Аспекты применения средств информационной безопасности хостинг-провайдерами России

COMNEWS RESEARCH

МАЙ 2017

АСПЕКТЫ ПРИМЕНЕНИЯ СРЕДСТВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ХОСТИНГ-ПРОВАЙДЕРАМИ РОССИИ

Отчет по итогам инициативного исследования

СОДЕРЖАНИЕ

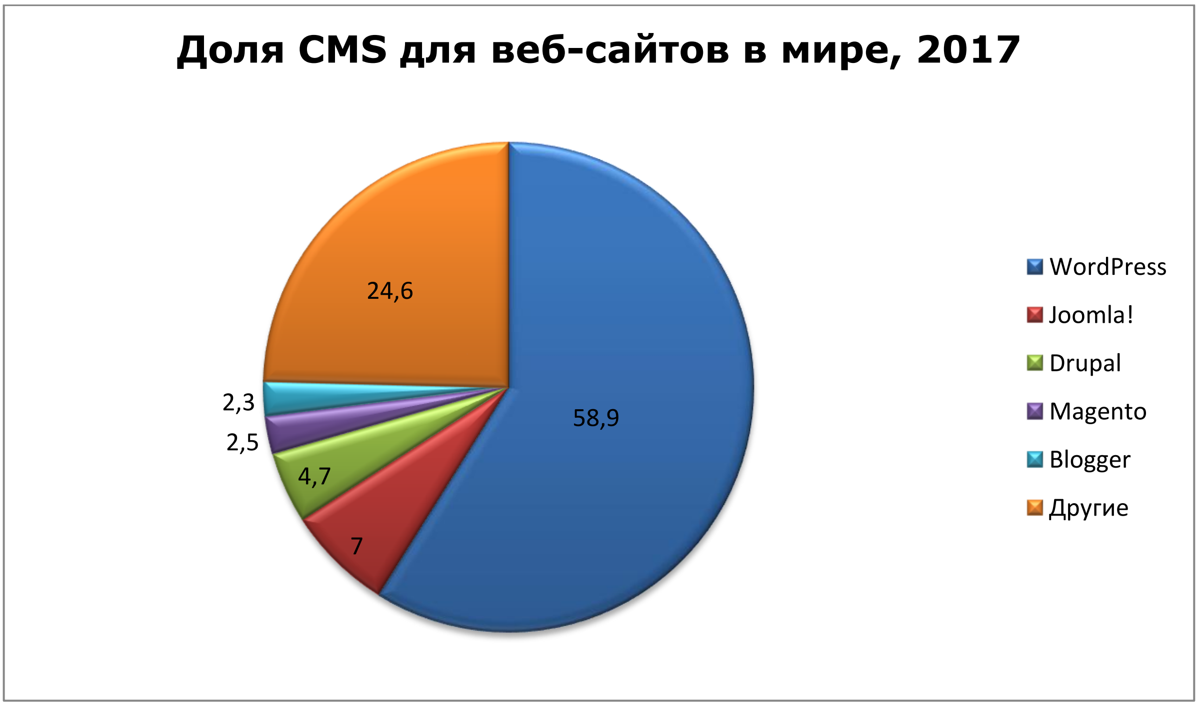
АСПЕКТЫ ПРИМЕНЕНИЯ СРЕДСТВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ХОСТИНГ-ПРОВАЙДЕРАМИ РОССИИ

Отчет по итогам инициативного исследования

1. ВВЕДЕНИЕ. ОБЗОР ТЕКУЩЕЙ СИТУАЦИИ НА РЫНКЕ

По данным статистического ресурса Internet Live Stats, в Интернете, в начале 2017 года, насчитывалось более миллиарда веб-сайтов. Их количество, в том числе в России, продолжает неуклонно расти, во многом благодаря реализации программы по устранению «цифрового неравенства», в результате которой всё больше людей получают широкополосный доступ к сети Интернет, тем самым создавая новое количество интернет ресурсов – от блогов до функционально сложных проектов и интернет-магазинов. Этому росту способствует также взрыв технологий, в числе которых системы управления содержимым веб-сайта или контентом с открытым исходным кодом (CMS - Content Management System). Около 75% интернет-ресурсов в мире создаются и работают на четырех ключевых платформах: WordPress, Joomla!, Drupal, Magento и Blogger. WordPress лидирует на рынке CMS с долей около 60%.

Диаграмма 1.1. **Доля CMS для веб-сайтов на мировом рынке, май 2017 г.**



Источник: W3techs

Такая популярность и юзабилити WordPress (по сравнению с другими CMS) обусловлена простыми и понятными для владельца веб-сайта свойствами: доступный функционал, простота администрирования, высоко расширяемая платформа, ориентация на конечного пользователя.

Другие CMS получили распространение в более нишевых сегментах рынках. Magento, например, сделала ставку на развитие в области e-commerce, этой системой пользуется каждая четвертая компания, продающая он-лайн свои услуги или товары. В то время, как Drupal, из-за гибкости и многозадачности часто называют не CMS, а CMF (Content

Management Framework) или каркасом для систем управления контентом и веб-приложений. Это определяет универсальность платформы. На базе Drupal можно реализовать любой проект: от корпоративного веб-сайта до портала органов государственной власти.

Россия также поддерживает тренд лидерства WordPress (с учётом версий WordPress 4.4, 4.5, 4.6, 4.7) с долей на рынке 40,71%. При этом, несмотря на достаточно широкий выбор иностранных CMS, российские владельцы веб-сайтов (с доменным именем .ru) активно используют отечественные разработки такие как: 1C-Bitrix, Data Life Engine, которые в совокупности занимают почти 16% на местном рынке, что превышает долю такого гиганта как Joomla! (13,03%).

Диаграмма 1.2. **Доля CMS для веб-сайтов на российском рынке, май 2017г.**

Источник: BuiltWith

Массовое развитие веб-сайтов создает новые угрозы на просторах Интернета, немалая часть которых напрямую связана с компетенциями веб-мастеров и поставщиков услуг, ответственных за разработку и администрирование веб-сайтов.

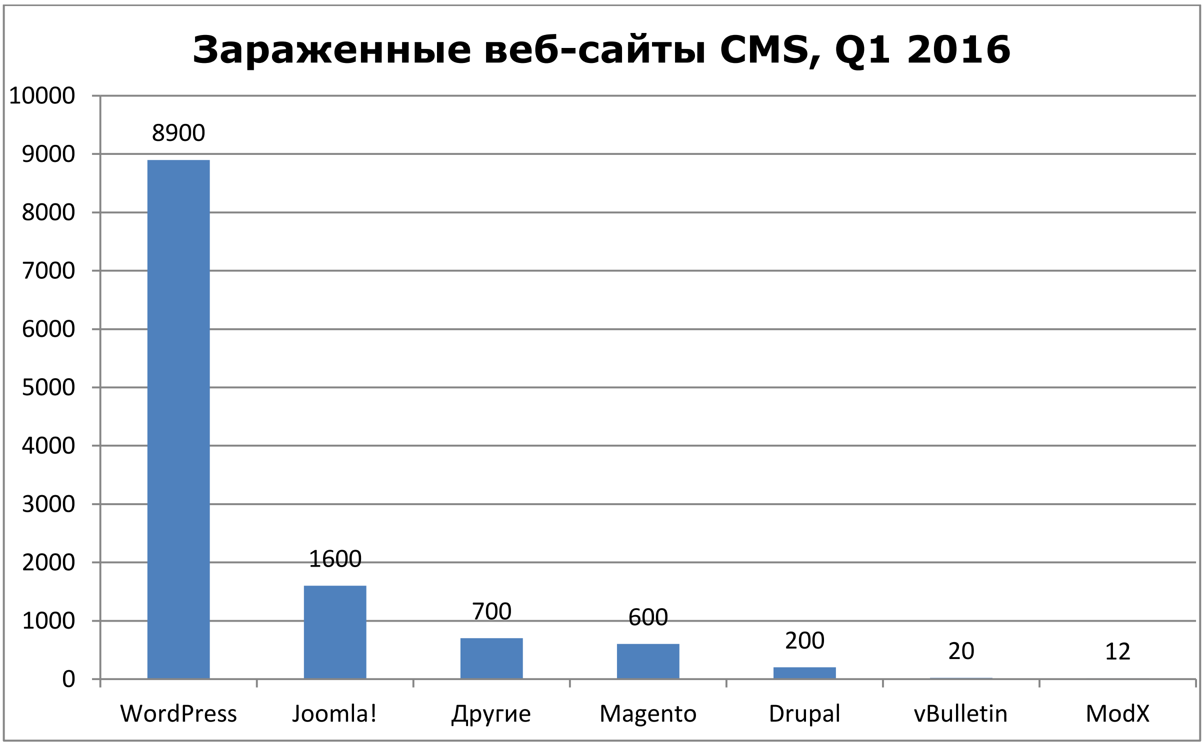
По данным Google более 50 миллионов владельцев веб-сайтов в марте 2016 года получили предупреждения о том, что с их портала пытались украсть информацию или установить вредоносное программное обеспечение (ПО). В марте 2015 года таких инцидентов было лишь 17 миллионов. За год количество взломанных сайтов возросло на 34%. Каждую неделю черные списки Google пополняются 20 000 веб-сайтами с вредоносным ПО, кроме того, регистрируется не менее 50 000 веб-сайтов, которые еженедельно генерируют фишинг-атаки.

АСПЕКТЫ ПРИМЕНЕНИЯ СРЕДСТВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ХОСТИНГ-ПРОВАЙДЕРАМИ РОССИИ

Отчет по итогам инициативного исследования

По данным Securi[1] из 11 000 веб-сайтов, зараженных вредоносным ПО, 75% созданы на платформе WordPress, при этом, свыше чем на 50% веб-сайтов работали на базе устаревшего ПО. Веб-сайты, работающие на базе платформ Joomla! и Drupal имеют еще бОльший процент устаревшего ПО, по информации Securi цифра достигает 80%. В числе наиболее поражаемых CMS-платформ аналитики называют WordPress, Joomla!, Magento. При этом наибольшее количество случаев инфицирования аналитики связывают с неправильной разработкой, настройкой и обслуживанием веб-сайта веб-мастерами, администраторами и защитой со стороны хостинг-провайдера, а не с уязвимостью ядра CMS-платформы.

Диаграмма 1.3. **Распределение CMS по количеству зараженных веб-сайтов**



Источник: Securi

В числе возможных причин активных вирусных атак на веб-сайты, построенные на этих CMS-платформах, называют:

- уязвимый код;
- слабую программную реализацию;
- популярность.

Во всех случаях, независимо от платформы, главная причина заражения связана, как правило, с эксплуатацией уязвимостей программного обеспечения в расширяемых

[1] Securi «Website Hacked Trend Report», 2016, H1.

компонентах платформы, а не в ее ядре. Расширяемые компоненты напрямую связаны с интеграцией плагинов, расширений, компонентов, модулей, шаблонов, тем и других подобных факторов.

Часто владельцы веб-сайтов полагают, что если с их веб-сайта нет возможности украсть информацию, касающуюся, например, номеров кредитных карт, то веб-сайт априори не будет взломан, так как не представляет живого интереса для хакеров. Тем не менее, это не так. Взломанный веб-сайт может содержать сразу несколько файлов, модифицированных различными семействами вредоносных программ (связь «many-to-many»). Все зависит от намерения или цели злоумышленников, каким образом в дальнейшем использовать свой новый актив (актив - это термин, используемый для описания веб-сайта, который заполучили хакеры и который является частью их сети). Рассмотрим, как хакеры используют взломанные веб-сайты на площадке WordPress.

Таблица 1.1. **Типы использования взломанных веб-сайтов хакерами на площадке WordPress**

Тип применения	%
Дефейс веб-сайта	26
Рассылка спама	19
SEO спам	17
Злонамеренный редирект	14,8
Другие	12,65
Фишинговые страницы	4
Распространение Malware	2,5
Похищение пользовательской информации	1,25
Атаки на другие веб-сайты	1
Ransomware	0,9
Размещение вредоносного контента	0,5
Referrer спам	0,4

Источник: Worldfence

Описание типов использования взломанных веб-сайтов хакерами на площадке WordPress:

Дефейс сайта	• страница веб-сайта заменяется другой страницей, чаще всего содержащей рекламу, угрозы или вызывающие предупреждения
Рассылка спама	• массовая рассылка нежелательных информационных сообщений
SEO спам	• внедрение ключевых слов и ссылок на веб-сайт, для продвижения ранжирование сайта
Злонамеренный редирект	• перенаправление траффика веб-сайта на вредоносные ресурсы
Фишинговые страницы	• копирование интерфейса интернет-ресурса для кражи пользовательских аккаунтов
Распространение Malware	• установка вредоносного ПО на веб-сайт и компьютеры посетителей веб-сайта
Похищение пользовательской информации	• похищение информации о пользователях, кредитных картах
Атаки на другие сайты	• использование сервера взломанного веб-сайта для атак на другие ресурсы
Ransomware	• блокировка веб-сайта с последующим требованием выкупа за восстановление доступа
Размещение вредоносного контента	• использование сервера взломанного веб-сайта для размещения вредоносного контента и файлов (фактически используется учётная запись хостинга в качестве файлового сервера)
Referrer спам	• настройка трафика таким образом, чтобы он выглядел как фальшивий трафик, тем самым меняя истинную картину статистики сайта

Как видно из Таблицы 1.1 на ресурсах, созданных на WordPress, основным видом атак является дефейс веб-сайта – направлен на то, чтобы каждый посетитель веб-сайта узнал, что этот веб-ресурс взломан. Фактически эта деятельность направлена на урон репутации и уменьшение клиентской базы веб-ресурса.

Можно выделить основные последствия взлома веб-сайта:

- снижение позиций в поисковой выдаче и уход лояльных посетителей;
- фатальные повреждения программного кода;
- кража личных данных и паролей клиентов веб-сайта;
- индексация внешних (чужих) страниц;
- необратимое уничтожение данных.

Примечательно, что большинство веб-сайтов на платформе WordPress не хранят конфиденциальные данные, кроме учетных записей пользователей конкретного веб-сайта и, возможно, адресов электронной почты. В этой связи ситуация усугубляется тем, что владельцу взломанного веб-сайта будет сложно обнаружить кражу данных, если это произошло.

Несмотря на то, что в таблице 1.1 Ransomware (от англ. ransom — выкуп) - взлом веб-сайта с последующим вымогательством выкупа за восстановление доступа, занимает низкие позиции для платформы WordPress, в 2016 году, по данным Malwarebytes, в глобальном измерении количество атак такого вида хакерства возросло на беспрецедентные 267%. Хакеры, с небольшими навыками кодирования или вообще без них, могут купить комплекты «под ключ», известные под названием «Ransomware as a Service» (RaasS), которые берут на себя все хлопоты по интернет преступлениям.

В мае 2017 года случилась самая крупная за всю историю эпидемия вируса-вымогателя WannaCry (WCry или WanaCryptor 2.0). Данная атака была хорошо спланирована киберпреступниками и осуществлена на крупные телекоммуникационные и транспортные компании, правительственные и правоохранительные органы, больницы и образовательные учреждения. Эпидемия программы-вымогателя WannaCry затронула более 150 стран, были выведены из строя сотни тысяч компьютеров. Наибольший удар пришелся на Россию. Компьютеры под управлением Windows в разных уголках планеты оказались заблокированы вирусом, который требовал за разблокировку примерно $300 криптовалютой. Простая переустановка операционной системы не имела смысла — вирус не просто лишал пользователя возможности управления компьютером, но также шифровал на нём данные, чтобы пользователь не смог получить к ним доступ без специального ключа[2]. Несмотря на то, что идти на уступки преступников считается плохой практикой, пользователи всё же перечисляли биткоины. Но, в результате, не зафиксировано ни одного случая, чтобы злоумышленники вернули данные. Жертвами стали пользователи Windows. Но если у пользователя Windows Vista, Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2012 или Windows Server 2016 и, что самое важное, ОС настроена на автоматические обновления (Windows выпускал ранее патчи-релизы для этих уязвимостей), то компьютер был вне опасности. После того, как атаку удалось остановить, вопросы информационной безопасности вновь вышли на новый уровень. Теперь ими задались и владельцы веб-сайтов, понимая, что взлом - это реальная угроза, которой подвергается каждый.

[2] Блог компании Acronis, Inc. https://habrahabr.ru/company/acronis/blog/328796/.

АСПЕКТЫ ПРИМЕНЕНИЯ СРЕДСТВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ХОСТИНГ-ПРОВАЙДЕРАМИ РОССИИ

Отчет по итогам инициативного исследования

По данным компании Securi, у 66% скомпрометировавших себя веб-сайтов в мире обнаружен PHP – бэкдор (от англ. back door — «чёрный ход»), скрытый внутри веб-сайта. Бэкдоры позволяют злоумышленникам обойти любые существующие средства управления доступом к среде веб-сервера. Эффективность бэкдоров обусловлена их иллюзорностью для большинства технологий сканирования веб-сайтов. Сами бэкдоры часто хорошо написаны, не всегда используют обфускацию («запутывание» кода) и не представляют никаких внешних признаков компрометации для посетителей веб-сайта.

По данным Google, только 6% веб-мастеров веб-сайтов обнаруживают заражение посредством активного мониторинга подозрительной активности. Напротив, 49% веб-мастеров узнают о заражении, когда получают предупреждение браузера при попытке просмотреть свой собственный веб-сайт; еще 35% - через другие сторонние каналы отчетности, такие как, информация со стороны хостинг-провайдера или уведомление от коллеги или друга, получившего предупреждение браузера. В большинстве случаев возникает одна и та же проблема - веб-мастера редко получают поддержку от своих хостинг-провайдеров. Аналогичным образом, исследование StopBadware и CommTouch показало, что 46% операторов веб-сайтов сами проводят процедуру чистки веб-сайта, а 20% обращаются за профессиональной помощью. Только у 34% веб-мастеров есть бесплатная поддержка со стороны своего хостинг-провайдера. Эти два исследования дают качественные доказательства тех сложностей, с которыми в настоящее время сталкиваются веб-мастера, и потенциальной ценности уведомлений об угрозах со стороны третьих сторон.

По мнению аналитиков, хостинг-провайдеры, предоставляя свою площадку для размещения интернет-проекта, крайне редко озабочиваются вопросами, связанными с информационной защитой клиентов. Хостинг не может нести ответственность за взлом веб-сайта, так как не является исполнителем по изготовлению и сопровождению веб-сайта (именно через уязвимости в коде веб-сайта, несвоевременном обновлении платформы веб-сайта, чаще всего взламываются интернет-проекты). Ответственность за взлом находится на стороне веб-разработчика или сотрудника компании - владельца веб-сайта. Тем временем, со стороны хостинг-провайдера может быть гарантия защиты веб-сайта от известных видов взлома и атак. Кроме того, хостинг-провайдер может взять на себя и такие задачи, как лечение веб-сайта после взлома, устранение уязвимости, обновление платформы веб-сайта.

Аналитики ComNews Research изучили бизнес-модели хостинг-провайдеров России, чтобы определить, кто из них обеспечивает защиту веб-проектов от взлома в качестве гарантированного сервиса, проанализировав юридические обязательства перед клиентами, а также статистику других мер информационной защиты.

2. МЕТОДОЛОГИЯ

Исходное количество хостинг-провайдеров для выборки исследования составило 250 участников. Учитывая тот факт, что часть запросов осталась без ответов (команда ComNews Research столкнулись с тем, что указанные контактные телефоны не работали; не отвечала техническая поддержка, что наглядно показывает уровень качества работы хостинга), а абоненты некоторых хостинг-провайдеров обслуживаются централизованно другим хостингом, фигурант находится на стадии закрытия или слияния с другим участником рынка, в итоговом аналитическом сравнении принял участие 201 хостинг-провайдер[3]. См. Приложения 1, 2, 3.

На первом этапе сбора информации были проведены анкетирование и опросы участников данного исследования (отправка запросов и телефонное интервьюирование). Второй этап состоял из агрегации и структурирования данных. В рамках второго этапа состоялся отбор претендентов на включение в перечень «безопасных хостингов». На третьем этапе методом верификации данных определен пул хостингов, обеспечивающих защиту веб-сайтов от взломов и определены сроки начала оказания услуг. В итоговый перечень «безопасных хостингов» включены компании, которые:

- имеют юридическое лицо в России;
- оказывают защиту веб-сайта в автоматическом режиме (защита включена в базовую услугу shared-хостинга) для всех платформ веб-сайтов.

Для проверки полученных данных исследовательская команда ComNews Research, использует методы кросс-верификации и экспертной оценки. Данные, полученные в ходе интервью или письменного опроса, проверяются на совпадение и/или комплиментарность с данными из альтернативных источников, как формальных, так и неформальных. Кроме того использовались данные полученные из открытых источников (например: официальные договоры-оферты, статистические данные).

[3] В исследовании компания Reg.ru также включает в себя 6 обслуживаемых ей хостинг-провайдеров: Host-telekom.ru, Leaderhost.ru, Mobyhost.ru, Omegahost.ru, Agava.ru, 50web.ru.

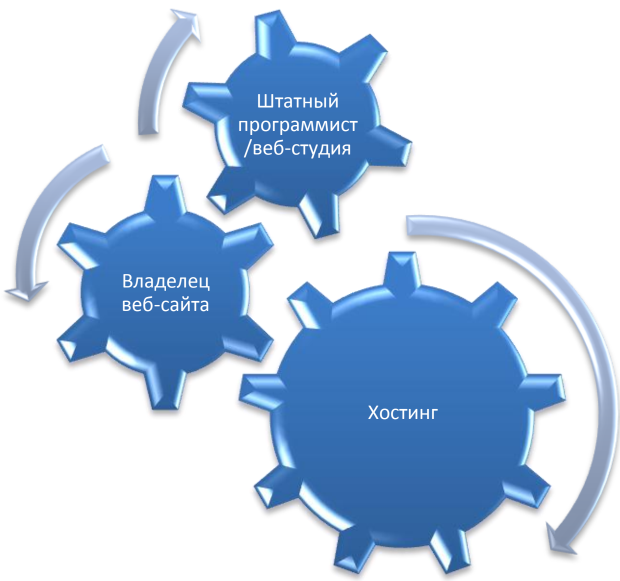
3. Хостинг-провайдеры в России, обеспечивающие информационную защиту веб-сайтов от взлома

Задача хостинг-провайдера – предоставление площадки для размещения интернет-проекта клиента. Услуги хостинга включают в себя: услуги виртуального хостинга, выделенного сервера размещение и хранение информационного ресурса клиента, предоставление клиенту дискового пространства.

Типовая схема взаимодействия «владелец веб-сайта» – «хостинг» представлена на Рисунке 3.1.

1. Владелец веб-сайта - Заказчик.
2. Штатный программист или веб-студия на аутсорсинге, задачами которых являются обслуживание, обновление, нахождение и устранение уязвимостей в коде веб-сайта, грамотная разработка и развертывание веб-сайта.
3. Хостинг-провайдер, предоставляющий технологическую площадку для размещения веб-сайта.

Рисунок 3.1. **Схема взаимодействия «владелец веб-сайта» - «хостинг»**



Источник: ComNews Research

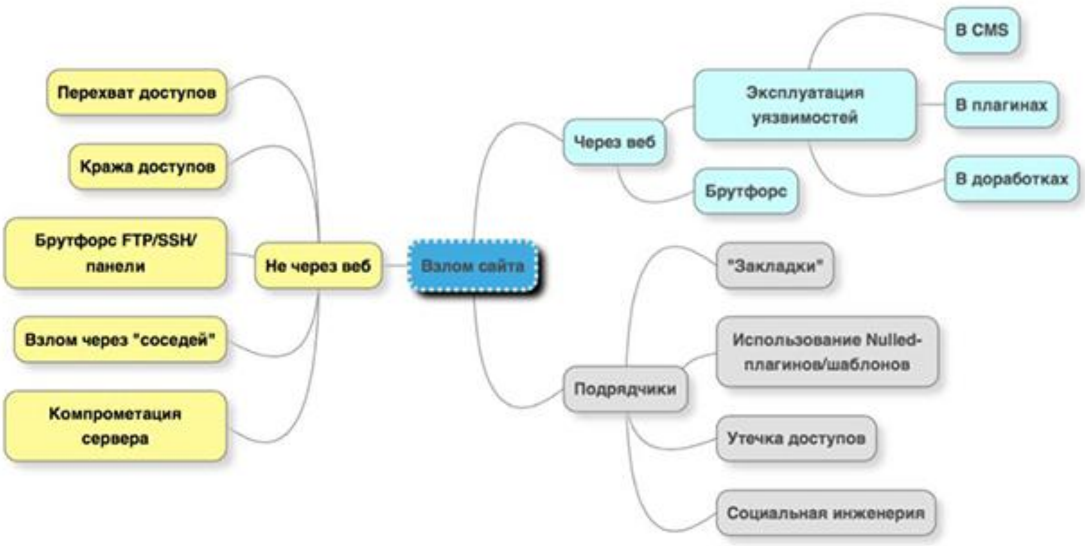
Штатный программист обязан регулярно обновлять платформу веб-сайта, устанавливать последние версии CMS-платформы с целью предотвращения взлома интернет-площадки. Но, как показывает практика, взламывают не только устаревшие версии CMS но, и наоборот — «обновленные» CMS. Хостинг, зафиксировав подозрительную активность со стороны веб-сайта (например: рассылку спама), просто блокирует веб-сайт, постфактум отправляя клиенту отчет о взломе. После чего, владелец веб-сайта может начинать подсчитывать убытки, связанные с дискредитацией веб-сайта. Программист же, может самостоятельно вычищать веб-сайт от вредоносного кода, менять пароли, или обратиться к своему хостингу (если услуга лечения оказывается хостингом) или сторонней специализированной организации.

На российском рынке можно выделить следующие компании (де-факто аутсорсинговые компании с точки зрения владельцев веб-сайтов и хостингов), специализирующиеся на защите веб-сайтов от взлома: Revisium, Pentestit и др. Эти компании предоставляют комплексную защиту от взлома веб-сайта. Компания Revisium запустила бесплатную программу «AI-Bolit - сканер», которая проверяет веб-сайт на взлом, вирусы и хакерские скрипты. Эта программа стала достаточно популярной на рынке, благодаря простоте и клиенто-ориентированности. Хостинги интегрируют AI-Bolit в панель управления, а веб-разработчики используют его для поиска вредоносного кода и в собственных сервисах мониторинга веб-сайтов.

Можно выделить следующие возможные варианты взлома[4]:

- взлом в результате веб-атак;
- взлом веб-сайта не через веб, но без участия человека;
- взлом по вине сотрудников и подрядчиков.

Рисунок 3.2. **Варианты взлома веб-сайтов**



Источник: Cossa, Revisium

[4] Григорий Земсков «Как взламывают сайты (через уязвимости, по вине сотрудников или подрядчиков) и как от этого уберечься» http://www.cossa.ru/234/134334/.

- Взлом в результате веб-атак. На него приходится более 80% от всех возможных вариантов несанкционированных вторжений. В этой связи веб-мастера и владельцы веб-сайтов обращают внимание на закрытие уязвимостей и обновление плагинов и CMS до актуальной версии;
- Взлом веб-сайта не через веб. Взлом веб-сайта не через веб-уязвимости представлен довольно большим классом технических «возможностей» для злоумышленников:
  - ✓ Перехват или кража доступов. Зараженный вирусом-трояном компьютер, с которого удалённо работают сотрудники компании, или небезопасное подключение к wi-fi фрилансера, который решил внести правки на веб-сайт, находясь в коворкинге, могут стать причиной кражи доступов от веб-сайта и хостинга.
  - ✓ Работа по wi-fi в общественных местах — отдельная возможность для взлома. Пользователь не знает, кто сидит за соседним столом и не «снифферит» (перехватывает) ли кто-то этот трафик, чтобы воспользоваться собранной информацией в недобропорядочных целях. Часто заражают wi-fi роутеры, в результате чего весь незащищенный трафик, идущий через них, оказывается перехваченным (пароли, конфиденциальная информация и пр.).
  - ✓ Брутфорс атаки (подбор пароля от FTP/SSH/панели хостинга). Многие владельцы веб-сайтов и веб-администраторы не задумываются о надёжности своих паролей — ставят для удобства простые и короткие комбинации, которые весьма легко «угадываются» роботами подбором по заранее заготовленному словарю. На первый взгляд, ситуация выглядит довольно надуманной, но многие до сих пор используют в качестве пароля от администраторского аккаунта банальное «12345» или admin/admin.
  - ✓ Взлом веб-сайта через «соседей» по аккаунту хостинга. На практике редко встречается ситуация, когда веб-сайты размещают изолированно друг от друга, по одному на аккаунте. Обычно рядом с веб-проектом соседствует один или несколько веб-сайтов, иногда это тестовая площадка основного веб-сайта, развернутая на техническом домене. Веб-сайты, которым не уделяется должное внимание в плане защиты или забытые или ненужные веб-проекты, могут стать причиной взлома всего аккаунта, в том числе и защищенного веб-сайта.
  - ✓ Компрометация сервера хостинга. Если хостинг не обладает нужными компетенциями, не имеет должного опыта для грамотного и безопасного администрирования, сервер смогут взломать через уязвимые компоненты или небезопасные настройки.
- Взлом веб-сайта по вине подрядчиков или сотрудников.

Для выполнения операций с веб-сайтом владелец предоставляет все ключи своему веб-программисту или студии. В данном случае существует риск кражи паролей и доступов или заражения компьютера, в результате чего, веб-сайт начинает генерировать подозрительный трафик, появляются переходы на сторонние веб-сайты. Даже бдительный и осторожный пользователь может стать жертвой случайного инцидента. Но факт остается фактом: работающий веб-ресурс взломали.

Существует устойчивое заблуждение владельцев веб-сайтов, что после того, как веб-сайт вылечат, веб-проекту больше ничего не угрожает. Веб-сайт, который был взломан однажды, скорее всего, будет взломан повторно, если не предпринимать превентивные меры защиты от взлома. Причем, одна защита оборудования здесь абсолютно бесполезна, так как более 80% современных атак используют уязвимости приложений, а не уязвимости сетевой архитектуры. Необходим комплекс мер на Транспортном и Сетевом уровнях – Layer 4 и Layer 3 (защищенные серверы и иное передающее оборудование) и на уровне Приложения (Layer 7 – WAF - Web Application Firewall) модели OSI.

Для защиты веб-сайта от взлома через веб, одним из ключевых инструментов, который используют, является WAF - защитный экран для приложений, осуществляющих передачу данных через HTTP и HTTPS. WAF может отслеживать http-трафик в реальном времени, работая, как система обнаружения вторжения и позволяя отреагировать на подозрительные события, которые имеют место быть в веб-системах. Также WAF может среагировать на угрозу сразу, чтобы предотвратить атаку еще до того, как она достигнет цели. На серверах фильтруется большинство атак, направленных на уязвимость популярных CMS, включая Joomla!, WordPress и др. Решение позволяет осуществлять мониторинг http-трафика и выполнять анализ событий в режиме реального времени. Используемые на уровне http-сервера фильтры справляются с многочисленными угрозами, такими как: межсайтовый скриптинг, SQL инъекции, подстановка JavaScript-блоков на страницы и др. Функции отличающие WAF от защитных систем предыдущих поколений рассмотрены в таблице 3.1.[5].

Таблица 3.1. **Отличия между WAF, IPS, NGFW/UTM**

Функции	**WAF (Web Application Firewall)**	**IPS (Intrusion Prevention system)**	**NGFW/UTM (Next Generation Firewall/Unified threat management)**
Multiprotocol Security	–	+	+
IP Reputation	+ –	+ –	+ –
Сигнатуры атак	+	+ –	+ –
Автоматическое обучение, поведенческий анализ	+	–	–
Защита пользователей	+	–	–
Сканер уязвимостей			
Виртуальный патчинг	+	–	–
Корреляции, цепочки атак	+	–	–

Источник: Positive Technologies

[5] Блог компании Positive Technologies https://habrahabr.ru/company/pt/blog/269165/.

По мнению аналитиков можно выделить следующие ключевые меры по защите веб-приложения от взлома:

- Отслеживание системных логов и использование бесплатных и коммерческих баз для блокировки не только попыток взлома по сигнатурам, но и баз адресов злоумышленников.
- Сигнатуры атак. Сигнатурный подход к обнаружению атак применяется повсюду, но только грамотный препроцессинг трафика, доступный для WAF, может обеспечить корректное применение сигнатур. Недостатки препроцессинга приводят к избыточной сложности сигнатур атак: администраторы не могут разобраться в сложнейших регулярных выражениях, весь смысл которых в том, что их авторы, например, всего лишь пытались учитывать возможность передачи параметра, как открытым текстом, так и в форме шестнадцатеричного кода.
- Технология IP-Reputation - опирается на внешние чёрные и белые списки ресурсов, и одинаково доступна любым периметровым средствам защиты.
- Блокировка Tor-сетей: Tor-сетями часто пользуются злоумышленники для взлома веб-сайтов. Сети Tor позволяют осуществлять действия в сети анонимно. Так как Tor является открытой системой, все адреса публичных узлов Tor известны, благодаря чему, их легко включить в «чёрный список» с последующей блокировкой.
- система Virtual Patching - защищает приложения веб-сайта от неисправленных уязвимостей, обнаруживая и блокируя попытки атак и вторжений в режиме on-line, что позволяет не приостанавливать работу веб-сайта. Даже известные уязвимости невозможно устранить сразу: исправление кода требует средств и времени, а зачастую и остановки важных бизнес-процессов; иногда в случае использования стороннего ПО исправление невозможно вообще. Для парирования таких «частных» угроз в системах IDS/IPS, а по наследству в UTM/NGFW, применяются пользовательские сигнатуры. Но проблема в том, что написание такой сигнатуры требует от пользователя глубокого понимания механизма атаки. В противном случае пользовательская сигнатура может не только «пропустить» угрозу, но и породить большое количество ложных срабатываний. В наиболее современных WAF используется автоматизированный подход к виртуальному патчингу. Для этого используется анализатор исходных кодов приложения (SAST, IAST), который не просто показывает в отчёте строки уязвимого кода, но тут же генерирует эксплойт, то есть вызов с конкретными значениями для эксплуатации обнаруженной уязвимости. Эти эксплойты передаются в WAF для автоматического создания виртуальных патчей, которые обеспечивают немедленное закрытие уязвимости ещё до исправления кода.
- Защита на стороне ОС сервера. Анализ системных логов, логов secure на наличии попыток авторизации ftp, http, mysql, ssh и блокировка брутфорс атак.
- Технология «Заморозка веб-сайтов» (цементирование) обеспечивает защиту веб-сайта от внедрения вредоносного кода. Технология работает за счет добавления/изменения расширенных атрибутов файла. Следует учитывать, что действие подобных атрибутов перекрывает полномочия пользователя,

направленные на модификацию или удаление файлов. Иными словами, даже администратор ОС сервера не может изменить замороженные файлы пока расширенные атрибуты не сняты, а злоумышленник не сможет модифицировать файлы, загружать вредоносный код, поскольку все служебные директории и файлы становятся доступны «только для чтения». Как результат:

- ✓ злоумышленник не может загрузить вредоносный код на веб-сайт, поскольку большинство директорий только для чтения;
- ✓ если хакеру удается загрузить шелл-скрипт во временный каталог или каталог загрузки файлов, то он не может воспользоваться загруженным скриптом, поскольку в этих директориях запрещено выполнение .PHP скриптов;

- Сканирование файлов веб-сайта на хостинге на наличие вирусов, веб-шеллов, бэкдоров, спам-рассыльщиков, фишинговых страниц, дорвей-страниц и других вредоносных и хакерских скриптов.
- технологии Cloudlinux OS. Основное назначение CloudLinux - изолирование процессов пользователей друг от друга и ограничение использования ресурсов каждым отдельным пользователем. Благодаря этому веб-сайты лучше защищены от соседских нагруженных проектов и соседей-злоумышленников. Можно сказать, что CloudLinux обеспечивает виртуализацию на уровне пользователей:

✓ Lightweight Virtualized Enviroment (LVE) – технология, обеспечивающая изоляцию пользователей, позволяющая ограничить ресурсы, доступные конкретному процессу или пользователю (CPU, память, использования диска, количество процессов).

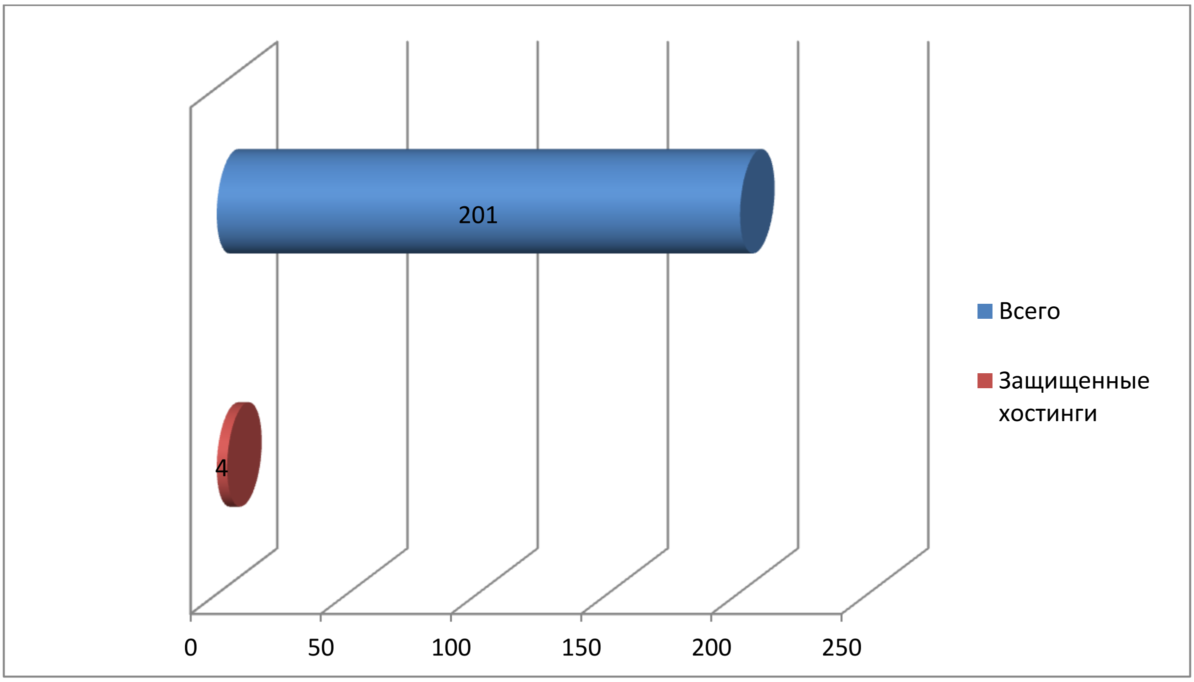
✓ CageFS - виртуальная файловая система, персональная для каждого пользователя. Файловые системы пользователей изолированы друг от друга, поэтому пользователи не могут обращаться к чужим файлам. Это способствует предотвращению хакерских атак и воровства данных, повышая уровень безопасности.

В ходе исследования мы столкнулись с тем, что, хостинг-провайдеры намерено или непреднамеренно де-факто дезинформировали своих клиентов, сообщая, что хостинг обеспечивает защиту веб-сайта от взлома только потому, что у них защищенные серверы. Для неопытного пользователя, в большинстве случаев, нет разницы, идет ли речь о защите сервера или о защите его сайта.

Безопасный хостинг не просто обеспечивает мониторинг и сканирование вирусов, но и использует меры по безопасности, направленные на обеспечение превентивной защиты от взлома веб-сайта.

По итогам исследования определилось, что только 2% хостинг-провайдеров, обеспечивают защиту веб-сайтов клиентов от взлома по умолчанию (то есть базовая услуга shared-хостинга уже включает в себя защиту веб-сайта от взломов, а не как дополнительная услуга, далее «безопасный хостинг»).

Диаграмма 3.1. **Количество «безопасных хостингов»**



Источник: ComNews Research

Такой колоссальный разрыв свидетельствует о том, что пока сегмент «безопасных хостингов» находится на начальном этапе развития. Можно предположить, что этот факт обусловлен незаинтересованностью хостинг-провайдеров или же нежеланием взваливать на себя дополнительные обязательства, внедрять новые технологии и программно-аппаратные комплексы. Но с другой стороны мы имеем типичную ситуацию, когда рынок сам себя регулирует: нет спроса – нет услуги. По мнению экспертов, проблема кроется в том, что пока степень осведомленности владельцев веб-сайтов о веб-угрозах невелика, владельцы малого бизнеса неохотно тратят средства на обеспечение превентивной защиты. Для многих взлом собственного веб-сайта по-прежнему нечто абстрактное и далекое, и способствует тому множество заблуждений про безопасность веб-сайтов, которыми предприниматели себя успокаивают и обманывают. Пока еще многие не готовы решать проблему безопасности заранее и обращаются по факту возникновения инцидента.

По мнению экспертов, каждый клиенто-ориентированный хостинг мог бы обеспечивать хотя бы частичную защиту от типовых атак на веб-сайты. Например, создать внешний рубеж обороны веб-сайтов, отфильтровывая значительную часть веб-атак и закрывать уязвимые компоненты веб-сайтов клиентов проактивной защитой. Конечно, массово защитить веб-сайты на 100% невозможно, поскольку у каждого веб-сайта есть своя архитектура, особенности: кому-то требуются внешние подключения, кому-то разрешенные системные функции и пр. Но даже общие меры, в целом, снизят число зараженных веб-сайтов, поскольку большая часть страдает именно от нецелевых автоматизированных средств. Второй важный момент, отмеченный экспертами и о котором стоит задуматься хостинг-компании - это техническая изоляция веб-сайтов на аккаунте хостинга, когда каждый веб-сайт работает внутри некоторой виртуальной машины. Правильно настроенные права и конфигурация веб-сервера позволяет изолировать зараженный ресурсы и исключить массовый взлом веб-сайтов на аккаунтах пользователей.

В ходе исследования специалисты ComNews Research определили хостинги России, которые обеспечивают защиту веб-сайтов от взлома, в рамках базового тарифа услуг shared - хостинга. Перечень хостингов можно увидеть в Таблице 3.2. Примечательно, что из представленных компаний, только один крупный и известный хостинг – Reg.ru.

Таблица 3.2. **Перечень хостингов с защитой веб-сайтов от взлома**

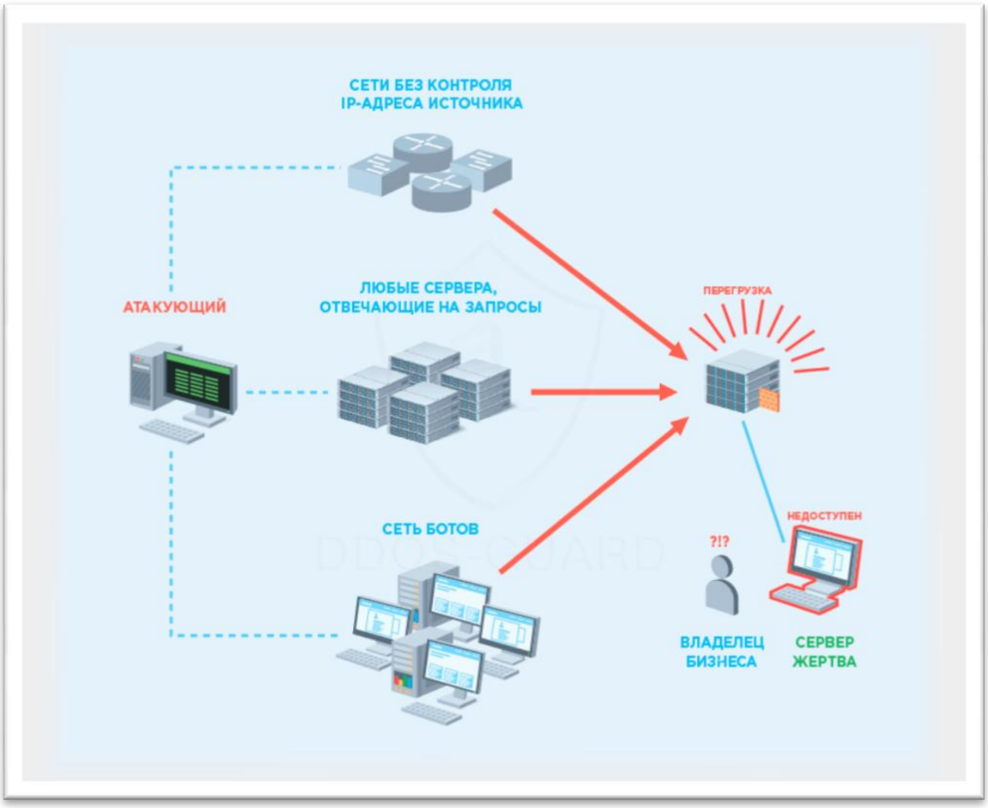
№	Хостинг-провайдер, юридическое лицо владелец	Юридическое лицо владелец	Месторасположение, город
1	Hostlend.ru	ООО «ИТ-Новация»	Москва
2	Optibit.ru	ООО «Оптизон»	Красноярск
3	Reg.ru	ООО «Регистратор доменных имен РЕГ.РУ»	Москва (главный офис), 29 офисов по России
4	Yutex.ru	ООО «ИТ-Ютекс»	Ижевск

Источник: ComNews Research

Кроме того, ComNews Research выявил хостинг-провайдеров, которые за дополнительную оплату, в качестве дополнительной услуги, в том числе на отдельных серверах, также оказывают защиту веб-сайта от взлома: «WEB[XL]» (собственная разработка PHPSecure), «Flynet.pro» (защита на отдельных серверах), «Mchost.ru», Ddosov.net (защищённый хостинг предоставляется только совместно с услугой «Удалённая DDoS защита»), «Stalkerhost.net» (защита на отдельных серверах), «webguard.pro», «StormWall». Необходимо понимать, что если дополнительная услуга защиты веб-сайта будет оказана не на отдельном сервере, то возможность взлома будет достаточно велика, так как при взломе соседей защищенного веб-сайта, опасности подвергаются все веб-приложения аккаунта, в том числе и защищенные.

В рамках исследования специалисты ComNews Research также провели монтиринг хостингов, обеспечивающих защиту от DDoS–атак (Distributed Denial of Service attack). Под DDoS понимается комплекс действий, способный полностью или частично вывести из строя интернет-ресурс. В качестве жертвы может выступать практически любой интернет-ресурс, например веб-сайт, игровой сервер или портал госуслуг. На данный момент практически невозможна ситуация, когда хакер в одиночку организует DDoS-атаку. В большинстве случаев злоумышленник использует сеть из компьютеров, зараженных вирусом. Вирус позволяет получать необходимый и достаточный удаленный доступ к зараженному компьютеру. Сеть из таких компьютеров называется ботнет. Как правило, в ботнетах присутствует координирующий сервер. Решив реализовать атаку, злоумышленник отправляет команду координирующему серверу, который в свою очередь дает сигнал каждому боту начать выполнение вредоносных сетевых запросов[6]

Рисунок 3.3. **DDoS-атака**



Источник: Ddos-guard

В части касающейся защиты от DDoS-атак, большинство хостинг-провайдеров (65%) имеют защиту от этого вида хакерских атак на уровне оборудования серверов, дата-центров и приложений. В эти 65% включены хостинги с DDoS защитой, которая установлена по умолчанию и как отдельная услуга.

[6] База знаний компании DDoS-GUARD.

Диаграмма 3.2. **Соотношение хостингов с DDoS защитой**

Источник: ComNews Research

Защита от DDoS-атак на уровнях Layer 3/Layer 4 не обеспечит защиту от DDoS конкретного веб-приложения, такая защита скорее нужна самому хостинг-провайдеру, чтобы его оборудование смогло выдержать DDoS атаку.

Важным аспектом клиенто-ориентированности хостинг-провайдера является наличие услуги лечения веб-сайта. Ни один веб-сайт не может получить 100% защиту от взлома, и когда взлом случился, клиенту необходимо как можно скорее вылечить веб-сайт для минимизации рисков. Для того, чтобы веб-сайт был полностью пролечен, без вредоносных компонентов, проводится сканирование файлов веб-сайта на наличие вирусов, веб-шеллов, бэкдоров, спам-рассыльщиков, фишинговых страниц, дорвей-страниц (поисковый спам) и других вредоносных и хакерских скриптов. Также выполняется диагностика страниц веб-сайта внешним сканером для определения мобильных и поисковых редиректов, опасных виджетов и кодов недобросовестных рекламных сетей. Проверяется база данных на наличие хакерских вставок и вирусных инжектов. В этой связи, возможность пролечить веб-сайт у своего же хостинга, наиболее оптимальный, в плане временных затрат, вариант.

Диаграмма 3.3. **Соотношение хостингов с услугой лечения веб-сайта**

Источник: ComNews Research

Как видно из Диаграммы 3.3, 52% хостинг-провайдеров оказывают услугу лечения веб-сайта после взлома. Мы учитывали и платные и бесплатные (в рамках предоставления shared-хостинга) услуги. Такое соотношения ещё раз подчеркивает, что хостинг-провайдерам нужно акцентировать внимание на Value Added Services (VAS), то есть, не просто ограничиваться основными услугами, но и создавать комфортную экосистему для клиентов. Таким образом, заказчики (владельцы веб-сайтов) смогут оперативно восстановить веб-сайт и минимизировать потери. Более того, такой хостинг будет намного привлекательнее для клиентов и сможет выступать в качестве единого оператора по обеспечению жизнедеятельности веб-приложений.

Интересным аспектом предоставления услуг хостинг-провайдера, который, по мнению экспертов, незаслуженно обходят стороной, является сам договор-оферта на оказание услуг. Традиционно, в договорах, прописываются права и обязанности сторон, регламенты оказания услуг и другие условия. ComNews Research проанализировал договоры-оферты и регламенты для физических и юридических лиц исследуемых хостингов, и определил, сколько хостинг-провайдеров прописывают у себя в договоре пункты по информационной безопасности и берут на себя ответственность обеспечения информационной безопасности серверов и ресурсов клиента (защищенные серверы, сетевое оборудование).

Диаграмма 3.4. **Соотношение хостингов с юридическими обязательствами (договорные обязательства) перед клиентами об обеспечении информационной безопасности**

Источник: ComNews Research

В ходе исследования мы выяснили, что только 11% хостинг-провайдеров в договорах-офертах прописывают пункт об информационной безопасности и берут на себя ответственность обеспечить безопасность серверов и ресурсов клиента. Безусловно, данный тип защиты не подразумевает обеспечение защиты от взлома веб-сайта, но наглядно показывает, какое внимание хостинги уделяют вопросам, связанных с информационной безопасностью.

Из этих 11% хостингов есть только один хостинг («Optibit.ru»), который «на добровольной основе принимает дополнительные обязательства (при наличии технической возможности)» для защиты веб-сайта от взлома: проведение круглосуточного мониторинга сети, принятие мер по обнаружению источников угрозы; блокировка распространения спама; сканирование услуг хостинга на вредоносное программное обеспечение; анализ трафика на попытку взлома и блокировка злоумышленника; блокировка IP-адреса при DDoS-атаках. Наличие таких гарантий - несомненное преимущество для владельцев веб-сайтов при выборе технологической площадки.

Важным моментом при выборе хостинг-провайдера является наличие услуги обязательного резервного копирования. Довольно часто веб-сайты, из-за действий вирусов, злоумышленников, физических поломок сервера, сбоев в программном обеспечении, некорректных действий веб-программистов, теряют базы данных и, де-факто, перестают существовать. Чтобы восстановить веб-сайт есть два пути:

- сделать его заново;
- восстановить из ранее сохраненной резервной копии.

Резервное копирование это сохранение копий веб-сайта вместе со всем содержимым и настройками на специально отведённом месте сервера.

На Диаграмме 3.5. можно увидеть, сколько хостинг-провайдеров берут на себя ответственность выполнять резервное копирование данных клиента в рамках договора-оферты о предоставлении услуг в России.

Диаграмма 3.5. **Соотношение хостинг-провайдеров с юридическими обязательствами (договорные обязательства) перед клиентами об обеспечении резервного копирования**

Источник: ComNews Research

В ходе исследования выяснилось, что только у 29% хостингов есть обязательство перед клиентом-заказчиком выполнять резервное копирование (в том числе и совместное обязательство хостинга и владельца веб-сайта). В остальных случаях, эта функция полностью возложена на клиента.

4. Обзор используемых мер хостинг-провайдерами по обеспечению информационной защиты клиентов

Для shared-хостингов ответственность за безопасную настройку сервера лежит на администраторе хостинга. Для выделенных серверов - на владельце сервера.

Как в случае shared -хостинга, так и в случае выделенных серверов конфигурация должна обеспечивать минимальную свободу действий, не нарушающих работоспособность веб-сайта. То есть на сервере должны быть разрешены только самые необходимые функции, а все остальные маневры - запрещены. Например, если веб-сайт не выполняет внешних подключений к другим серверам, должны быть отключены опции внешних соединений. Если веб-сайт не использует системные вызовы (system, shell_exec, и др.), эти функции необходимо отключить. Кроме того, должна быть ограничена область видимости файловой системы из скриптов и многое другое. Обо всем этом должен позаботиться системный администратор сервера.

На одном сервере shared-хостинга размещаются сотни веб-сайтов, и каждому веб-сайту требуются свои функции. Поэтому хостинги максимально лояльно подходят к вопросам настроек сервера, разрешая практически все. Применение таких политик сказывается на общем уровне безопасности всех веб-сайтов, размещенных на серверах. В этой связи, особое внимание уделяется применяемым мерам по обеспечению безопасности веб-приложений. Проанализировав ответы хостинг-провайдеров, можно выделить следующие технологии по обеспечению безопасности (кроме тех, которые были перечислены в пункте 3).

Антивирус Virusdie позволяет найти подозрения, возможные заражения в файлах веб-сайта и устранить их в автоматическом режиме. По желанию клиента, хостинг-провайдер устанавливает Virusdie на сервере. Антивирус позволяет обнаруживать и устранять шеллы, бэкдоры, вирусы-трояны, редиректы и вредоносные коды в PHP, HTML, JS, файлах изображений и системных файлах. Virusdie не просто удаляет определенные файлы или помещает их в карантин, а «лечит» их, удаляя фрагменты кода и, в случае необходимости, дописывает недостающие для сохранения работоспособности веб-сайта фрагменты.

Антивирус Maldet. Сканер для Linux, предназначенный для поиска веб-шеллов, спам-ботов, вирусов-троянов, злонамеренных скриптов и других типичных угроз, характерных для веб-пространств, и особенно актуален для виртуальных shared-хостинг платформ. Главное отличие от других Linux-антивирусов — его веб-направленность, сканирование файлов веб-сайтов.

Хостинг провайдеры также осуществляют **сканирование логов и сканирование вирусов на уровне сервера**, что позволяет обеспечить защиту оборудования от вредоносного ПО и попыток взлома.

Мониторинг заблокированных веб-сайтов в Google Safe Browsing. Мониторинг заблокированных веб-сайтов в Google Safe Browsing является дополнительной защитой пользователей от опасных интернет-ресурсов. Де-факто это реестр опасных веб-сайтов, которые были замечены в распространении вирусов, либо подозреваются в мошенничестве.

Защита от брутфорс атак. Брутфорс — это метод взлома, основанный на переборе всех вариантов паролей по словарю - злоумышленник пытается получить доступ к серверу перебирая все возможные комбинации. Среди используемых программ хостинг-провайдерами для защиты от брутфорс атак: Fail2Ban, DenyHosts и др.

Дополнительная авторизация на уровне сервера и панелей администраторов. Взломанный веб-сайт, как правило, используется для рассылки спама или заражения посетителей веб-сайта вирусом. При этом злоумышленник подменяет некоторые файлы, для возможности дальнейшего доступа к уязвимым файлам. Еще одна большая проблема - это уязвимости в панелях администратора, в частности визуальном редакторе панели администратора веб-сайта. Лечение такого веб-сайта занимает много времени и средств и доставляет много неудобств. Для решения этой проблемы, существует дополнительная авторизация, которая делает бессмысленным подбор пароля ботнетами хакеров.

Блокировка веб-сайта. Одной из наиболее частных мер хостинг-провайдеров является блокировка веб-сайта. Чаще всего происходит в случае нарушения веб-сайтом правил пользования хостингом, взломом веб-сайта, DDoS-атаки, превышения допустимой нагрузки на сервер, вследствие чего, страдают другие абоненты хостинг-провайдера.

Программа PHPsecure (собственная разработка хостинга WebXL) – защита от PHP-скриптов, фильтрация запросов, сканнер угроз. Защита происходит в режиме реального времени.

Технология «freeze» - “заморозка” сайтов (собственная разработка хостинга Optibit)- позволяет запретить изменять файлы, даже если злоумышленник получил пароль к FTP или взломал скрипты используя уязвимость сайта.

Защита от DDoS атак. По данному виду защиты специализируется около 66% исследуемых хостингов. Защита от **DDoS атак** достаточно распространена среди хостинг-провайдеров. Некоторые оказывают её как базовую услугу – по умолчанию, в рамках услуги shared-хостинга, другой сегмент хостингов – в качестве дополнительной услуги. Из применяемых технологий можно выделить собственную разработку хостинга StormWall, с использованием системы FlowSense. Система FlowSense постоянно просматривает все потоки данных, идущие к серверу, отслеживает аномалии и автоматически определяет текущий тип атаки. По результатам происходит динамическая подстройка параметров защиты с использованием BGP FlowSpec (RFC 5575) и API системы хостинга.

5. Профили хостинг-провайдеров России, обеспечивающих информационную защиту веб-сайтов от взлома

Первым провайдером в России, который в октябре 2014 года начал оказывать сервис по защите веб-сайтов от взлома, стал хостинг из Красноярска «Optibit.ru», через год – в конце 2015 года - возможности по защите от атак на основе известных уязвимостей появились у клиентов крупнейшего хостинг-провайдера России - «Reg.ru». В апреле 2016 года запустил услугу хостинг из Ижевска «Yutex.ru», а в ноябре 2016 года - хостинг «Hostlend.ru» начал оказывать защиту веб-сайтов от взлома.

Таблица 5.1. **Характеристики «безопасных хостинг-провайдеров»**

№	Хостинг-провайдер	Дата начала оказания защиты веб-сайтов от взлома	Услуга лечения веб-сайта	Юридическое обязательство об обеспечении информационной безопасности перед клиентом (договор)	Юридическое обязательство об обеспечении резервного копирования (договор)
1	Optibit.ru	Октябрь 2014	+	+	+
2	Reg.ru	Конец 2015	+	–	+
3	Yutex.ru	Апрель 2016	+	–	–
4	Hostlend.ru	Ноябрь 2016	+	–	+

Источник: ComNews Research

При этом, из всех «безопасных хостингов», только один хостинг-провайдер берет на себя юридические обязательства перед клиентом об обеспечении информационной безопасности сервисов и ресурсов, а также обеспечении мер по защите веб-сайтов от взлома. Все компании, за исключением хостинга «Yutex.ru», обязуются перед клиентом выполнять резервное копирование веб-сайта.

5.1. Hostlend.ru

Компания ООО «ИТ-Новация» (бренд «Hostlend.ru»), расположена в г. Москве, основана в 2013 году. Предоставляет услуги виртуального хостинга, выделенного виртуального сервера, выделенного сервера, а также услуги регистрации доменов. Отказоустойчивость серверов составляет 99,9%. Используется сетевое и передающее оборудование производства Cisco, Juniper, HPE и Supermicro[7].

[7] Информационно-аналитический сборник «Красноярск-Электронный» N5, 2013 г. http://www.admkrsk.ru/administration/structure/infotelecomupr/Documents/сборник%20(2).pdf.

Таблица 5.1.1. **Сетка тарифов хостинг-провайдера «Hostlend.ru»**

Стоимость, руб./мес.	Хостинг	VPS	Аренда сервера	Регистрация/Продление Доменов
Min	100 (1 Гб)	500 (30 Гб)	8400 (32 Гб)	160 (*.ru*)
Max	2200 (60 Гб)	3400 (150 Гб)		420 (*.de*)
Средняя	1500 (31 Гб)	1950 (90 Гб)	8400 (32 Гб)	290

Источник: ComNews Research

5.2. Optibit.ru

Красноярская компания ООО «Оптизон» (бренд «Optibit.ru») основана в 2008 году. Предоставляет услуги виртуального хостинга, выделенного виртуального сервера, выделенного сервера, а также услуги регистрации доменов. Компания владеет собственным дата-центром, а также Сибирской точкой обмена трафиком SIBIR-IX. Дата-центр «Оптизон» генерирует 20-30 Гигабит/с, что составляет 30-40% от общего городского трафика SIBIR-IX [8] Наличие собственной ИКТ инфраструктуры обеспечивает определенную независимость компании от внешних поставщиков услуг. В 2014 году через дата-центр «Optibit.ru» «транслировалась» в Сибирском регионе олимпиада Сочи-2014. Используется сетевое и передающее оборудование производства Cisco, HPE и DEPO Computers[9].

Таблица 5.2.1. **Сетка тарифов хостинг-провайдера «Optibit.ru»**

Стоимость, руб./мес.	Хостинг	VPS	Аренда сервера	Регистрация/Продление Доменов
Min	667 (5 Гб)	315 (5 Гб)	4300 (8 Гб)	180 (*.ru, рф*)
Max	1250 (20 Гб)	5040 (9 Гб)	17600 (48 Гб)	2990 (*.guru*)
Средняя	959 (13 Гб)	2677 (7 Гб)	10950 (28 Гб)	1585

Источник: ComNews Research

[8] Optibit.ru https://www.optibit.ru/.
[9] Optibit.ru https://www.optibit.ru/.

5.3. Reg.ru

Компания ООО «Регистратор доменных имён РЕГ.РУ» (бренд «Reg.ru») основана в 2006 году и является одним из крупнейших российских хостингов и регистратором доменов. Особенностью Reg.ru является поглощение компанией других хостинг провайдеров, таких как «Host-telekom.ru», «Leaderhost.ru», «Mobyhost.ru», «Omegahost.ru», «Agava.ru», «50web.ru». Эти бренды, продолжают функционировать, но абоненты полностью переданы на обслуживание Reg.ru. На данный момент в компании на обслуживании более 2 700 000 доменов[10].

Таблица 5.3.1. **Сетка тарифов хостинг-провайдера «Reg.ru»**

Стоимость, руб./мес.	Хостинг	VPS	Аренда сервера	Регистрация/Продление Доменов
Min	84 (7 Гб)	449 (15 Гб)	6675 (16 Гб)	199 (*.ru, рф*)
Max	824 (35 Гб)	20607 (500 Гб)	24302 (1920 Гб)	105225 (*.ki*)
Средняя	454 (21 Гб)	10553 (258 Гб)	15488 (968 Гб)	52712

Источник: ComNews Research

5.4. Yutex.ru

Компания «ООО ИТ-Ютекс» (бренд «Yutex.ru»), была основана в 2011 году, и расположена в г. Иркутске. Предоставляет услуги виртуального хостинга, выделенного виртуального сервера, выделенного сервера, а также услуги регистрации доменов. Отказоустойчивость серверов составляет 99,95%. На обслуживании хостинга состоит более 12 тысяч веб-сайтов[11].

Таблица 5.4.1. **Сетка тарифов хостинг-провайдера «Yutex.ru»**

Стоимость, руб./мес.	Хостинг	VPS	Аренда сервера	Регистрация/Продление Доменов
Min	199 (4 Гб)	410 (30 Гб)	2680 (4 Гб)	117 (*.рф*)
Max	599	1050	5320	2000 (*.kz*)

[10] Reg.ru https://www.reg.ru/.
[11] Yutex.ru https://www.yutex.ru/.

	(30 Гб)	(120 Гб)	(32 Гб)	
Средняя	399 (17 Гб)	730 (75 Гб)	4000 (18 Гб)	1059

Источник: ComNews Research

Необходимо отметить, что стоимость и выбор услуг хостинг-провайдеров зависит от многих факторов, ключевыми из которых являются: профессионализм технической поддержки, процессорная мощность и объем жесткого диска.

6. ВЫВОДЫ И РЕКОМЕНДАЦИИ

Глобальная сеть Интернет стремительно трансформируется. Ещё 5-6 лет назад Интернет был «дружелюбным», почти безопасным, взломы случались, но не были столь массовыми и носили точечный, целевой характер.

За последние 4 года сеть стала агрессивной и опасной, происходят постоянные атаки на веб-приложения (проверка уязвимостей, поиск чувствительных файлов и др.). По данным Google, за один год количество взломанных веб-сайтов возросло на 34%.

Основная масса взломов - нецелевые веб-атаки с помощью автоматизированных средств, выполняемые посредством ботов или инструментов хакеров. Если посмотреть на соотношение трафика реальных посетителей и ботов, то сейчас оно составляет 50/50. То есть почти половина запросов к веб-сайту - это боты, и большая часть запросов от ботов является сканированием веб-сайтов на различные уязвимые компоненты, версии CMS-платформ, подбор паролей и пр. Атаки становятся более сложными, трафик шифруется и маскируется под легитимные запросы. Сейчас достаточно сложно выделить в трафике запросы от ботов, используя стандартные инструментальные средства анализа.

Атаки проводятся по большим выборкам веб-сайтов, уязвимых к определенным видам хакерских атак, например, уязвимым версиям модуля Joomla! или WordPress. Автоматическим нецелевым взломам подвержены, как бесплатные, так и коммерческие CMS. Любой веб-сайт, безопасности которого не уделяют внимание, становится потенциальным объектом взлома и заражения.

В 2016 году наблюдался беспрецедентный рост Ransomware. В глобальном измерении количество атак такого вида хакерства возросло на 267%. В 2017 году эта тенденция нашла своё яркое продолжение. В начале мая 2017 года состоялась самая крупная эпидемия программы-вымогателя WannaCry. Вирус захватил более 150 стран, наибольший удар пришелся на Россию. Хакеры заразили компьютеры с операционной системой Windows вирусом-вымогателем WannaCry, который требовал от пользователя «выкуп» в биткоинах за снятие блокировки с операционной системы. В России хакеры атаковали компьютеры Сбербанка, мобильного оператора «МегаФон», МВД и МЧС России. Атака была остановлена, а вопросы информационной безопасности всё чаще начали звучать в информационном пространстве. Взлом перестал быть чем-то абстрактным и для владельцев веб-сайтов.

Вопрос защиты своих ресурсов от взлома, становится критическим, а средства защиты более востребованы не только на уровне крупных интернет-площадок, но и среди блогеров, компаний малого и среднего бизнеса, владельцев веб-сайтов с небольшой аудиторией.

В этой связи, непрофильные компании в области информационной безопасности запускают услуги связанные с мониторингом и обеспечением информационной защиты. Так, например, компания ПАО «МТС» до конца этого года планирует выйти на рынок услуг информационной безопасности для продажи сторонним заказчикам коммерческих сервисов по противодействию киберугрозам. Для выхода на новый рынок МТС запустила центр мониторинга информационной безопасности (Security Operations Center, SOC), работающий в режиме 24x7. Пока SOC работает для нужд МТС, а в дальнейшем будет выходить на коммерческий уровень.

Требования возрастают и к выбору хостинг-провайдеров. Традиционно, защитой от взлома обязан заниматься веб-программист, или веб-студия конкретного интернет-проекта: обновлять платформу, плагины, закрывать уязвимости своего веб-сайта. На данный момент, 98% хостингов выступает не более чем cloud resource. С учетом теперешних угроз, такая схема взаимодействия недостаточна. Хостинг не может гарантировать 100% защиту от взлома, но, с целью обеспечения безопасности в современном интернете, должен внедрять на своих ресурсах средства защиты от известных атак. На данный момент, большинство владельцев веб-сайтов предполагают, что защитой является: мониторинг угроз, сканирование, лечение. Владельцы не всегда понимают, для чего нужна превентивная защита от взлома: анализ сигнатур, патчи уязвимостей, защита WAF, технологии CloudLinux, цементирование (заморозка) веб-сайтов и др. Такой расклад порождает типичную рыночную ситуацию: нет спроса - нет предложения.

Тем не менее участники рынка понимают, что количество и агрессивность взломов будет расти и защита веб-сайта становится необходимой мерой для дальнейшего существования того или иного веб-проекта. В этой связи выбор площадки под веб-сайт не должен ограничиваться категориями дорого/дёшево, в первую очередь должны оцениваться наличие средств (аппаратно-программного комплекса) и компетенций в области защиты веб-сайтов от действий хакеров и вредоносного ПО. В ходе исследования, мы выяснили, что только у 2% хостинг-провайдеров («Hostlend.ru», «Optibit.ru», «Reg.ru», «Yutex.ru») установлены на базовом тарифе shared-хостинга средства и технологии защиты веб-проектов от взлома, а первым хостингом, который начал оказывать услуги защиты веб-сайта от взлома, оказался Красноярский хостинг «Optibit.ru». Примечательно, что при анализе договоров-оферт хостингов, только у компании «Optibit.ru» была формулировка о принятии обязательств выполнения мероприятий по защите веб-приложений от злоумышленников. Всего 11% хостингов в рамках договора берут на себя обязательство обеспечивать информационную безопасность серверов и средств клиента, в остальных 89,5% случаев, вся ответственность лежит на клиенте.

В том случае, если веб-сайт всё-таки взломали, первый вопрос, который возникает перед владельцем веб-сайта, где, и как быстро его можно восстановить. Скорость решения вопроса имеет большое значение, так как хостинги, в большинстве случаев, не дают время на удаление причины, а практически сразу (при обнаружении подозрительного трафика) блокируют веб-сайт. Веб-сайт, будучи скомпрометирован, моментально теряет свои позиции в поисковике и посетителей веб-сайта (следовательно – теряет деньги). Если хостинг заинтересован в том, чтобы клиенты не уходили за помощью к специализированным компаниям, он имеет в своем портфеле предложений услуги лечения веб-сайта. ComNews Research определил, что 52% исследуемых хостингов предлагают услугу (платную/бесплатную) лечения веб-сайта. Можно сказать, что в плане лечения хостинги имеют возможность потенциального роста, кроме того, создание VAS позволит увеличить прибыль компании, создав благоприятную среду для своих клиентов. К таким услугам стоит отнести и резервное копирование.

Майские события показали, что своевременный бэкап является важным аспектом сохранности веб-сайта. Благодаря столь простому действию, данные будут восстановлены, и веб-сайт, в случае взлома, не придется создавать заново. Проанализировав договоры, выяснилось, что только 29% хостингов берут на себя обязательство осуществлять регулярное резервное копирование. В остальных случаях, за бэкап отвечает только клиент.

Ситуация с защитой от DDoS более оптимистична, 65% хостингов имеют средства защиты от данного вида хакерских атак на уровне Layer3 /Layer 4, а также Layer 7 (стоимость услуги защиты от DDoS на уровне Приложения достаточно высока и в среднем составляет 18 - 20 тысяч руб/месяц).

Анализ рынка хостинг-провайдеров показал, что несмотря на:

- очевидные изменения в сети Интернет, которые несут постоянные угрозы и риски для пользователей;
- всевозрастающее количество взломов веб-сайтов из года в год;
- потребность в защите веб-площадок клиентов от взломов;

хостинг-провайдеры, пока что имеют достаточно слабые позиции в сегменте защиты информационной безопасности веб-приложений клиентов (2% хостингов), а также весьма низкий процент принятия на себя юридических обязательств в части обеспечения информационной безопасности серверов и ресурсов клиентов, а также выполнения резервного копирования (11 % и 29% соответственно). В части касающейся услуг лечения веб-сайтов и защиты от DDoS атак наблюдается более высокий процент проникновения этих сервисов (52% и 65% соответственно), но с учётом того, что такие услуги должны становиться массовыми для обеспечения потребностей клиентов, остается достаточно большой потенциал для дальнейшего роста уровня внедрения.

Стоит отметить, что внедрение соответствующих технологий и сервисов требует увеличения CAPEX (Capital expenditure), что для хостингов может быть неподъемной ношей в плане окупаемости, особенно для небольших операторов. Практика показывает, что вложения в модернизацию и совершенствование своей инфраструктуры являются стратегически важным и необходимым направлением в бизнесе операторов. Вложения средств закономерно «потянут» за собой рост цен на тарифы. По мнению хостингов, такая мера может отпугнуть клиентов, которые уйдут на более дешёвые площадки. Такой риск есть всегда. Но тенденции современного мира сети Интернет наглядно демонстрируют, что взломы будут учащаться и становиться более сложными и массовыми. Учитывая то, что на одном аккаунте хостинга размещаются сотни веб-сайтов, взлом одного веб-сайта будет означать взлом и его «соседей» – всего аккаунта. Встроенные механизмы изоляции веб-сайтов внутри виртуальной площадки, технологии «цементирования» становятся необходимостью. В ином случае, владельцы веб-сайтов будут искать хостинги, у которых установлены средства и применяются технологии защиты от взломов, которые позволят минимизировать возможности взлома. Иными словами наличие средств обеспечения информационной безопасности веб-сайтов становится «must have», для компаний, оказывающих услуги хостинга. Применение хостингами технологий защиты от взломов, позволит существенно снизить количество инцидентов и повысить надежность не только каждого аккаунта, но и каждого веб-сайта.

Приложение 1. Перечень использованной литературы

1. Securi «Website Hacked Trend Report», 2016, H1.
2. Malwarebytes «State of Malware Report», 2017.
3. Блог компании Acronis, Inc. https://habrahabr.ru/company/acronis/blog/328796/.
4. Григорий Земсков «Как взламывают веб-сайты (через уязвимости, по вине сотрудников или подрядчиков) и как от этого уберечься» http://www.cossa.ru/234/134334/.
5. Блог компании Positive Technologies https://habrahabr.ru/company/pt/blog/269165/.
6. База знаний компании DDoS-GUARD.
7. Hostlend.ru http://hostlend.ru/.
8. Информационно-аналитический сборник «Красноярск-Электронный» N5, 2013 г. http://www.admkrsk.ru/administration/structure/infotelecomupr/Documents/сборник%20(2).pdf.
9. Optibit.ru https://www.optibit.ru/.
10. Reg.ru https://www.reg.ru/.
11. Yutex.ru https://yutex.ru/.

Приложение 2. Таблица1. Перечень хостингов с защитой веб-сайтов от взлома

См. Таблицу 1. Excel во вложении к Отчету.

Приложение 3. Таблица 2. Сводная таблица услуг защиты от DDoS-атак и лечения веб-сайтов

См. Таблицу 2. Excel во вложении к Отчету.

Приложение 4. Таблица 3. Юридические обязательства хостинг-провайдеров перед клиентами

См. Таблицу 3. Excel во вложении к Отчету.