# Захист інформації в інформаційних комунікаційних системах

УДК 004.056

В.Г. Абдуллаев[1,2]

[1] *Азербайджанская государственная нефтяная академия, Баку*
[2] *Институт кибернетики НАН Азербайджана, Баку*

## ЗАЩИТА ОТ СПАМА В ИНТЕРНЕТ-ПРОСТРАНСТВЕ

*В статье рассмотрены основные методы и правила для эффективной борьбы с рекламными сообщениями. Также рассмотрены методы фильтрации почтовых сообщений на стороне сервера. И предложены варианты противодействия способам обхода методов фильтрации и защиты от рекламных сообщений.*

***Ключевые слова:*** *спам, рассылка рекламных сообщений, методы фильтрации.*

### Введение

СПАМ – это сообщения рекламного характера, которые доставляются без согласия пользователя, а также сообщения для мошеннических целей. Количество пользователей в сети Интернет с каждым годом увеличивается, в 2011 году – 718 миллионов, а в 2012 – уже 1,3 миллиарда пользователей Интернет [1]. Это связано со многими факторами, такими как удешевление оборудования (как результат цена доступа к сети снижается), активное распространение планшетных компьютеров и смартфонов (пользователи мобильного интернета). Доля спама в мировом трафике составляет почти 80% за 2011 год [2]. В 2012 году общее количество обнаруженных и удаленных сообщений составляет 65 миллиардов комментариев [3]. Как показывает статистика, уровень спама к концу 2012 года значительно возрос. На данный момент уровень спамовских комментариев превысил показатель 120 миллионов комментариев в день.

На рост спама повлияло массовое появление незащищенных сайтов, вики и форумов. Также люди, которые рассылают спам, начали активно использовать нелегальные методы, такие, как взлом сайтов, заражение компьютеров пользователей для создания ботнетов (сеть зараженных компьютеров и серверов, которые используются злоумышленниками в целях нанесения вреда) с целью рассылки спама. Значительный рост также спровоцировало увеличение трафика из Китая – это связано с продвижением подделок известных брендов.

С ростом популярности сервисов мгновенных сообщений и социальных сетей также растет количество спама в данных сервисах. Также отмечается рост спама в смс сообщениях. Убытки, которые приносит спам, колоссальные. Это – время, перегруженность оборудования и как результат – снижение срока эксплуатации. Все это приводит к финансовым потерям как организаций, так и государственных учреждений.

### Постановка задачи

Рассмотреть правила и разработать методы защиты e-mail от спама. Учитывая спам, который с каждым годом увеличивается в объёме и количестве, а также то, что усовершенствуются приемы обхода разных методов защиты, необходимо также постоянно усовершенствовать методы защиты. Соблюдение простых правил обеспечит уменьшение количества спама. Также необходимо учесть спам, который публикуется на сайтах и форумах в комментариях. Разработать противодействия способов обхода спам фильтров.

### Правила использования e-mail адресов в Интернете

Один из надежных методов, который, в принципе, понизит количество спама на электронный адрес, и затруднит заполучить адрес злоумышленниками – это соблюдение простых правил:

- Не следуют публиковать свой электронный адрес на общедоступных сайтах в открытой форме. Можно использовать специальные символы, что затруднит его распознавание. Также можно использовать адрес в виде картинки.
- Большинство пользователей имеют аккаунты в социальных сетях. А учитывая последнюю тенденцию, что на сайтах очень часто используется авторизация через социальную сеть, в таком случае лучше воспользоваться аккаунтом социальной сети.
- Также не стоит использовать адрес при регистрации на малоизвестных форумах и сайтах.
- Можно завести специальный адрес, для регистрации на форумах и сайтах, или использовать

службы для получения одноразовых адресов, к примеру сервис – http://mailinator.com/.

- Не следуют отвечать на спам, или переходить по ссылкам из письма, в том числе на ссылку, что обеспечивает отписку от рассылки. Как правило, данными действиями подтверждается реальный адрес. Также не следует открывать вложения.
- Желательно отключить загрузку картинок, которые в письме, чтоб не отслеживалась активность пользователя.
- При получении ссылки от неизвестного человека или от контакта, который находится у вас в списке, но ссылка вызывает подозрение, лучше отказаться от перехода по ней.
- Необходимо создавать длинные имена адресов, к примеру, который состоит из фамилии и имени, чтоб исключить метод подбора адреса случайными генераторами.

Выполнение простых правил и осторожность обеспечивают частичную защиту от спама, а также персонального компьютера, который может стать одним из узлов мошеннической сети.

## Способы защиты e-mail адресов и Веб-страниц

Классическая схема работы почтовых служб показана на рис. 1.

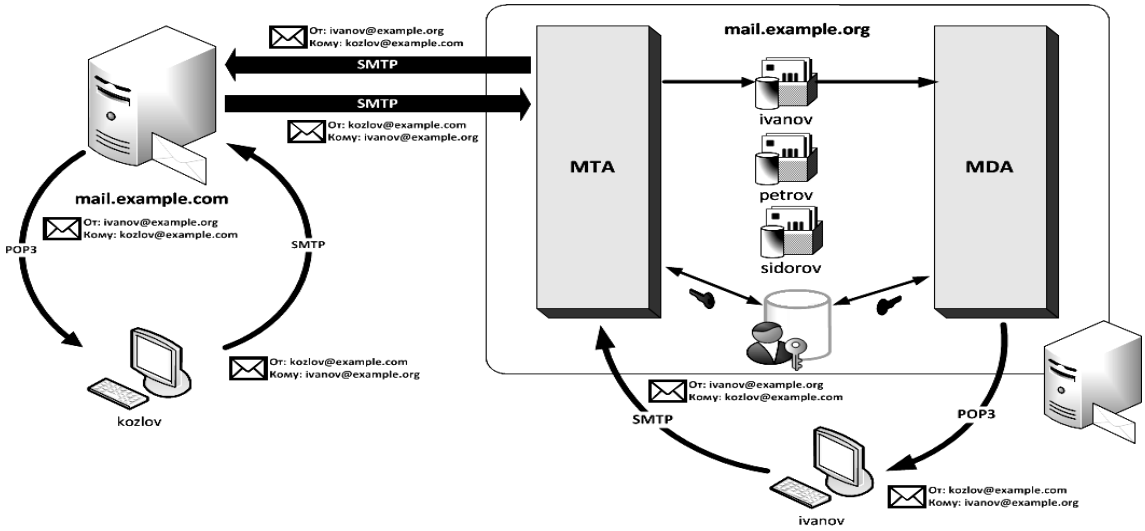


Рис. 1. Классическая схема работы почтовых служб
(MTA – Mail Transfer Agent – агент пересылки почты; MDA – Mail Delivery Agent – агент доставки почты)

Для того, чтоб защитить e-mail адреса, которые размещены на сайтах, есть разные способы и правила, которые реализуются исключительно технически, или соблюдение элементарных действий. Самое главное – это защита от ботов (автоматических программ (скриптов), предназначенных для сбора информации или отправки сообщений).

На большинстве Веб-страниц есть формы обратной связи для написания обращений, жалоб и так далее, или в блогах, комментариях к статьям. Самым распространённым и относительно надежным является размещение CAPTHA (*Completely Automated Public Turing test to tell Computers and Humans Apart* – автоматизированный текст Тьюринга для определения различий компьютер или человек) [4]. В основе данного метода лежит задание такой задачи, которую может решить только человек, к примеру, могут быть изображения искривлённых символов, или изображения математической задачи, как правило, сложение, автоматические скрипты не могут распознать искаженный текст, но это может сделать человек. Также есть варианты модифицированных примеров, таких как посчитать количество рисунков, с изображением определенного образа.

Сейчас существует достаточно способов обхода CAPTHA:

- Создание базы данных ответов или получение базы данных нелегальным путем. Некоторые разработчики используют готовую базу данных заданий и ответов, то есть задачи не генерируются случайным образом. Поэтому злоумышленники могут в ручном режиме сформировать базу данных или скачать ее. Противодействие – не создавать базы данных, а задания генерировать случайным образом.
- Неквалифицированное написание скрипта, что приведет при определенном формировании запроса к странице получать правильный ответ. Решение – использовать готовые скрипты, которые себя зарекомендовали, как надежные, или обращается к профессиональным исполнителям.
- Автоматическое распознавание возможно в том случае, если достаточно неискаженная или не завуалированная картинка с заданиями. Также использование только одного метода маскировки задания. Это все способствует разработке метода автоматического распознавания. Решение – использовать разные методы маскировки, которые будут меняться в произвольном порядке.

- Автоматический подбор вариантов ответов. Ответ на задание автоматически подбирается. Для защиты от данного метода служит блокировка IP адреса или аккаунта на определенное время, при повторе полная блокировка без восстановления.
- Ручное распознавание. Специальные сервисы, которые используют человеческий ресурс для распознавания. Данный способ обхода обойти, практически, не реально. Если отслеживать с какого адреса или аккаунта приходят эти сообщения, временно блокировать, а также ввести определенное время для ввода ответа. Как правило, используются разные данные, поэтому необходимо в ручном режиме модерировать сообщения.

Дополнительными методами борьбы с нежелательными сообщениями может быть запрет анонимных комментариев, разрешение комментариев только со стороны зарегистрированных пользователей, или авторизация через социальные сети. Также использование надёжных скриптов, что обеспечивает минимальное количество проблем в безопасности системы. Также запрет прямых публикаций сообщений, разрешение публикаций только после одобрения администратором.

Для фильтрации сообщений на Веб страницах, можно использовать фильтры для фильтрации сообщений по ключевым словам. Принцип действия данного скрипта в следующем: после того, как пользователь отправил сообщение, скрипт анализирует его, и если сообщение содержит ключевые слова или URL, которые есть в базе данных скрипта, сообщение не публикуется, а отправляется администратору на проверку.

## Методы фильтрации почты на почтовых серверах

Для фильтрации почтовых сообщений, на сервере можно использовать черные списки, серые списки, выставлять рейтинг пользователю, фильтровать сообщения по домену отправителя, а также по ключевым словам в теме и теле письма.

Существуют черные списки e-mail адресов и IP – это списки, в которые включены данные пользователей и систем, которые были замечены в рассылке спама или вредоносных сообщений. Сервер при получении нового сообщения автоматически определяет, не внесен ли пользователь в эти базы данных. Если в рейтинге они существуют, такие сообщения автоматически отправляются в папку спама или удаляются, в зависимости от настройки системы. Данные списки получили название DNSBL (DNS Black List). Данный метод утратил свою актуальность из-за того, что злоумышленники, как правило, используют пользовательские адреса и компьютеры. И после внесения их в данные списки пользователи долгое время не могут отправлять сообщения.

Также возможна автоматическая фильтрация (СПАМ фильтры), как на стороне сервера, так и на стороне клиента. Один из подходов заключается в анализе содержимого письма (по ключевым словам), и в зависимости от содержания делается вывод. Один из применяемых методов – статистический анализ содержимого письма, как правило, используется байесовский метод фильтрации спама. Суть этого метода заключается в анализе слов в теле письма на возможность (вероятность) его отношения к спаму [5], после чего делается вывод. В начале использования данного метода необходимо провести обучение фильтра на выявления спама. При активном и правильном обучении эффективность фильтрации спама можно довести до 95%, но для обеспечения необходимо постоянно проводить обучение. В последнее время популярным стал метод серых списков. Суть его заключается в том, что при первой попытке отправить письмо, сервер отвечает ошибкой. Программы для рассылки спама не умеют оперативно обрабатывать такие ситуации. Поэтому, пока они повторно начнут отправлять, очень высокая вероятность того, что они будут находиться в черных списках. Данный метод дает эффективность до 90%. Дополнительной мерой защиты от спама является запрос PTR-записи. PTR-запись связывает IP-адрес с именем домена (рис. 2).

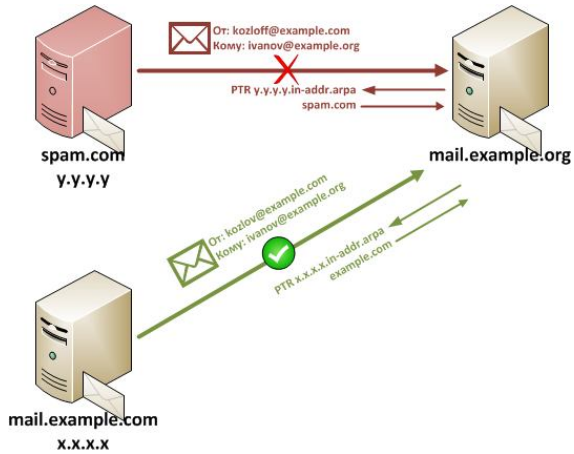


Рис. 2. Пример запроса PTR

Запросив PTR, MTA примет почту только в случае совпадения IP с именем домена. Учитывая, что спам, как правило, приходит с IP, который не совпадает с именем домена, защита в данном случае достаточно эффективна.

## Дополнительные методы защиты

В почтовые сервера встраиваются модули для определения признаков массовой рассылки. Эти модули подсчитывают контрольную сумму письма и проверяют на серверах служб Razor и DCC. Если встречаются с аналогичными контрольными суммами письма, большая вероятность, что это спам.

Ужесточаются требования к письмам отправителя: проверка доменного имени, обратного адреса, IP адреса компьютера, с которого идет рассылка.

## Альтернативные методы защиты

Каждое рекламное сообщение имеет в себе слова и слоганы, которые составляют части рекламного сообщения. К примеру «Купите», «лучшее предложение», и так далее. Проведя анализ почтового сообщения, кроме темы сообщения, можно с точностью определить, сообщение является рекламным или нет. Аналогично данному методу работают системы распознавания плагиата, когда ищутся части сообщения, которые взяты из других источников.

В данном методе есть ряд недостатков. Прежде всего, что во время обучение системы, оператор будет видеть чужие сообщения, проверяя соответствия оценки системы. Вторая проблема, это защита конфиденциальной информации, но в случае корпоративного сектора, это не является ключевой проблемой. Третья – затраты дополнительных ресурсов на обработку информации, увеличение затрат. Но, несмотря на ряд недостатков, данный метод может выступить эффективным методом борьбы с спамом.

## Выводы

Учитывая постоянный рост спама, можно сделать вывод, что данный метод продвижения товаров и услуг приносит выгоду заказчикам. Поэтому не стоит ожидать понижения количества спама в ближайшее время. Выполнение простых правил поведения в сети Интернет, как правило, значительно снизит объем получаемой почты. В результате, можно сказать, что все зависит от поведения пользователя. И за ним стоит выбор, следовать этим правилам или нет.

Достаточно эффективным и распространенным методом борьбы со спамом есть CAPTHA. Как показывает статистика, в 2011 году, ежедневно приблизительно вводится 200 миллионов CAPTHA во всем мире [6]. Данный метод хорошо зарекомендовал себя в формах обратной связи – комментариях, но не дает гарантии полной фильтрации рекламных сообщений. Использование специального программного обеспечения и методов повышает эффективность фильтрации сообщений. Но, как правило, все методы требуют постоянного усовершенствования, потому что практически все, кто занимается рассылкой нежелательных сообщений, усовершенствуют методы обхода систем защиты.

Нужно понимать, что спрос формирует предложение. Если предприниматели будут дальше заказывать рассылку спама, а пользователи откликаться на рекламные сообщения, спрос будет расти и объем спама также будет увеличиваться. Не стоит забывать о юридических аспектах – в некоторых странах приняты законы об уголовной ответственности за рассылку спама. Но простые правила поведения и использование эффективных методов защиты в совокупности принесут результат, и количество получаемого спама уменьшится. Также желательно постоянно проводить обучение систем на повышение их эффективности.

Комбинация вышеперечисленных методов защиты даст значительное снижение нежелательных сообщений, а также снизит нагрузку на сервера и сетевой трафик, и не будет отнимать время у пользователей.

## Список литературы

*1. The statistics portal [Электронный ресурс]. – Режим доступа к ресурсу: http://www.statista.com/statistics/74592/quarterly-worldwide-smartphone-sales-by-operating-system-since-2009.*

*2. Компьютеры и огротехника. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.computery.ru/news/news2010.php?nid=8302.*

*3. A Spammy Year in Review. [Электронный ресурс]. – Режим доступа к ресурсу: http://blog.akismet.com/2012/12/21/a-spammy-year-in-review.*

*4. Completely Automated Public Turing test to tell Computers and Humans Apart. [Электронный ресурс]. – Режим доступа к ресурсу: http://ru.wikipedia.org/wiki/CAPTCHA.*

*5. Байесовская фильтрация спама. [Электронный ресурс]. – Режим доступа к ресурсу: http://ru.wikipedia.org/wiki/Байесовская_фильтрация_спама.*

*6. Welcome to the new TED.com. [Электронный ресурс]. – Режим доступа: http://www.ted.com/ talks.lang.ru/luis_von_ahn_massive_scale_online_collaboration.html.*

*Поступила в редколлегию 21.01.2015*

**Рецензент:** д-р техн. наук, проф. С.И. Юсифов, Азербайджанская государственная нефтяная академия, Баку.

### ЗАХИСТ ВІД СПАМУ В ІНТЕРНЕТ-ПРОСТОРІ

В.Г. Абдуллаєв

*У даній статті розглянуті основні методи і правила для ефективної боротьби з рекламними повідомленнями. Також розглянуті методи фільтрації поштових повідомлень на стороні сервера. І запропоновані варіанти протидії способам обходу методів фільтрації і захисту від рекламних повідомлень.*

***Ключові слова:*** *спам, розсилка рекламних повідомлень, методи фільтрації.*

### ANTI-SPAM PROTECTION ON THE INTERNET SPACE

V.H. Abdullayev

*In the article main methods and rules for effective control of advertising messages are considered. Methods of mail messages filtering on the side of server are also considered. And the options against the ways of bypassing the filtering and protection of advertising messages are offered.*

***Keywords:*** *spam, advertising messages, filtering method.*