серверов с информацией о текущем состоянии и надежных протоколов. Поэтому независимо от того, куда вы подключаетесь, вы точно будете знать, чего ожидать. С точки зрения производительности, скорость соединения просто потрясающая. В целом, это очень надежный продукт с хорошим пользовательским интерфейсом, который отлично подходит для локальной домашней сети. Компания также сотрудничает с SugarSync и предоставляет 250 ГБ зашифрованного облачного хранилища для каждого плана.

ProtonVPN - с открытым исходным кодом и особым акцентом на безопасность

Компания была основана инженерами и учеными из CERN с целью создания зашифрованных сообщений электронной почты и VPN для защиты активистов и журналистов. Ее головной офис находится в Швейцарии, где действуют очень строгие законы о неприкосновенности частной жизни. ProtonVPN серьезно относится к безопасности, поэтому использует надежные протоколы, сильное шифрование и функцию kill switch, которая предотвращает утечку ваших данных в интернет. Наконец, все приложения имеют открытый исходный код, которые, как заявляет компания, постоянно проходят независимую проверку.

Norton Secure VPN - известный и пользующийся доверием бренд

Производительность Norton Secure VPN находится на среднем уровне, а среди доступных платформ можно найти только Mac, iOS, Windows и Android. Его не рекомендуется использовать на роутерах, Linux или игровых площадках. В многоуровневых ценах на услуги с первого раза не разберешься, но если кратко - стоимость повышается на \$10 при переходе с одного устройства на пять и еще на \$10 при переходе на десять устройств. Norton - это отличный VPN от надежного бренда, который заслуживает доверия. Компания также имеет круглосуточную поддержку по телефону в режиме реального времени и предлагает отличную 60-дневную гарантию возврата денег.

StrongVPN - простой и понятный VPN

StrongVPN выделяется тем, что его настройка ясна и проста для понимания. Он не ведет журналов, не собирает информацию о пользователях и, конечно же, надежно шифрует данные. Strong также отличается хорошей производительностью и отлично выполняет свою работу. К тому же, недавно компания увеличила количество одновременных подключений - с 5 до 12. Она также включила 250 ГБ защищенного хранилища SugarSync во все планы.

В заключении скажем, что какие бы VPN сервисы вы не использовали, не стоит забывать о минимальных правилах гигиены в интернет-пространстве. VPN – это не 100%-ная защита.

1. Как работает VPN? <https://www.cactusvpn.com/ru/beginners-guide-to-vpn/how-does-a-vpn-work/> (дата обращения: 09.11.2020).
2. 10 лучших VPN для России в 2020 году: протестированы все приложения, скорости, безопасность и другие параметры <https://ru.wizcase.com/> (дата обращения: 09.11.2020).

Шабает М.Б., Джангаров А.И.
Базовая защита сайта от хакерских атак

*Чеченский государственный университет
(Россия, Грозный)*

doi: 10.18411/lj-12-2020-42
idsp: ljjournal-12-2020-42

Аннотация

В этой статье рассматривается актуальная тема обеспечения безопасности сайта. Обсудим, как защитить себя от кибератак, на что обратить особое внимание. Также

рассмотрим основные методы хакерских атак и решения, призванные им противодействовать.

Ключевые слова: хакерская атака, безопасность сайта, антивирус, киберзащита.

Abstract

The article describes the current topic of site security. We will discuss how to protect yourself from cyber attacks, what to pay special attention to. We will also consider the main methods of hacker attacks and solutions designed to counter them.

Keywords: hacker attack, site security, antivirus, cyber protection

Создание сайта - сложный и многоэтапный процесс, требующий учета многих аспектов. Веб-сайт должен выделяться не только графическим дизайном или общим контентом, но и своей функциональностью, удобством использования. Создание веб-сайта неразрывно связано с вопросом позиционирования. Чтобы разработать эффективную стратегию SEO, которая обеспечит видимость в результатах поиска, необходимо принять во внимание множество факторов ранжирования Google, включая безопасность веб-сайта. Как защитить себя от кибератак? На что обратить особое внимание?

Не стоит откладывать вопрос защиты веб-сайта на потом как вопрос малой важности - это важно на самом первом этапе, когда речь идет о начале разработки веб-сайта. Такой подход должен заставить, например, тщательно проанализировать выбор хостинга. Бесплатные решения очень рискованны. Стоит обратить внимание на то, предлагает ли провайдер адекватную административную поддержку, регулярную подготовку полных резервных копий данных (бесценно в случае хакерских атак, но также и других проблем с сайтом), ограничения доступа (на основе IP / адреса хоста), мониторинг. Хороший сервер будет также быстрее реагировать на запросы браузера, а скорость загрузки страницы - еще один фактор, влияющий на позиционирование, поэтому можно улучшить работу веб-сайта не в одном аспекте, а в двух.

Аспекты создания веб-сайта связаны не только с выбором хостинга, но и с совокупностью различных основных и второстепенных решений, которые будут важны для защиты сайта. Что еще нужно учесть? В первую очередь:

- установка SSL-сертификата - это позволит защитить передачу данных между сайтом и пользователями (например, информация о кредитной карте, конфиденциальные личные данные). Secure Sockets Layer эффективно зашифрует их, чтобы они не читались даже после их возможного перехвата;
- выбор надежных паролей и уникальных логинов - в обоих случаях нужно избегать типичных, автоматически устанавливаемых, легко взламываемых решений, максимально затруднять доступ к каждой используемой службе, не сохранять данные в браузере, не сохранять их в файлах, сохраненных на диске;
- качественная антивирусная защита - бесплатный, непроверенный антивирус - не лучшее решение, нужно найти защиту, которая будет в рамках выделенного бюджета и в то же время обеспечит полноценную и безотказную работу;
- архивирование данных - желательно позаботиться о периодическом архивировании данных и их безопасном хранении, что дополнительно повысит защиту;
- обновления, тестирование и проверка веб-сайта - улучшать, развивать свой веб-сайт в соответствии с последней информацией о текущих угрозах, использовать общедоступные полезные инструменты, которые

позволят быстро обнаруживать любые нарушения, использовать проверенные расширения плагинов, темы;

- защита от кражи контента - добавление водяных знаков к фотографиям, включая информацию об авторских правах, блокировка копирования текстов, добавление ссылки на повторяющийся текст - все это затруднит распространение контента на сайте;
- поиск дополнительных решений - нужно оставаться открытыми для дополнительных эффективных методов защиты (таких как система межсетевого экрана веб-приложений, которая защищает от атак приложений 24/7).

Почему стоит обращать внимание на столько вопросов? В процессе создания сайта вскрывается множество потенциальных угроз. Речь идет не только о краже конфиденциальных данных аудитории или клиентов, которые затем продаются и используются в мошеннических целях. К наиболее популярным опасностям также относится, например, временная блокировка веб-сайта, которая позволяет киберпреступникам получить финансовую компенсацию за восстановление его полной функциональности.

Не менее часто имеется дело с кражей паролей или логинов (для систем CMR или FTP-сервера), захватом веб-сайта и перенаправлением его на спам-контент или с использованием его для массовой рассылки вредоносного спама. Разработчики веб-сайтов также рискуют установить на сервер множество трудно удаляемых вирусов, которые затем могут распространяться, сознательно или нет. Атакованный веб-сайт также может оказаться на более низкой позиции в результатах поиска из-за манипуляций хакеров на уровне контента. Таким образом, опасности касаются самого веб-сайта, а также взаимодействия пользователя с веб-сайтом или заражения других страниц.

Рис 1. Топ видов атак на веб-сайты

Методы хакерских атак все еще развиваются и совершенствуются, а их разнообразие делает невозможным использование одного универсального решения для всех угроз безопасности при создании веб-сайта. В настоящее время чаще всего встречаются:

- SQL-инъекция - метод, использующий вредоносный код SQL для управления серверной базой данных с целью получения доступа к конфиденциальной информации (например, к данным компании, спискам пользователей, данным частных клиентов);
- фишинг - в данном случае речь идет о захвате конфиденциальных данных (данных банковских счетов, кредитных карт, паролей для входа), но на этот раз путем выдачи себя за определенное лицо, компанию или учреждение. Существует три основных метода фишинга: целевой фишинг, уэйлинг и клонированный фишинг;
- вредоносное ПО - это атака, при которой компьютер заражается вредоносным ПО, например, во время установки, загрузки файлов, просмотра зараженных веб-сайтов или по электронной почте. К наиболее популярным типам вредоносного ПО относятся: черви, трояны, эксплойты или программы-вымогатели;
- DDoS-атака - атака, которая может быть проведена на веб-сайте или в сети и может привести к одновременной вредоносной активности из нескольких источников (компьютеров) с целью блокирования операции путем захвата всех свободных ресурсов.

Это лишь некоторые из множества разнообразных форм атаки на сайт. Пренебрежение проблемами безопасности может иметь серьезные последствия - уничтожение достижений в области позиционирования, проблемы с изображениями, блокировка или даже удаление сайта, но можно остановить такие осложнения, если прибегнуть к хорошим, проверенным мерам безопасности.

1. Как защитить и обезопасить свой сайт <https://akiwa.ru/blog/kak-zashchitit-i-obezopasit-svoy-sayt/> (дата обращения: 08.11.2020).
2. Защита сайта от хакерских атак https://pcnews.ru/blogs/zasita_sajta_ot_hakerskih_atak-699652.html (дата обращения: 08.11.2020).
3. Бабаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. - 432 с.
4. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.

Шабает М.Б., Магомедов И.А.
Базовая SEO оптимизация

Чеченский государственный университет
(Россия, Грозный)

doi: 10.18411/lj-12-2020-43
idsp: ljjournal-12-2020-43

Аннотация

В этой статье рассматривается актуальная тема оптимизации веб-сайта и повышение его позиции в поисковой выдаче. Обсудим, какие действия можно предпринять для достижения более высоких позиций. Также в данной статье даны общие рекомендации по SEO-оптимизации.

Ключевые слова: seo, оптимизация, позиционирование сайта, продвижение, веб-сайт