ответ любым приемлемым способом : с помощью тайных операций, военных действий, или других средств, имеющихся в распоряжении президента».

В США в 2003 году выделяется 52 млрд. долларов в рамках «Национального Плана Защиты Информационных систем в 2000 – 2003 году», при этом на безопасность компьютерных систем управления выделяется 4, 2 млрд долларов, а на создание общенациональной системы контроля за иностранцами на территории США (3 млн человек с просроченными визами) – 2 млрд долларов.

Силовые ведомства приступили к исследованиям перспектив боевого применения вирусов, исходя из доказанной в 1987 г Фредом Коеном теоремы о невозможности создать алгоритм для обнаружения всех типов вирусов.

Особое место – инициатива ФБР по установке на компьютерах подозреваемых лиц специальной программы «Волшебный фонарь» Magic Lantern

Многие страны имеют программы разработки технологий кибер атак; США, Россия, Китай, Франция и Израиль наращивают кибер арсеналы и средства тотальной кибер войны; террористы создают оружие массового поражения; Россия становится питательной средой для хакеров, а российский аналог АНБ (а также организованная преступность) принимают в свои ряды самых талантливых людей.” Рынок информационной безопасности - около 3 млрд долларов, ежегодные убытки порядка 18 млрд долларов.

Американские хакеры могут поплатиться пожизненным заключением.

«Нам никогда не удастся справиться с киберпреступлениями, если общество будет продолжать относиться к ним, как к шутке» - мнение адвоката компании Майкрософт. Доклад ЦРУ : «в предстоящие 15 лет США столкнутся с новым поколением террористов, уголовников и противников государства, вооруженных не танками или самолетами, а компьютерными вирусами и логическими бомбами…»

Кевин Митник –участник наиболее сложной в истории ФБР погони, после отбытия срока стал наиболее высокооплачиваемым специалистом по безопасности.

виктор хилько коммерсант среда 29 марта 2006 №54 опаснее ножа и фомки

В 2006 г компания IBM провела опрос 600 крупнейших американских и европейских компаний. Респондентов спрашивали об угрозах, которым подвержена ИТ-инфраструктура их предприятий. Большая часть опрошенных ИТ-специалистов (57%) заявили, что кибер-преступники — хакеры, вирусо-писатели, Интернет-мошенники и прочие—уже давно наносят их компаниям больший ущерб, чем технологически неподкованные грабители и воры. Результаты этого опроса косвенно подтверждаются данными, которые недавно обнародовало ФБР США. Ежегодный ущерб американских производителей от действий киберпресгупников составляет $67 млрд.

А в мировом масштабе, по оценкам компании Synergy Research, в 2005 году убытки от «высокотехнологичных» правонарушений превысили $300 млрд. Для сравнения: оборот всей мировой IT-индустрии составил порядка $1 трлн. По расчетам компании «Ашманов и партнеры», из-за простоев персонала, связанных с приемом и удалением спама, российские предприятия теряют до $30 млн ежегодно. По оценкам компании «Корбина Телеком», российские связисты из-за незаконного подключения и неоплаченных телефонных переговоров теряют около $150-200 млн в год. А убытки «домашних» пользователей ПК из-за краж паролей доступа и затрат на восста новление загубленного вирусами ПО ежегодно составляют $15-20 млн.

Компаниям, производящим антивирусное ПО и другие средства информзащиты, не приходится жаловаться на отсутствие спроса. Их оборот, по оценкам компании iKS-Consulting, растет на 20-30% в год. По более опти мистичным оценкам, рост объемов продаж составляет 45% в год; для сравнения- оборот всей российской высокотехнологичной индустрии в целом увеличиваются на 15-20 %. В качестве наиболее ярких примеров роста аналитики IDC, к примеру, приводят «Лабораторию Касперского»; по их оценкам, в последние два-три года ее обороты росли более чем на 60% ежегодно

Объем российского рынка средств информационной безопасности, по оценкам iKS-Consulting, $170-200 млн в 2005 году. По более оптимистичным оценкам (компании «Открытые технологии»), объем рынка — около $400 млн.

Точным оценкам рынка мешает, во-первых, высокий уровень программного пиратства в России (учитывать софт, внедренный нелегально, крайне сложно) и, во-вторых, отсутствие четких критериев оценки. «Кто-то из экспертов учитывает только антивирусный и антихакерский софт, кто-то добавляет к этому аппаратное обеспечение, кто-то еще приплюсовывает услуги»,— поясняет аналитик iKS-Consulting Константин Анкилов.

Большинство экспертов по информационной безопасности выделяют следующие сегменты рынка информзащиты: системы управления доступом к информационным ресурсам, антихакерские системы, системы управления безопасностью контента (антивирусы, антиспамовые фильтры), средства шифрования информации.

По оценкам аналитиков компании IDC, быстрее всего развивается сегмент рынка управления доступом к информационным ресурсам. Объемы его пока невелики, не превышают $10 млн. Быстрый рост обусловлен развитием сложных информационных систем, со сбором и обработкой больших объемов информации, поступающих с различных пользовательских терминалов (например, с оборудованных сканерами штрих-кодов касс).

«70% сбоев в таких системах возникает из-за случайного доступа технически неподготовленных сотрудников к компонентам системы, которыми они не умеют и не имеют права пользоваться,— говорит аналитик IDC Тимур Фарукшин.— Неудивительно, что в такой ситуации системы разграничения доступа оказываются все более востребованы».

Не менее привлекательным эксперты находят и рынок аппаратных систем информационной безопасности, львиную его долю составляют биометрические системы распознавания личности. Сейчас объем этого рынка составляет примерно $30 млн в год, ежегодные темпы роста — около 40%.

По постановлению правительства РФ об одобрении «Концепции создания государственной системы изготовления, оформления и контроля паспортно-визовых документов нового поколения» паспортно-визовые документы будут содержать информацию о владельцах в электронном виде. Новая система в 2007 г свяжет более 8 тыс. паспортно-визовых подразделений, пунктов погранконтроля на границах России и консульских учреждений МИД РФ.

Государство готово выделить на этот проект около $500 млн, это как минимум на 20% больше, чем годовой оборот всего рынка информационной безопасности в России.

«Безусловно, этот проект встряхнет рынок систем информзащиты. Это хороший пример поддержки государством российских компаний, специализирующихся в области информационной безопасности,— считает аналитик J'Son & Partners Сергей Горбунцов.—Для отрасли введение биометрических паспортов повлечет далеко идущие последствия, наработки в рамках этой программы впоследствии будут использоваться при создании коммерческих продуктов».

Российские компании, работают исключительно на растущем внутрироссийском рынке. По оценкам IDC, до 65% средств информзащиты ввозится в Россию из-за рубежа, 35% производится российскими компаниями. Из года в год это соотношение не меняется.

«Говорить о перспективах экспорта российских продуктов за рубеж пока не приходится. Конкурентоспособных предложений практически нет,— отмечает Михаил Савельев из компании „Информзащита".— Переломать зарубежный рынок, занятый крупнейшими мировыми производителями, нашим компаниям не под силу».

Экспортный потенциал у российского рынка систем информзащиты есть.

В первую очередь это касается антивирусных программ. По оценкам «Информзащиты», сейчас объем экспорта систем информационной безопасности из России составляет около $50 млн в год, причем антивирусные средства составляют 60% этого объема.

Более половины выручки антивирусной «Лаборатории Касперского» (аналитики оценивают ее в $30 млн в год) компания получает за счет экспорта.

«Мы работаем не только на рынках России и СНГ, но и в странах Западной Европы — Германии, Великобритании, Франции,— говорит руководитель информационной службы компании Ольга Кобзарева.

— В этих странах нам принадлежит 3-4% рынка, и мы считаем это хорошим результатом».

Еще одно перспективное направление экспорта - биометрика. Правда, речь идет пока об экспорте не готовых продуктов, а перспективных разработок российских программистов. Насколько такой экспорт может быть успешным, говорит проект a4vision, организованный в 2001 году выпускниками МГТУ им. Баумана Артемом Юхиным и Андреем Климовым. Изобретенная ими технология трехмерного распознавания человеческого лица 3D Facial пока только выходит на массовый рынок. Однако патентованная технология оказалась настолько удачной, что за три года a4vision привлек инвестиций на сумму почти $30 млн. Сейчас в развитие 3D Facial инвестируют такие компании, как Oracle, Motorola, Logitech.

Компания занимает почетное 4-е место по объемам выручки от продажи защитного программного обеспечения. На первых местах - Symantec, McAfee, Trend Micro; конкурентом Лаборатории Касперского является словацкая компания Eset Software со своим продуктом Nod32.

Евгений КАСПЕРСКИЙ, разработчик антивирусных программ С анонимностью в сети будет покончено *Аргументы и Факты № 1-2 2008 г. с. 51*

- Давненько не слышно о масштабных атаках на Сеть, как, например, было с вирусом «I love you» и прочими. Почему?

- Редкие попытки запустить очередного «червяка» встречаются. Но, во-первых, антивирусные компании стали лучше работать. Во-вторых, для тех видов мошенничества, что используются сейчас, не нужны эпидемии и миллионы заражённых компьютеров. Хакерам достаточно десятка тысяч машин. Они просто выкладывают заражённый файл на веб-страницу и рассылают на неё ссылку. Так можно воровать банковскую информацию, снимать деньги за навязанные услуги, атаковать интернет-ресурсы...

Угроза уголовного наказания сдерживает вирусописателей. Авторы знаменитых «червей» были арестованы и теперь сидят в тюрьме. А кому туда хочется? Для тех, кто пишет зловредные программы, главное заработать побольше денег. Им не нужно светиться

- Если начинающий пользователь, купит компьютер и подключится к Сети, сколько вирусов он наловит в первый же день? Это зависит от его активности. Если пользователь безалаберно шарит по сайтам (особенно набирая в поисковиках слова «секс», «порно»), не используя при этом антивирусную защиту, то десяток разных «зловредов» в течение часа ему гарантирован.

-- А известно, сколько в мире (и в России в частности) «заражённых» компьютеров?

Такой статистики не существует.

Но есть данные по числу заражённых файлов. Мы непрерывно мониторим Сеть и добавляем что-нибудь новенькое в нашу базу данных, по 200-300 образцов в сутки.

Сейчас антивирусная база насчитывает около 250 тыс. записей.

А зловредных программ, думаю, больше миллиона. Другое дело, против них всех уже есть зашита.

- Чем сложнее становятся операционные системы, тем они уязвимее. Говорят, появились вирусы, проникающие с компьютера в MP3-плееры. Каких ещё сюрпризов стоит ждать от киберпреступников?

- Что касается MP3-плееров, это был экспериментальный вирус, написанный под конкретную разновидность iPod с целью доказать: и до него можем добраться!

Дальше будут появляться не столько вирусы для операционных систем и приложений, сколько новые «бизнес-идеи». Одна из последних - как заработать на бирже с помощью «троянских» программ.

Хакеры выбирают компанию, скупают её акции. Затем, используя «троянского коня», взламывают какое-нибудь брокерское агентство и получают доступ к его базе. И через неё продолжают скупать акции, тем самым поднимая их стоимость.

Уязвимость - болезнь всех современных операционных систем. К сожалению, неизлечимая.

Но тут приходится выбирать: либо удобство, либо безопасность.

Неужели проблема компьютерной преступности неразрешима?

Почему же? Выход есть – это полная идентификация пользователей Сети. Чтобы войти в Интернет, надо будет вставлять в компьютер пластиковую карту и вводить ПИН-код. Тогда пользователя можно будет при необходимости найти и привлечь к ответственности. Реализация такого глобального проекта будет стоить очень дорого, но к этому всё равно придут.

Проблема Интернета - в анонимности его пользователей, и от неё придётся избавляться.

Заместитель генерального прокурора России Иван Сыдорук заявил, что власть должна законодательно контролировать интернет «для усиления борьбы с экстремизмом».

Это не первое подобное заявление силовиков, поэтому за свободу интернета вступились правозащитники: они уверены, что госконтроль над интернетом приведет к появлению преследуемых государством «кибердиссидентов».

Специалисты в области интернета уверены, что осуществить цензуру в сети будет весьма сложно.

Спасибо,

Пожалуйста, вопросы