

# О безопасности сайта замолвите слово

**Константин Онищенко,**  
директор по развитию агентства интернет-рекламы «Идеал»

Сфера интернет-коммуникаций — одна из немногих сфер, увеличивших динамику развития во время кризиса. Инвестиции в интернет-составляющую бизнеса окупаются быстрее офлайновых, и спрос на разработку веб-приложений только возрастает. Однако любой коммерческий сайт подвержен рискам. Особенно, если он «мозолит глаза» конкурентам.

## Шпионаж и кражи

**С** интернет-вирусами сталкивался каждый. В основном их считают забавой неадекватных программистов, а наибольший вред, который от них ожидают — это уничтожение данных на компьютере или необходимость переустановки операционной системы, программ и драйверов. На самом деле запуск вирусов в Интернете все больше приобретает мошеннический характер. Те же вирусы типа «троян» могут запускать адресно с целью похитить пароли доступа к управлению сайтом и FTP, пароли к аккаунтам в социальных сетях или оболочке интернет-банкинга. Попав в компьютер, на котором содержатся файлы с паролями, вирус находит нужную информацию и передает ее мошеннику через Интернет. Даже если пароли содержатся не на жестком диске, а у вас в

памяти, разновидность вируса способна считывать вводимые на клавиатуре символы.

Завладев доступом к CMS сайта и FTP, мошенник может уничтожить или украсть информацию, разместить компрометирующие фото или тексты. И годами создаваемую репутацию можно потерять за несколько часов. Случаются кражи исходного кода сайта, например, какого-нибудь эксклюзивного модуля. Также хакер может разместить в коде сайта вирус, который быстро заметят поисковые системы. Дальнейшие действия поисковиков — это предупреждение пользователей о том, что веб-страница заражена, а также очень быстрое ухудшение поисковых позиций сайта.

Нередки случаи, когда распространением вирусов занимаются целые группировки мошенников. За примером идти далеко не нужно. Недавно была обнаружена крупномасштабная сеть (ботнет) под названием Kleber, которая объединяла более 75 000 зараженных компьютеров в двух с половиной тысячах учреждений и компаний из 196 стран мира. С помощью «троянской» программы «Zeus» мошенники отслеживали информацию частного характера, вводимую на зараженных компьютерах, в том числе — пароли к управлению сайтами. Стандартные антивирусы оказались бессильными, и какое-то



Агентство «Идеал» — одна из лидирующих компаний на рынке продвижения веб-сайтов в поисковых системах. Основано в 2002 году, офисы расположены в Москве и Киеве. В настоящее время киевский офис обслуживает более 420 клиентов.

[ideal.kiev.ua](http://ideal.kiev.ua)

время были заражены даже сети нескольких компаний из списка TOP-Fortune 500.

Выпытывать конфиденциальную информацию, для того чтобы навредить вашему сайту, могут и без помощи вирусов. Распространены такие приемы, как рассылка фиктивных писем от имени интернет-провайдеров и т. д. Повод может быть самый разный, например, необходимость восстановить данные после сбоя или DoS-атаки.

Как уберечься от этих подвохов?

1. Неплохо еще на стадии разработки сайта побеспокоиться, чтобы система управления к нему была лицензионной. Это в большой степени поможет защититься от вирусов и вовремя узнать, если они появятся.
2. Не храните пароли доступа к системе управления сайтом на жестком диске компьютера, а пароли доступа к FTP — в настройках FTP-клиента. Регулярно меняйте пароли доступа к админ-панели и FTP, минимизируйте доступ к паролям персонала и систематически делайте резервные копии (бэкапы, от англ. backup).
3. Поинтересуйтесь у вашего хостинг-провайдера, как часто он делает резервные копии и где их хранит, просите его время от времени давать вам копии и подстраховуйтесь, делая бэкапы сами. На часто обновляемых сайтах бэкапы можно делать раз в сутки, на редко обновляемых — после каждого обновления. Копии (последнюю и предпоследнюю) лучше всего хранить на сменном носителе (диск, флэшка) и на жестком диске компьютера, не входящего в общую сеть.
4. Компьютер, на котором администрируется сайт (как и вся локальная сеть, в которую он входит), может «подхватить» вирус в Интернете, а затем ваш сотрудник выложит зараженный файл на корпоративный сайт. Поэтому пользуйтесь качественными антивирусами и не забывайте их обновлять.
5. Перед добавлением на сайт какого-либо кода (новой функции, счетчика, кода рекламной сети и т. д.), изучите репутацию подрядчика, убедитесь, что другие компании успешно пользуются его услугами.
6. Не закачивайте нелицензионные программы, потому что высока вероятность подхватить «троян». Если речь идет о специализированных программах для работы с сайтом, то у мошенников большое искушение присоединить вирусы-шпионы.
7. Если сайт начал стремительно терять позиции в поисковых системах, нужно немедленно обращаться к специалистам.
8. Воспользуйтесь услугами Webmaster Tools от Google. Это поможет вам оперативно узнать о наличии зараженных страниц, если такие появятся, а избавившись от «заразы», сделать запрос Google на включение страниц в индекс обратно.
9. Регулярно проверяйте отображение сайта через поисковые системы. Если система выдаст предупреждение о том, что ваш сайт посещать опасно — значит, он заражен вирусом. Чаще всего излечить страницу антивирусом невозможно. Необходимо, чтобы специалист нашел в коде сайта ссылку на вирус и удалил его. Просканируйте компьютер или все компьютеры локальной сети антивирусом, а также смените пароли доступа к FTP для всех пользователей.
10. Обратите внимание на такой важный момент: сайт со временем становится все уязвимее. Это связано с особенностями функционирования кода, нередко — с вмешательством слишком самоуверенных администраторов. Поэтому хорошо подумайте перед тем, как самостоятельно менять что-либо в коде. А также периодически проводите аудит сайта, привлекая специализированные компании. Аудит — важное звено в обеспечении безопасности сайта. По результатам исследования компании Positive Technologies, опубликованном в конце 2009 года, из 10 459 проанализированных сайтов российских компаний различных секторов экономики 83% имели критичную уязвимость к заражению вирусами, взломам, краже информации, присоединению к хакерской сети, подбору паролей.

## Вооруженные нападения

Еще одна реальная опасность — это DDoS-атаки (от англ. Distributed Denial of Service, распределенная атака типа «отказ в обслуживании»). Суть состоит в том, что сайту-жертве одновременно дают запрос на получение информации множество компьютеров. Минимальные последствия — страницы сайта медленно загружаются, возрастают затраты на хостинг, максимальные — сервер не справляется, и сайт перестает работать. При постоянных атаках сайт начинает терять позиции в поисковых результатах, уменьшается количество клиентов, ухудшается их лояльность.

Часто атаки проводятся с ботнета, то есть сети зараженных компьютеров — их владельцы становятся невольными соучастниками. Управляющие же бот-сетью могут заниматься рэкетом, требуя с крупных компаний деньги за обещание не нападать. Единственный выход для владельца ресурса — это покупка специализированного аппаратного решения, оборудования по защите от DDoS и оплата услуг системного администратора или же пользование услугами специализированных организаций.

Если вы обслуживаетесь у хостинг-провайдера, то первым принимает DoS-атаку он. Как он поведет себя в такой ситуации? Попытается бороться или, как делается чаще всего, отключит сайт? Этот вопрос следует задать еще на этапе выбора провайдера. Если ваш сайт находится на собственном сервере, тогда вам нужно самостоятельно беспокоиться о полном комплексе оборудования для защиты, и экономия здесь может привести к плохим последствиям.

Реальную историю об атаке рассказывает (пожелав остаться неизвестным) владелец и основатель одного крупного специализированного сетевого СМИ. «В декабре 2009 года на наш ресурс была осуществлена DDoS-атака. Сайт вначале тормозил, потом перестал отвечать сервер и из-за загрузки оборудования хостинг-провайдер просто отключил ресурс. Никакие манипуляции провайдера и системных администраторов не помогли вернуть сайт в сеть, поэтому мы обратились в специализированную компанию.

На сегодня в Украине небольшой выбор «анти-доссеров», так как для этого необходимо дорогостоящее спецоборудование. Из компаний, специализирующихся на этих услугах, в Интернете можно найти только две: stop-dos.net и antiddos.org. Первая компания — аффилированная структура «Укртелекома», имеет более широкие возможности. На тот момент мы воспользовались ее услугами из-за масштабности атаки.

Пока ситуацию не вернули под контроль, наше СМИ было недоступно для пользователей 10 дней, временно произошли пессимизация сайта и снижение поискового трафика. Теперь наши ежемесячные расходы на защиту сайта составляют \$400. Атаки продолжаются, но тщетно».

Существует еще один вид агрессии против сайта — спам-атаки. Снова-таки множество компьютеров одновременно шлют запросы сайту через форму обратной связи, сервер не справляется — и сайт перестает работать. Защита от таких нападений несложная, хотя разработчики сайтов далеко не всегда советуют ее — это установка так называемых «капч» (требование ввести символы перед отправкой формы). Чем больше вариантов символов в защитном «арсенале» капчи, тем лучше. Желательно — больше сотни.

## Двойники

Чтобы создать дубликат сайта, злоумышленникам даже не нужно красть пароли. Вредительство с помощью «двойника» может быть самым разным. Например, на дубликаты сайта могут разместить о вас какую-нибудь нехорошую информацию. В случае с интернет-магазином могут изменить ассортимент по своему усмотрению. Или же принимать заказы ваших клиентов, получать с них деньги, а товар, конечно же, не поставлять. Противостоять этому можно, регулярно проверяя конкурентное окружение вашего сайта.

## Понижение сайта в поисковых результатах

Позиция коммерческого сайта в поисковых результатах Google и Yandex приобретает огромное значение для успешности биз-

неса. К сожалению, и здесь «умельцы» нашли способы вредить конкурентам.

Чтобы напакостить сайту, мошенники могут манипулировать его внешними ссылками. Поэтому нужно периодически отслеживать ссылочное окружение сайта, набрав в поисковой строке `links:www.адрес сайта`. Беспокоиться следует, если, например, вдруг появилось большое количество сомнительных ссылок на ваш сайт, и вы не совсем понимаете, откуда они взялись. Это уже повод обратиться к специалисту.

Стоит побеспокоиться, если вдруг очень резко и необъяснимо возросла посещаемость на счетчике сайта (например, на Бигмире или на любом другом). Вполне возможно, вам искусственно «накручивают» счетчик, и поисковые системы уже готовятся применить санкции в отношении вашего сайта.

Контент у нас в стране крадут сплошь и рядом. Умельцы могут украсть ваш контент (например, новости или посты) таким образом, что оригинал текста на вашем сайте поисковые системы сочтут плагиатом.

Еще одна угроза для поискового рейтинга сайта — дорвеи (от англ. doorway — входная дверь, портал). Это прикрепленные к основному сайту веб-странички, напечатанные ключевыми словами. На 1-2 дня они повышают авторитетность основного сайта, а затем оба попадают под фильтры поисковых систем. Иногда дорвеи можно определить «на глаз», но в основном они незаметны. О «дорвейном» нападении на ваш сайт вы можете догадаться, обнаружив резкое, ничем не объяснимое повышение посещаемости.

Ну и, конечно, нужно помнить, что не меньшей, а часто даже большей беды можно натворить, оптимизируя и продвигая сайт самостоятельно.

#### **Советы:**

1. Регулярно отслеживайте позиции вашего сайта в поисковых системах, динамику смены позиций, а также ссылочное окружение сайта.
2. Не занимайтесь оптимизацией сайта, если не уверены, что прекрасно владеете seo-навыками. Безопаснее обратиться в специализированную компанию, которая занимается продвижением сайтов в поисковых системах.

3. Обнаружив резкое понижение позиции сайта в поисковых системах или целенаправленное вредительство, немедленно обращайтесь к специалистам.

4. Чтобы предотвратить кражу контента, ставьте всевозможные копирайты на страницах, кого-то это отпугнет. Если вы часто и регулярно (например, каждый день) добавляете посты или блоги и у вас есть подозрение на кражу контента, размещайте эти тексты в разное время. Поисковые роботы заходят на вашу страницу с определенным интервалом, и часто достаточно от 15 мин. до 1-2 часов, чтобы новая информация была проиндексирована и признана вашей. Именно за этот промежуток времени и стараются украсть текст. Сбив с толку воров, можно решить проблему.

## **Присвоение доменов**

Лишиться права собственности на домен сайта намного проще, чем кажется на первый взгляд. Достаточно забыть продлить срок аренды доменного имени. Нередки случаи, когда злоумышленники узнавали дату окончания срока и, если компания забывала об этом вопросе на несколько часов, домен тут же перекупали у регистратора. Причем с точки зрения закона правонарушения в этом, конечно же, нет. Затем новые владельцы домена или начинают шантажировать, требуя выкуп, или размещают на домене свой сайт. Как известно, за доменом остается Page rank и тематический индекс цитирования (ТИЦ), то есть авторитетность в поисковых системах. Если сайт, у которого украли имя, имел прекрасные позиции в поисковиках, этим могут воспользоваться.

#### **Советы:**

1. По возможности продлите срок аренды сайта на несколько лет вперед. К данным о сотруднике, который регистрировал доменное имя, нужно относиться очень ответственно. Чтобы не вышло так, что сотрудник уволен, а затем не известно, когда заканчивается срок аренды домена, потому что вся корреспонденция с хостинг-провайдером приходит на его личный адрес.

2. Если вы решили купить домен с высоким Page rank и ТИЦ на вторичном рынке, будьте осторожны. С одной стороны, сайт, размещенный на таком домене, намного проще продвигать в поисковых системах. С другой стороны, вторичный рынок — теневой, со всеми вытекающими отсюда рисками.

### **Защитит ли закон?**

Если вашему сайту навредили, логично обратиться в суд, но реально ли защитить свои интересы? Законодательство мало защищает владельцев веб-ресурсов, потому что поймать за руку злоумышленника сложно. С другой стороны, дает о себе знать низкая правовая культура в нашей стране. «Несмотря на наличие соответствующих статей в криминальном кодексе, прецедентов обвинения интернет-мошенников пока еще очень мало», — сообщает Евгений Шевченко, генеральный директор интернет-агентства UaMaster. Намного лучше обстоит ситуация с возвращением через суд украденных или незаконно присвоенных доменов, поскольку в этом случае споры решают международные учреждения.

### **Кто ответственный?**

В процессе разработки и функционирования сайта задействовано несколько сторон: разработчики, регистраторы доменных имен, хостинг-провайдеры, сео-студии, администратор сайта и т. д. Возникает вопрос: кто, в какой мере и за какие сферы безопасности сайта ответственный?

Начнем с разработчиков. К сожалению, большинство будет стараться не затрагивать тему безопасности сайта. Это легко объяснить: где и как студии приобретают CMS, кто и как разрабатывал «движок» — тайна, покрытая мраком. Желательно получить правдивую информацию по этим вопросам. «Культура программирования в Украине оставляет желать лучшего. В какой-то мере виноваты сами заказчики. Исходя из реалий нашей страны, они больше внимания уделяют, например, вопросам налогообложения, чем безопасности IT-продукта, — утверждает Дмитрий Днепровский, директор департамента информационной безопасности ЗАО «Софтлайн».

В большой мере ответственность за безопасность сайта лежит на хостинг-провайдере. Еще на этапе его выбора стоит узнать (и постараться прописать это в договоре), как он поведет себя в случае DoS-атак на ваш сайт, какие общие меры безопасности принимает в «мирное время». Возможно, общение с провайдером стоит поручить специалисту, который сможет расспросить о периодичности обновления операционных систем, проверки логов, веб-сервера и сервера баз данных. Если вам устанавливают (будем надеяться) лицензионную CMS, зайдите на сайт ее разработчиков и посмотрите списки рекомендуемых хостинг-провайдеров, это поможет сделать выбор.

И все же, основная ответственность за безопасность сайта лежит, конечно же, на самой компании. Никто не побеспокоится о вашем сайте, кроме вас.