

КОНСАЛТИНГ
ТЕХНОЛОГИИ
РАЗРАБОТКА

ЗАКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
"АШМАНОВ и ПАРТНЕРЫ"

Телефон (095) 422-7198. Интернет: www.ashmanov.com

Спам: итоги 2003 года

Аналитический отчет

Авторы: И. Ашманов, А. Власова,
К. Зоркий, А. Калинин,
С. Кошкин, А. Тутубалин

© ЗАО "Ашманов и Партнеры"
Москва, 12 января 2004 г.

Содержание:

1. КРАТКОЕ РЕЗЮМЕ: ГОД ПОД ЗНАКОМ СПАМА.....	3
2. О НАШЕМ ИССЛЕДОВАНИИ: КАК МЫ АНАЛИЗИРУЕМ СПАМ.....	5
3. СПАМ: ТЕНДЕНЦИЯ БУРНОГО РОСТА.....	5
3.1. Доля СПАМА В ПОЧТОВЫХ ПОТОКАХ МИРА	5
3.2. Доля СПАМА В РУНЕТЕ	6
3.3. РОСТ УЩЕРБА, ПРИЧИНЯЕМОГО СПАМОМ	6
4. СПАМ – КАЧЕСТВЕННОЕ РАЗВИТИЕ.....	7
4.1. НЕРАВНОМЕРНОЕ РАСПРЕДЕЛЕНИЕ СПАМА	7
4.2. СЕЗОННЫЕ ВСПЛЕСКИ СПАМА	7
4.3. МЕНЯЕТСЯ СОДЕРЖАНИЕ СПАМА.....	7
4.3.1. <i>Распределение по тематикам</i>	8
4.3.2. <i>Тематическое распределение спама в Рунете</i>	8
4.4. ПОЯВЛЕНИЕ НОВЫХ СПАМЕРСКИХ ТЕМ	10
4.4.1. <i>Политический спам</i>	10
4.4.2. <i>Спам, эксплуатирующий интерес к "горячим" новостям</i>	10
4.4.3. <i>Предложения антиспамерского ПО</i>	11
4.5. ИЗМЕНЕНИЕ ЯЗЫКОВОГО СООТНОШЕНИЯ СПАМА В РУНЕТЕ	11
4.6. ЗАКАЗЧИКИ И ИСПОЛНИТЕЛИ	11
5. СПАМЕРЫ НА ОСТРИЕ ТЕХНОЛОГИЧЕСКОГО ПРОГРЕССА.....	12
5.1. ПОЯВЛЕНИЕ ПРОФЕССИОНАЛЬНЫХ СИСТЕМ РАССЫЛОК	12
5.2. ИСПОЛЬЗОВАНИЕ ЗАРАЖЕННЫХ КОМПЬЮТЕРОВ ПОЛЬЗОВАТЕЛЕЙ.....	12
5.3. ЧЕРНЫЕ СПИСКИ РАБОТАЮТ ВСЕ ХУЖЕ	12
5.4. ТИПОВАЯ "СПАМ-МАШИНА" ОБРАЗЦА 2003 Г.	13
5.5. СПАМЕРЫ ПЕРЕШЛИ К "ОТВЕТНЫМ" УДАРАМ.....	13
5.5.1. <i>Организация распределенных атак на RBL-системы</i>	13
5.5.2. <i>Организация спамерских "псевдорассылок"</i>	13
5.6. ИСПОЛЬЗОВАНИЕ СПАМЕРСКИХ ТЕХНОЛОГИЙ ДЛЯ РАССЫЛКИ ВИРУСОВ	13
5.7. НОВЫЕ ТЕХНИЧЕСКИЕ ПРИЕМЫ ОБХОДА ФИЛЬТРОВ	14
5.7.1. <i>Использование графики</i>	14
5.7.2. <i>Модификация текста сообщения</i>	15
5.7.3. <i>HTML-трюки</i>	15
6. ПРОГНОЗ НА 2004 Г.	16
6.1. ДАЛЬНЕЙШИЙ РОСТ ОБЪЕМОВ СПАМА	16
6.2. СОВЕРШЕНСТВОВАНИЕ ТЕХНИЧЕСКИХ ВОЗМОЖНОСТЕЙ СПАМЕРОВ	17
6.3. КОНСОЛИДАЦИЯ И СТРУКТУРИРОВАНИЕ СПАМЕРСКОГО СООБЩЕСТВА	17
6.4. КЛИЕНТЫ СПАМЕРОВ	18
7. ПРИЛОЖЕНИЕ: ПЕРВЫЕ СПАМ-ИТОГИ 2004 ГОДА.....	18

1. Краткое резюме: год под знаком спама

Уходящий год заставил нас по-новому взглянуть на проблему спама. Из побочного раздражающего фактора спам превратился в **крупномасштабную угрозу** электронной почте. Данные различных опросов показывают, что обычные пользователи, чья работа не связана с Интернетом и IT-технологиями, могут существенно сократить объемы электронной переписки или даже вообще отказаться от использования электронной почты, чтобы избежать проблемы спама.

С начала года **рост количества спама** превзошел все, даже самые пессимистичные прогнозы, дававшиеся в конце прошлого года. Если по нашим и западным оценкам в конце 2002 года спам составлял 30-40% от общего числа электронных писем в мире, то уже летом 2003 доля спама превысила отметку 50%. По нашим сведениям, на конец года спам составляет около 75-80% всей входящей корреспонденции в публичных почтовых службах Рунета.

Убытки от спама, на первый взгляд незначительные для отдельного пользователя, в масштабах всей индустрии и даже отдельной крупной компании выглядят впечатляюще. По разным оценкам, на спаме компании теряют от \$50 до \$200 в год в расчете на одного офисного сотрудника. В результате в прошедшем году ущерб от спама по порядку величины стал сравним с потерями, которые нанесли мировому сообществу компьютерные вирусы и хакеры. В России этот ущерб можно оценить в 150-200 миллионов евро, а консервативная оценка ущерба во всем мире близка к 10 миллиардам долларов. Нужно заметить, что благодарить за это следует всего пару сотен человек (большинство которых живет и работает в США), на долю которых приходится 80-90% мусорных рассылок.

Взрывной рост количества спама вынуждает крупные интернет-сервисы "большого" Интернета и Рунета в частности, а также ведущие IT-компании внедрять новые **технологии фильтрации** почты. Усиливается борьба со спамом на Hotmail, Yahoo! и MSN, которые внедряют все новые технологии фильтрации, а также предлагают пользователям ввести списки "доверенных адресатов", чтобы избежать ошибочного уничтожения фильтрами нужных писем. В Рунете запущен бесплатный фильтр спама Spamtest.ru, на крупнейшем российском почтовом сервисе Mail.Ru внедрен "Антиспам Касперского", Яндекс объявил о запуске собственного сервиса "Спамооборона", почтовый сервис портала KM.RU внедрил защиту от спама "Карантин" от компании "E-Style ISP", петербургский провайдер Петерлинк установил "Антиспам Касперского", московский провайдер Корбина Телеком объявил о внедрении собственного фильтра спама, построенного на бесплатной технологии SpamAssassin.

В течение 2003 года существенно развились **технологии спамеров**, приспособившихся к новым условиям существования. Основное количество спама рассылается уже не напрямую, а с помощью сетей, состоящих из захваченных спамерами пользовательских машин. Теперь спамеры рассылают троянские программы, которые, заражая машины пользователей, служат площадкой для рассылки спама. В рассылках участвуют сотни тысяч зараженных компьютеров, пользователи которых могут об этом даже не подозревать. Это приводит к резкому всплеску потоков спама и снижению эффективности черных списков (RBL).

Угасание метода "черных списков" становится все более очевидным. Фильтрация по IP-адресам становится неэффективной из-за использования динамических множеств захваченных пользовательских машин, одновременно приводя ко многочисленным ложным срабатываниям и нередко вызывая нарушения связности отдельных сегментов

сети Интернет. Показательным стал случай с закрытием известного сервиса Osirusoft, подвергавшегося неоднократным атакам, который перед закрытием 26 августа 2003 года поместил в черный список весь мир (весь диапазон IP-адресов). В результате огромное число пользователей электронной почты во всем мире потеряли корреспонденцию за два дня - она отвергалась теми почтовыми серверами, которые использовали списки Osirusoft для борьбы со спамом.

Производители фильтров достаточно быстро реагируют на изменения тактики и стратегии спамеров, обучая программы распознавать все новые уловки. За 2003 год те или иные фильтры спама были установлены на большинстве публичных почтовых сервисов "большого" Интернета и Рунета в частности.

Спамеры ищут адекватный ответ и начинают использовать методы "**замусоривания**" текста для обмана фильтров, основанных на анализе содержимого писем. Наиболее часто используются подстановка латинских символов вместо кириллицы, замена текста изображениями, динамическое (в пределах одной партии писем) изменение содержимого писем.

Это приводит к удорожанию себестоимости спамерских рассылок, в таких условиях успешную рассылку могут провести только хорошо оснащенные спамерские конторы. Спамерский бизнес укрупняется, его клиентская база расширяется за счет малого бизнеса.

Любой пользователь Рунета мог видеть, что осенью 2003 года спамеры впервые решили **пожертвовать читаемостью писем** ради обхода фильтров. Специально сделанные грамматические ошибки, удвоение букв, мусорные концы слов позволяют сразу отличить "на глаз" спамерский мусор от обычного письма. Бич Рунета 2003 года – Центр американского английского осенью 2003 года заметно снизил активность и рассылает уже совершенно нечитабельные письма.

В результате борьбы щита и меча на первый план выходят **лингвистические методы** фильтрации спама, для которых не важно, с какого адреса пришло послание. Антиспамерское ПО разбирает содержимое письма в поисках сигнатур, характерных для "мусорных писем".

Меняется **тематика спамерских рассылок**: там, где приняты антиспамерские законы, число предложений товаров и услуг от малого бизнеса начинает падать, освобождая поле деятельности для мошенников и порнографов. Напротив, в Рунете происходит резкий рост числа рассылок от малого бизнеса. Налицо и широкое использование спама в политических кампаниях осенних выборов.

Рассылка спама постепенно становится не только асоциальной, но и **нелегальной деятельностью**. В 2003 году опасность спама признали законодательные органы ведущих стран мира. Законы против спама приняты Европейским союзом, Австралией, США. В России ведущими интернет- и ИТ-компаниями образована Национальная коалиция против спама, одним из направлений деятельности которой являются проекты поправок к законодательству (Закону о рекламе, Кодексу об административных правонарушениях и др.) и внесение их в Государственную Думу. Впервые в России в сентябре была проведена Первая национальная конференция "Проблема спама и ее решения".

Наш **прогноз на следующий год**, к сожалению, неутешительный. 2004 год будет годом пика спама. Мы предполагаем, что количество спама в ящиках пользователей достигнет своего пика весной-летом 2004 г. и составит 60-70% от всей входящей почты. Спам будет чрезвычайно технически изощренным, кроме того, начнется эпоха мобильного спама (SMS-спама).

Однако к концу 2004 года практически на всех массовых сервисах и в крупных компаниях будут внедрены те или иные эффективные фильтры спама. Кроме того, уже в первой половине 2004 г. в США и Западной Европе будут завершены первые успешные процессы против спамеров, а к осени 2004 года в России и Восточной Европе будут приняты национальные законы против спама. В результате этих мер поток спама должен пойти на убыль и в 2005 году заметно снизиться.

2. О нашем исследовании: как мы анализируем спам

Компания "Ашманов и Партнеры" является ведущим производителем антиспам-фильтров в России. Наши фильтры установлены на интернет-сервисах Mail.ru, в Петерлинке, РТКомм, РБК и многих частных компаниях. Ежедневно наши фильтры обрабатывают 10-15 миллионов писем, а наша Лаборатория "Спамтест" получает и анализирует примерно 100-150 тысяч различных спамерских писем в день.

Такой представительный поток данных позволяет нам охватить практически всю картину мирового и российского спама. Наши фильтры автоматически разбирают входной поток спама примерно по 550 рубрикам, так что тематическая и календарная картина спама оказывается полностью открытой для анализа.

В данном отчете мы использовали как статистические данные Лаборатории "Спамтест", так и данные наших коллег из США и Европы.

3. Спам: тенденция бурного роста

3.1. Доля спама в почтовых потоках мира

По данным исследований Radicati Group¹ ежедневно в мире рассылается 15 миллиардов спамерских сообщений. Мы оцениваем это количество чуть ниже – в 8-10 миллиардов. В 2003 году впервые сложилась ситуация, когда доля спама в почтовом трафике превысила долю обычных писем².

Компании, предоставляющие интернет-услуги (в том числе – почтовые службы), ежедневно классифицируют как спам от 50% до 80% всех получаемых почтовых сообщений.

Крупнейший зарубежный провайдер, компания AOL, сообщает о блокировке примерно 80% всей почты как UCE (Unsolicited Commercial E-Mail, "незапрошенные коммерческие сообщения") и Scam (незаконные предложения, мошенничество). А мировой лидер по продажам антиспам-услуг, компания BrightMail³ оценивает спамерский трафик как 56% процентов от всех почтовых потоков в Интернете, что на 16% больше, чем аналогичная оценка спам-трафика в декабре 2002 г.

¹ Международная аналитическая компания, специализируется на исследованиях в области средств коммуникации и IT-технологий; наиболее пристальное внимание в статистических исследованиях компании уделяется таким рыночным зонам, как США, Европа и страны Тихоокеанского региона

² Информация из пресс-релиза компании BrightMail, одной из ведущих зарубежных компаний в области разработки антиспамерского программного обеспечения

³ См. http://www.brightmail.com/pressreleases/121803_spam_2003.html

3.2. Доля спама в Рунете

Крупные российские интернет-компании приводят сходные или даже более высокие цифры относительно доли спама в общем почтовом трафике. По данным почтовой службы Яндекса⁴ доля спамерских писем в почтовых потоках составляет не менее 40%, при этом в отдельную группу выделяются так называемые "рассылки", доля которых может составлять до 20% почтового трафика. Таким образом, общий объем массовой незапрошенной корреспонденции может достигать 60-80%. По данным почтовых служб Рамблера и Mail.ru спам также занимает до 80% почтового трафика⁵.

Для Рунета 2003 год показателен резким, практически лавинообразным, ростом количества спама. Например, анализируемая нами статистика спамерских потоков почтовой службы Mail.ru показывает рост спамерского трафика на 50% за последние 6 месяцев 2003 г.

При этом почтовые службы традиционно оценивают объемы спама по статистике распознанных и **отвергнутых** писем, т.е. приведенные цифры зачастую свидетельствуют только о количестве того спама, который блокируется современными технологиями фильтрации. В действительности ситуация обычно еще хуже.

По нашим данным, существующие фильтры пропускают от 3-5% до 20-30% спама в зависимости от качества алгоритмов и скорости обновления баз, таким образом в публичных почтах доля спама может достигать 85-90%, особенно при эпидемиях – в момент ввода в действие новых спамерских технологий.

3.3. Рост ущерба, причиняемого спамом

Ведущие аналитические компании пытаются оценить ущерб от рассылки незапрошенных коммерческих сообщений. Ущерб заключается как в материальных затратах (оплата трафика, потеря времени), так и в моральных (раздражение и дискомфорт, вызываемые спамом). И то и другое оценить достаточно трудно, хотя примерная оценка материального ущерба возможна.

В частности, в проектах PEW Research Center приведена цифра ущерба в 50 долларов США в год на офисного сотрудника, что составляет \$1500 для компании со штатом 30 человек (данные рассчитаны для США)⁶. Для сравнения, в 2002 году материальный ущерб на одного сотрудника оценивался в \$25,6.

Оценки ущерба от спам у разных аналитических агентств разнятся, колеблясь от нескольких миллиардов до 20-30 миллиардов в год. В любом случае, это – миллиарды долларов в год.

Опираясь на данные наших фильтров и данные от ведущих почтовых служб Рунета, мы оцениваем ущерб от спама в Рунете в 150-200 миллионов евро, что складывается из расходов компаний на непроизводительно используемое рабочее время и затрат провайдеров и почтовых служб на обслуживание паразитного трафика.

⁴ См., например, мониторинг почты Яндекса (<http://mail.yandex.ru/monitoring/>) и страницу мониторинга спама на Mail.ru (<http://mail.ru/antispam.>).

⁵ Под данным пресс-релизов компаний, статей и интервью в электронных СМИ (compulenta.ru, lenta.ru и пр.)

⁶ Аналогичные данные приведены в аналитическом отчете компании Radicati Group "Anti-Spam Market Trends 2003 – 2007".

4. Спам – качественное развитие

Спам меняется не только количественно. Содержание несанкционированных коммерческих предложений и способы их распространения необычайно быстро модифицируются. Спамеры приспосабливаются к условиям времени – появлению и развитию антиспамерского ПО, законодательным мерам против спама и т.д. Изменяется во времени и контингент заказчиков и исполнителей спамерских рассылок.

4.1. Неравномерное распределение спама

Потоки спама распределяются по конечным пользователям неравномерно. Примерно четверть пользователей получают менее 5 спамерских сообщений в день, но данные опросов показывают, что только 7% пользователей утверждают, что они вообще не получают спама. В 2003 г. треть респондентов – пользователей электронной почты согласилась с тем, что спам составляет не менее 60% от общего объема их почтового трафика⁷.

Пока не выявлено корреляции между общим объемом почтового трафика отдельного пользователя и количеством приходящего в его почтовый ящик спама. Но существует прямая зависимость между временем существования адреса и количеством "незапрошенных сообщений" – чем дольше существует ящик, тем больше спама начинает приходить в него с течением времени.

4.2. Сезонные всплески спама

Рост количества спама не является линейной функцией. Динамика почтовых потоков содержит свои "пики" и "провалы". Спам – это, прежде всего, выгодный рекламный бизнес, и, как и любой другой бизнес, он подвержен "сезонным" всплескам и затишьям. В течение 2003 года наблюдалось несколько прогнозируемых всплесков спамерской активности, приходящихся на периоды "после праздников/отпусков", а также на периоды традиционного потребительского оживления, например, в канун Нового года. Это конец января - февраль, конец мая – начало июня, конец августа – сентябрь, ноябрь-декабрь.

Кроме того, с периодичностью раз в один-два месяца возникают значительные "незапланированные" всплески рассылок, обусловленные техническими нововведениями спамеров (подробнее о технических спамерских приемах – см. ниже). В этом случае компаниям-разработчикам антиспамерского ПО обычно требуется время для реакции на новые технические ухищрения спамеров.

4.3. Меняется содержание спама

Для мирового сообщества характерно снижение доли предложений товаров и услуг (по данным BrightMail – на 15%), что обусловлено развитием антиспамерской законодательной базы. Доля откровенно мошеннических предложений (scam) также снизилась – примерно на 6% по сравнению с 2002 годом.

⁷ По данным исследований, проведенных в рамках программы Pew Research Center. PEW Center – организация, объединяющая независимых гражданских журналистов. В рамках этой структуры проводятся многочисленные аналитические исследования по различным направлениям деятельности. Данные взяты из аналитического исследования "SPAM", проведенного в рамках исследовательской деятельности одного из филиалов организации – "PEW Internet & American Life Project" (www.pewinternet.com)

Доля предложений "для взрослых" остается стабильной – около 20% всего спамерского трафика. Отмечен резкий рост количества предложений и услуг, связанных с Интернетом и IT-технологиями, начиная с рекламы антиспамерских программ до предложений услуг по созданию, хостингу, дизайну, продвижению, раскрутке сайтов.

4.3.1. Распределение по тематикам

По данным компании BrightMail, лидера на рынке средств фильтрации спама, 92% спама распределяются по следующим тематикам:

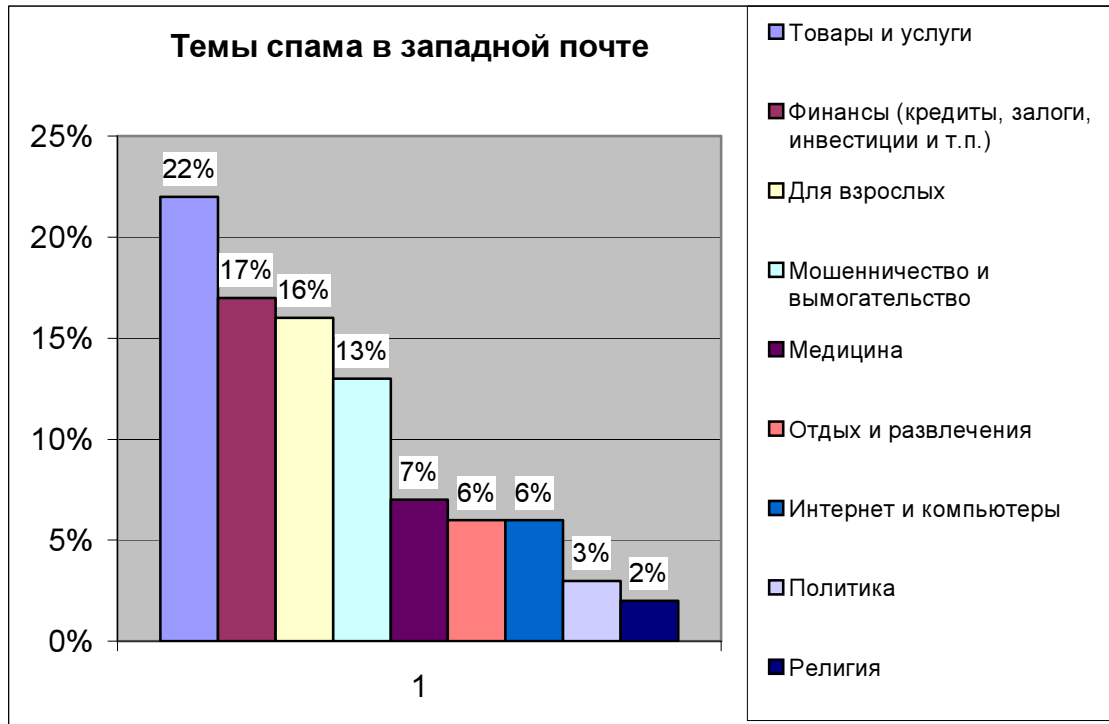


Диаграмма 1. Темы спама в западном Интернете

По данным Лаборатории "Спамтест", категория "Товары и услуги" в западном спае включают следующие подтемы в порядке частотности:

- Реклама средств для усиления потенции, увеличение половых органов,
- Дешевые медикаменты online,
- Сделки с недвижимостью, ссуды под недвижимость,
- Расходные материалы к принтерам, факсам и т.п.

Категория "Мошенничество и вымогательство" в первую очередь представлена так называемыми "нигерийскими письмами" (известными также как "Письмо 419"), содержащими просьбы о помощи в переводе, легализации, обналичивании крупных банковских сумм и пр. В последнее время по очевидным причинам появились также "иракские письма" того же свойства ("...я, вдова убитого американской ракетой генерала иракской армии, унаследовала тайный счет, на котором ...").

4.3.2. Тематическое распределение спама в Рунете

Развитие спама в Рунете в 2003 г. показало резкий рост количества предложений товаров и услуг, в основном, за счет русскоязычной рекламы, и, соответственно, снижения относительных долей предложений "для взрослых" и откровенного

мошенничества. Изменения касаются именно долевого распределения тематик. В количественном плане предложений "для взрослых" не стало меньше.

В Рунете широко представлены все перечисленные выше тематики спама (спам на английском языке), но к ним добавляются специфические "русскоязычные" рассылки, такие как:

- Предложения участвовать в семинарах/конференциях (маркетинг, PR, искусство переговоров, сбор долгов, пр.),
- базы данных с информацией о юридических и физических лицах,
- предложения услуг по спамерской рассылке,
- коммерческие предложения товаров и услуг (грузоперевозки, туры, недвижимость, окна, пр.)

Хорошо заметен сезонный характер русского спама – новогодние подарки, встреча Нового года, банкетные залы, летом – кондиционеры, зимой – обогреватели.

По данным Лаборатории "Спамтест", 85% спама в Рунете распределяется по следующим тематикам:

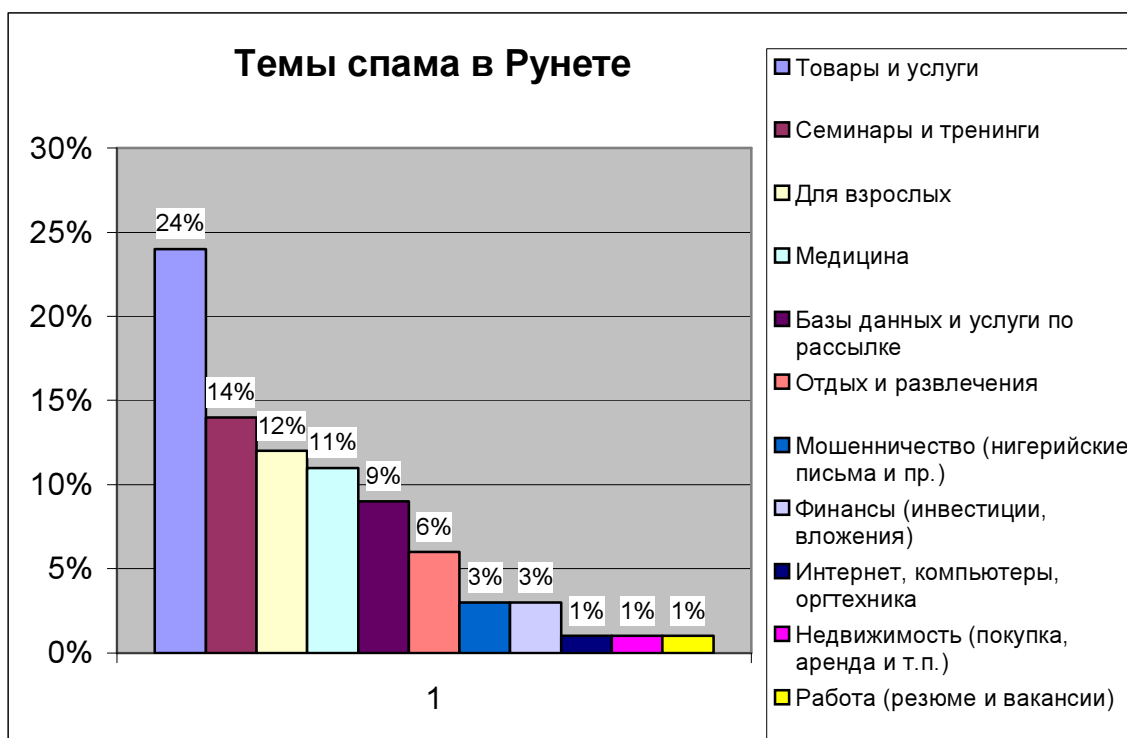


Диаграмма 2. Темы спама в Рунете

В диаграмме выше все данные даны без разделения спама по языкам (русский, английский).

Письма тематик "Семинары и тренинги", "Базы данных и услуги по рассылке" практически на 100% русскоязычные. В "Товарах и услугах" доля русскоязычных предложений равна примерно 60-70%.

Диаграмма ниже описывает тематическое распределение 95% русскоязычного спама. Для получения более детальной картины в отдельную рубрику выделена довольно частая тематика "Полиграфия".

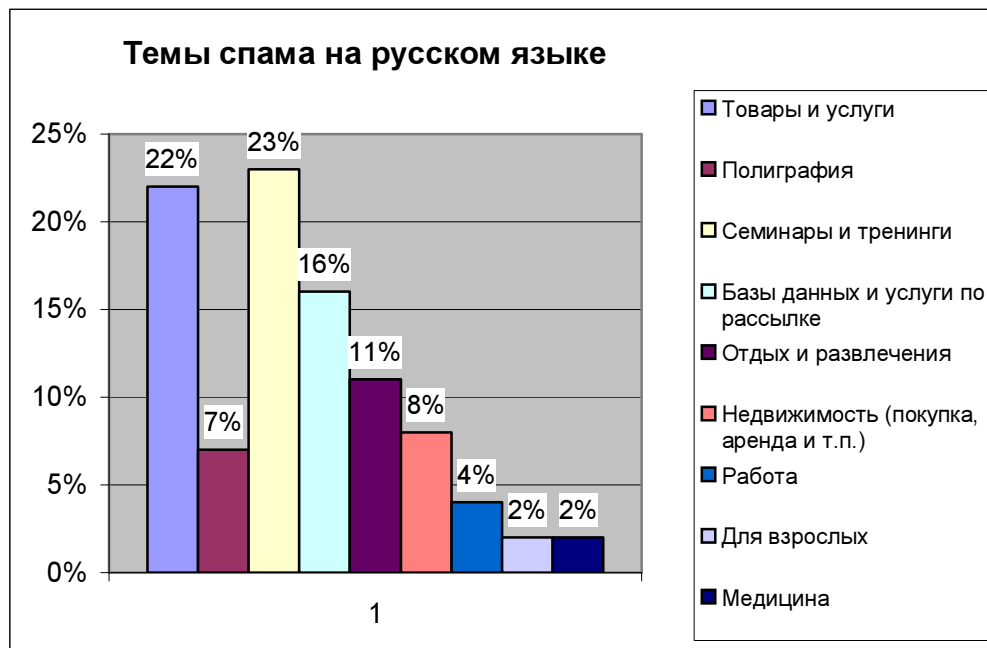


Диаграмма 3. Наиболее массовые темы спама на русском языке

4.4. Появление новых спамерских тем

4.4.1. Политический спам

Наши прогнозы про политический спам для Рунета, которые прозвучали летом этого года, полностью оправдались. Спам активно использовался в избирательной кампании 2003 года на всех уровнях. В спамерских посланиях упоминались большинство сколько-нибудь заметных политических партий и движений. В том числе рассылались агитационные сообщения, стилизованные под "личные" письма, например, спамерская рассылка, прошедшая за день до выборов, с агитацией против партии СПС.

Активно использовались спамерские технологии и на московских и региональных выборах. Наряду с электронной почтой применялись и сравнительно новые виды спама – через ICQ и SMS. Анонимность спама позволила использовать его как для распространения информации, так и для дезинформации с целью "подставить" конкурента.

К подобному "черному пиару" можно отнести мартовскую рассылку писем с предложениями организовать запись членов в партию "Единая Россия", вызвавшую бурю возмущения пользователей Рунета, а также письма якобы от депутатов партии "Яблоко".

Политический спам не обязательно "привязан" к выборам или другим политическим событиям. Например, прошедшая в октябре массовая рассылка с громким заголовком "Письмо президенту", насколько можно судить, имела целью заявить о существовании "Фонда помощи инвалидам" и о наличии у этого фонда определенной программы.

4.4.2. Спам, эксплуатирующий интерес к "горячим" новостям

Появилась разновидность спамерских рассылок, основанная на интересе пользователей к происходящему в мире. Типичным примером подобной рассылки может служить

письмо с заголовком "Saddam Hussein - Iraqi Most Wanted Cards", в котором предлагается приобрести колоду карт с изображением бывших иракских государственных и военных деятелей.

4.4.3. Предложения антиспамерского ПО

Во втором полугодии 2003 года широкое распространение получил спам с предложениями купить антиспамерское программное обеспечение. Первое впечатление, что борцы со спамом стали использовать методы противника для распространения своей рекламы – обманчиво. В большинстве случаев подобные письма – фальшивки, они содержат ссылки на сайты сомнительного содержания. Даже если предлагаемое на таких сайтах ПО служит для фильтрации спама, то его качество оставляет желать лучшего и не является продуктом ни одного из тех производителей ПО, именами которых прикрываются спамеры.

4.5. Изменение языкового соотношения спама в Рунете

Еще два года назад в Рунете рассылалось около 70% англоязычного спама, сейчас соотношение в среднем 50:50. Некоторые интернет-провайдеры даже склонны говорить о преобладании в почтовом трафике русскоязычной рекламы, что, безусловно, свидетельствует о росте квалификации российских спамеров и количества их российских заказчиков. В почтовых ящиках российских пользователей появились и "экзотические" языки – например, турецкий.

Растет доля писем на европейских языках, отличных от английского. Этот факт свидетельствует о том, что наши пользователи попали в зону интересов зарубежных рекламодателей.

Еще раз подчеркнем, что спам – это выгодный бизнес, и отдача от спамерской рассылки определяется не количеством адресов, по которым было разослано письмо, а количеством откликов на данное письмо. Рост интереса к российским пользователям – это признак того, что от них поступают отклики, удовлетворяющие заказчиков спама.

4.6. Заказчики и исполнители

В 2003 году наблюдались серьезные качественные и количественные изменения в социальной базе заказчиков спама. Из средства рекламы "теневого" бизнеса спам превращается в повседневный инструмент продвижения малого и среднего бизнеса. Низкий порог вхождения на "рекламный рынок" сделал спам наиболее привлекательным, а для начинающих коммерсантов порой и единственно доступным видом продвижения товаров и услуг на рынок.

Отсутствие реальной дешевой альтернативы спаму среди "законных" способов рекламы заставляет все большее число мелких и средних фирм обращаться к услугам спамеров.

Осенью 2003 года для нашего журнала Спамтест мы провели **опрос заказчиков спама** (взяв их телефоны из спамерских рассылок). К сожалению, никакой статистики с красивыми графиками построить на результатах опроса нельзя – 100% опрошенных в один голос отвечали ровно одно и то же: спам очень эффективен, раздражение интернет-пользователей не беспокоит, будем заказывать рассылки еще.

В свою очередь, исполнители спамерских рассылок матерятся и консолидируются. Рост денежных вливаний в эту теневую отрасль приводит к качественным изменениям в среде спамеров. Возросшая капитализация отрасли позволяет нанимать

профессиональных копирайтеров для лучшего оформления посланий и повышения процента отклика, а также – профессионалов в сфере интернет-технологий, способных усовершенствовать технологии распространения спама и создать серьезную угрозу антиспамерским фильмам.

Спам, как ни удивительно, становится одной из стандартных услуг, оказываемых обычными рекламными агентствами (естественно, не напрямую, а через субподрядчиков).

5. Спамеры на острие технологического прогресса

5.1. Появление профессиональных систем рассылок

По состоянию на конец 2003-го года, основная масса спама рассылается с помощью профессиональных систем – специализированного ПО, в разработку которого вложено очень много сил и средств.

Эти системы, в числе прочего, реализуют распределенную рассылку через зараженные троянскими компонентами пользовательские машины. По косвенным данным, используемые системы рассылки позволяют запоминать статус каждого адреса назначения и повторять попытки доставки через разные машины-посредники вплоть до момента успешной доставки. Эта особенность резко снижает эффективность черных списков адресов (RBL-систем).

5.2. Использование зараженных компьютеров пользователей

В 2003-м году основное количество спама рассылалось получателям не напрямую, а через посредство подключенных к Интернету пользовательских компьютеров. Чтобы пользовательская машина стала рассылщиком спама, на нее должно быть установлено "троянское" программное обеспечение, являющееся проху-сервером (по протоколу SOCKS или HTTP). Такое ПО попадает к пользователю несколькими возможными путями: через файлообменные сети, дыры в безопасности браузеров, заражение вирусом.

Пользовательский компьютер с таким троянским ПО (владелец компьютера об этом ПО не знает) может быть использован как для рассылки спама, так и для другой нелегальной активности (DDoS-атак, маскировки IP-адреса использующих его лиц и т.п.). Управляется подобное ПО через получение команд со специальных Web-серверов, либо же через интернет-чаты, то есть по IRC-каналам.

Можно с уверенностью утверждать, что в 2003-м году заражение пользовательских машин троянскими компонентами стало специализированным бизнесом, которым занимаются профессионально и с размахом; количество зараженных машин в мире составляет минимум несколько сотен тысяч.

5.3. Черные списки работают все хуже

Техническим следствием подобной технологии рассылок является устаревание метода "черных списков" (RBL-методов обнаружения спама). По состоянию на конец года, для рассылки спама ежедневно используется 20-50 тысяч **новых** (не известных антиспам-

системам) IP-адресов, преимущественно из сетей DSL и кабельных провайдеров США и Европы. Это количество включает в себя как новые зараженные машины, так и машины, получившие от своего провайдера (ISP) новый IP-адрес. В RBL-списки эти адреса попадают с задержкой (часы или даже дни), причем обнаруживаются и попадают в списки далеко не все адреса (от трети до половины).

Так как попытки доставки сообщения могут повторяться с разных IP до момента достижения успеха, а далеко не все используемые таким образом IP-адреса содержатся в популярных "черных списках" RBL, то зачастую использование RBL ведет лишь к увеличению количества отвергнутых сообщений, а общее количество прошедшего сквозь фильтр спама не меняется.

5.4. Типовая "спам-машина" образца 2003 г.

К середине 2003 г. сформировался механизм спамерской рассылки, обладающий определенными характерными признаками, своеобразная типовая "спам-машина":

- участие в рассылке нескольких десятков тысяч "затронутых" пользовательских машин;
- наличие профессионального спамерского ПО и автоматическое скачивание обновлений данного ПО;
- автоматическая модификация писем при посылке (в том числе, модификация графических изображений)
- "отладка" письма в реальном времени на почтовых ящиках публичных почтовых систем: многократная посылка разных вариантов сообщений (пока одно из них не "пробьет" антиспамерский фильтр)
- организация постоянного обмена информацией между спам-серверами (через чаты и удаленные сайты).

5.5. Спамеры перешли к "ответным" ударам

5.5.1. Организация распределенных атак на RBL-системы

В течение лета-осени 2003 г. отмечались многочисленные распределенные атаки на наиболее полезные RBL-системы, которые привели к временной неработоспособности систем SPEWS и SORBS и постоянному закрытию RBL-сервиса Osirusoft. С 1-го декабря закрылся сервис Easynet.NL, хотя причина закрытия не разглашается.

5.5.2. Организация спамерских "псевдорассылок"

С осени 2003 года появился новый вид массовых анонимных рассылок, не содержащих никаких предложений. Чаще всего в тексте подобных писем содержится бессмысленный набор символов или проставлена дата, или же письмо вообще не имеет ни текста, ни аттачмента. Необходимость подобных рассылок активно обсуждалась на форумах спамеров. Очевидно, эти рассылки используют время простоя спамерского ПО (когда нет заказа от клиентов), а целью их является общее "замусоривание" почтового трафика и затруднение работы антиспамерского ПО, особенно вероятностных статистических фильтров (байесовских).

5.6. Использование спамерских технологий для рассылки вирусов

В июне 2003 года для распространения компьютерного вируса впервые были использованы спам-технологии массовой рассылки копий вируса с анонимного

почтового сервера. Речь идет о повальной "эпидемии" новой модификации сетевого червя "Sobig". Использование спамерских технологий позволило вирусу практически мгновенно распространиться по сотням тысяч компьютеров. О том, что данная модификация "Sobig" распространялась как спам, свидетельствуют следующие факты: большинство разосланных зараженных писем в качестве адреса отправителя содержат подставные адреса, которые автоматически генерируются спамерским ПО; IP-адреса источников зараженных сообщений характерны для автоматических спамерских рассылок. С этого момента попытки подобных вирусных атак, производимых с помощью профессионального спамерского ПО, периодически повторяются.

5.7. Новые технические приемы обхода фильтров

2003 год характеризуется активным внедрением антиспамерских фильтров. В частности, в мае этого года почтовая служба Mail.Ru установила у себя почтовые фильтры⁸, использующие не только формальные правила отслеживания спама, но и контентный анализ содержимого писем. Рамблер и Яндекс также внедрили новые фильтры спама в своих почтовых системах⁹. В результате существенная часть спама в Рунете (до 50%) стала успешно распознаваться и фильтроваться.

Спамер были вынуждены искать новые технические средства борьбы с антиспам-фильтрами. К середине года уже появились принципиально новые технические "трюки" спамеров.

5.7.1. Использование графики

Летом 2003 г. появились первые случаи спамерских рассылок, в которых рекламный текст сообщения был представлен в виде изображения (графического файла). Началось с замены на картинки отдельных букв, но довольно быстро спамеры перешли к полностью графическим письмам.

Наиболее активно в рассылках представлены форматы *.gif и *.jpeg, что связано с хорошей "сжимаемостью" картинок в этих форматах.

К августу 2003 г. количество спама с графикой выросло в геометрической прогрессии, но затем оно стало постепенно уменьшаться, и к настоящему времени ситуация стабилизировалась. Доля писем с "картинками" в среднем составляет всего несколько процентов общего потока спама, и даже в случае особо массовых рассылок не превышает 6-7% от общего спамерского трафика, что обусловлено следующими факторами:

- в подавляющем большинстве случаев для каждого письма из спамерской рассылки используется один и тот же набор картинок, что позволяет сразу же распознать массовую рассылку при помощи простейших детекторов массовости;
- создание уникальных изображений для каждого письма требует наличия специализированного ПО, при этом упаковка большого количества изображений является длительной операцией и существенно снижает скорость рассылки писем. А это, в свою очередь, облегчает задачу отслеживания источников данной рассылки.

⁸ Фильтр Антиспам Касперского (разработанный ЗАО "Ашманов и Партнеры").

⁹ На Яндексе детектор массовых рассылок на основе механизма "шинглов" был установлен в ноябре 2002 года.

5.7.2. Модификация текста сообщения

Один из популярных и наиболее перспективных технических приемов спамеров – это всевозможные модификации текста сообщения, а именно, следующие.

5.7.2.1. Добавление к исходному тексту сообщения случайных текстовых блоков

Прием состоит в автоматической генерации случайных последовательностей символов, слов или целых фрагментов текста и добавлении их к исходному письму. В большинстве случаев подобные искусственные "вкрапления" в текст письма располагаются в конце сообщения, т.е. вне зоны активного пользовательского внимания. В результате качество восприятия текста практически не ухудшается. Не страдает и рекламная составляющая письма.

Такие приемы могут обмануть только простейшие фильтры, основанные на расчете и сравнении "строгих" контрольных сумм сообщений. Современные фильтры используют более сложные методы, чем простое сравнение строгих контрольных сумм.

5.7.2.2. Модификация слов в тексте письма

Приемы, основанные на модификации написания отдельных слов, в той или иной степени ухудшают "читаемость" письма. К таким приемам относятся:

- использование небуквенных символов для разбиения слова (например, пробелов или точек, как в слове "v.i.a.g.r.a");
- использование одинаковых по написанию букв разных алфавитов (например, буква "эс" русского и "си" латинского алфавитов не отличаются внешне, но использование случайных замен на латинские буквы в русских словах может привести к существенному ухудшению качества работы лексических фильтров);
- произвольное удвоение букв в словах или "дребезг клавиатуры" в терминологии спамеров ("удвоение");
- перестановка букв в словах ("пеерстанвока").

С некоторыми из этих способов антиспамерские фильтры могут справиться достаточно легко (тот же "дребезг клавиатуры"), с другими ситуация сложнее, но в любом случае страдает "читаемость" сообщения – адресату подобный текст сложнее прочитать, чем текст без ошибок.

Соответственно, можно ожидать, что рекламный отклик от таких сообщений будет заметно меньше, что вряд ли обрадует заказчиков рассылок. Скорее всего, эти приемы не смогут распространиться слишком широко.

5.7.3. HTML-трюки

Технические приемы, основанные на возможностях использования языка HTML, и на отличиях в отображении текстов HTML различными браузерами, можно условно поделить на две группы:

- добавление в сообщения "невидимого" текста (например, набранного тем же цветом, что и фон сообщения);
- использование различных размеров шрифта – крупно отображаются значимые фрагменты текста, а мелким, практически невидимым шрифтом набирается случайный текст.

Спамеры пытаются использовать особенности в показе текста сообщения в формате HTML у широко распространенных браузеров (Internet Explorer, Mozilla, Opera), чтобы создать ситуацию, когда один и тот же текст по-разному воспринимается человеком и фильтром. В результате контентные фильтры не срабатывают, так как пытаются обработать текст, значительно отличающийся от того, который видит пользователь.

Современные спам-фильтры включают в себя разборщики файлов в формате HTML (включая таблицы стилей CSS) с детекторами невидимого текста. На текущий момент приемы по созданию двойственного представления одного и того же документа довольно эффективно распознаются и обрабатываются современными средствами фильтрации.

6. Прогноз на 2004 г.

6.1. Дальнейший рост объемов спама

Ведущие аналитические компании прогнозируют дальнейшее увеличение потоков спама, которое угрожает принять лавинообразный характер и привести к существенному ухудшению коммуникативных свойств электронной почты. Компания BrightMail прогнозирует на 2004 год увеличение доли спама в мировом почтовом трафике минимум еще на 10%.

Повсеместно выражается озабоченность тем, что пользователи начинают испытывать серьезный дискомфорт при использовании электронной почты. Данные опросов показывают, что среднестатистический пользователь, чья работа не связана с Интернетом и IT-технологиями, готов существенно сократить объемы электронной переписки или даже вообще отказаться от использования электронной почты, чтобы избежать проблемы спама.

Наш собственный прогноз на следующий год – также неутешительный. 2004 год будет годом пика спама. Мы предполагаем, что количество спама в ящиках пользователей достигнет своего пика уже зимой-весной 2004 г. и составит 60-70% от всей входящей почты. Спам будет чрезвычайно технически изощренным, а также, возможно, плохо читаемым и странно выглядящим. Одновременно начнется эпоха мобильного SMS-спама.

Однако к концу 2004 года практически на всех массовых сервисах и в крупных компаниях будут внедрены те или иные эффективные фильтры спама. Кроме того, уже в первой половине 2004 г. в США и Западной Европе будут завершены первые успешные процессы против спамеров, а к осени 2004 года в России и Восточной Европе будут приняты национальные законы против спама. В результате этих мер поток спама должен пойти на убыль и в 2005 году заметно снизиться.

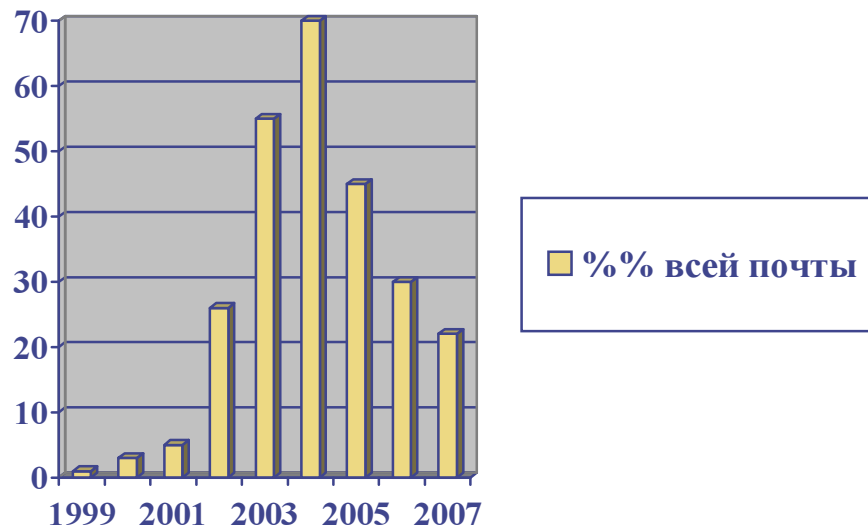


Диаграмма 4. Прогноз по доле спама в почте на 2004-2007

6.2. Совершенствование технических возможностей спамеров

Скорее всего, наибольшие проблемы в ближайшее время будут создавать сети из компьютеров, зараженных троянскими программами. Можно также предположить дальнейшее объединение усилий авторов вирусов со спамерами и создание коммерческих вирусов.

В связи с развитием технологий фильтрации спама, спамеры, безусловно, будут вынуждены изобретать новые "трюки", предназначенные для обмана фильтров. В настоящее время наиболее перспективным для спамеров представляется направление, связанное с использованием возможностей языка HTML (невидимый текст и тому подобное) и использованием скриптов в письмах.

Кроме того, мы ожидаем развития технологии автоматической генерации писем, которые формально различаются (тексты разные), но по смыслу совпадают (содержание писем передает одно и то же рекламное сообщение).

6.3. Консолидация и структурирование спамерского сообщества

Совершенствование средств фильтрации спама естественным образом привело к усложнению рассылки спамерских писем. Сейчас успешная спамерская рассылка (то есть такая рассылка, где велико не только количество отправленных писем, но и количество писем, доставленных получателям) характеризуется следующими свойствами:

- использование сложного программного обеспечения, генерирующего уникальные сообщения для каждого получателя;
- привлечение профессиональных редакторов для создания большого количества вариантов одного и того же сообщения;
- круглосуточное слежение за состоянием рассылок и их прохождением сквозь фильтры.

В результате новичку в этой области стало значительно сложнее организовать рассылку спама. Кроме того, возрастает себестоимость рассылки.

Можно с большой долей уверенности сказать, что в следующем году спамерскими услугами, направленными на русскоязычных пользователей сети Интернет, смогут заниматься только несколько **крупных организаций спамеров**, так как мелкие спамеры будут не в состоянии ни обеспечить постоянное развитие своих технических средств, ни поддерживать сложную внутреннюю инфраструктуру для рассылки спама.

Инфраструктура рассылки (сервера, хостинг, ПО для спамеров) несомненно, продолжит **миграцию в страны третьего мира**, где контроль за рекламными рассылками не такой строгий.

Ясно, что продолжит увеличиваться разделение труда (расслоение индустрии спама), связанное с разделением труда: различные виды деятельности будут выполняться разными лицами – хостинг серверов и ПО для рассылки, сбор и проверка адресов, написание ПО для рассылки, захват пользовательских машин и управление ими, и так далее, и тому подобное.

6.4. Клиенты спамеров

Мы предполагаем, что в 2004 г. в Рунете число клиентов спамеров будет быстро расти. Поскольку донести до малого бизнеса идею о неэтичности спама вряд ли реально, а закон РФ о спаме вряд ли будет принят раньше середины 2004 г., то малый бизнес как не знал ничего об асоциальном характере спама, так и не будет знать еще год-полтора.

В то же время поворот малого бизнеса к Интернету и высокая эффективность рассылок будут все сильнее привлекать клиентов к спамерам, особенно в таких областях как туризм, обучение, семинары и выставки, грузоперевозки и транспорт, недвижимость, строительство и ремонт.

7. Приложение: первые спам-итоги 2004 года

Как и следовало ожидать, в празднично-отпускной период 29 декабря – 11 января спама было существенно меньше, чем обычно.

Особенно резко заметен спад в русскоязычном спаме. Скорее всего, здесь влияют два фактора: а) спамеры тоже люди и отдыхают, б) на этот период нет заказов, т.к. потенциальные потребители находятся в отпусках, загулах и т. п.

Процентный объем русскоязычного спама в этот период не превышал 15-20%. Для сравнения, в начале декабря количество русскоязычных и англоязычных писем было примерно одинаковым.

На этом фоне оказались очень заметными письма, не содержащие "разумного" текста, т.е. полностью "мусорные" (внутри письма только случайные последовательности символов). Рассылки такого рода с темами наподобие "some garbage for ..." прошли во всех анализируемых нами почтовых потоках.

Тематическое распределение спама в "мертвый сезон" примерно следующее:

1. Англоязычные письма:

В основном представлены "вечные" тематики "Для взрослых", "Виагра" и "Получи кредит на замечательно выгодных условиях". Предложений товаров и услуг практически нет.

2. "Русскоязычные" письма:

- а) огромное количество предложений по организации e-mail рекламы и спамерских рассылок. Таким образом, на праздниках спамеры ищут клиентов.
- б) яркое проявление специфики нашей российской действительности: письма с предложениями полисов ОСАГО, в том числе и от достаточно известных страховых компаний, которым полагалось бы воздерживаться от подобных методов рекламы (например, предложения от компании "Наста").
- в) сезонные предложения: обогреватели для дома, подогрев для автомобильных сидений.

С 11-12 января 2004 началось легко объяснимое резкое оживление деятельности спамеров и рост числа "коммерческих" рассылок.