**Современные ВЭБ технологии.**

Готовы к инновациям в своем веб-приложении в 2022 году? Вот тренды в веб-разработке, за которыми стоит следить!

Стандарты в веб-разработке иногда меняются быстрее, чем их можно реализовать. Чтобы оставаться на шаг впереди, важно сосредоточиться на тенденциях, методах и подходах, которые набирают популярность. Независимо от ваших текущих интересов — развитие рынка, стартап-инновации или изобретения IT — вы должны быть в курсе этих тенденций. Самые горячие тренды веб-технологий, которые будут приняты в 2022 году

«Выяснение того, какой будет следующая большая тенденция, говорит нам, на чем мы должны сосредоточиться».

Даже если миллиардеры с десятилетним стажем, возглавляющие отрасль, порекомендуют нам это сделать, что мы можем сделать, кроме как согласиться? Чтобы упростить ваш поиск, сэкономить ваше время и помочь вашему бизнесу расти в новом десятилетии, здесь собраны некоторые из основных тенденций, о которых вам необходимо знать при развитии веб-бизнеса:

1. Голосовой поиск.

В настоящее время мы переживаем начало эры голосового поиска. Каждый смартфон уже оснащен цифровым голосовым помощником (Siri для iPhone, Google Assistant для телефонов на базе Android). Более того, набирают популярность умные колонки с искусственным интеллектом. В чем причина такого перехода к голосовым интерфейсам? Простота использования.

Общение — это то, чему нам не нужно учиться. Таким образом, дети и пожилые люди могут взаимодействовать с голосовыми интерфейсами без какого-либо обучения. Доступность. Цифровые голосовые помощники уже стали обычной функцией смартфонов. Умные колонки пока не так распространены, но ценник от 50 долларов является отличной предпосылкой для расширения.

В отчете говорится, что «использование голосового помощника достигает критической массы». А к 2022 году ожидается, что голосовыми помощниками будут пользоваться почти 123 млн. граждан США, или 37% всего населения. Используйте это для своего бизнеса.

Голосовой поиск — один из главных трендов электронной коммерции. Тем не менее, это также применимо ко всем предприятиям в Интернете. Если вы хотите, чтобы ваше веб-приложение было найдено, как можно скорее оптимизируйте его для голосового поиска. Также рассмотрите возможность разработки собственного приложения для умных колонок. Это даст вам еще один канал для создания лояльной аудитории и увеличения продаж.

2. Веб-приложения.

При создании веб-приложения производительность обычно снижается. Ограничения JavaScript делают тяжелые вычисления медленными, и это существенно влияет на взаимодействие с пользователем. Вот почему большинство популярных игр и мощных приложений доступны только в виде нативных настольных приложений.

WebAssembly здесь, чтобы изменить правила игры. Этот новый формат нацелен на производительность веб-приложений, подобную нативной. С WebAssembly код на любом языке программирования может быть скомпилирован в байт-код, который запускается в браузере.

Код WebAssembly выполняется быстрее, чем JavaScript. В результате вы можете писать критически важные для производительности части приложения на наиболее подходящем языке (C/C++/C#/Rust/Kotlin и т.д.). Затем WebAssembly позаботится о выполнении в браузере. Нативные приложения можно сразу запускать в браузере. Это означает доступ к большему количеству пользователей при сопоставимой производительности в Интернете без дополнительных затрат на разработку!

Все больше и больше популярных веб - и настольных браузеров, включая Microsoft Edge, Safari, Chrome, Opera Mobile и т. д., позволяют поднять UX до небес с помощью этого модного инструмента.

Используйте это для своего бизнеса

Веб-приложения становятся более мощными благодаря WebAssembly. Эту технологию определенно стоит попробовать, если вы планируете создать онлайн-редактор изображений или видео, веб-игру, платформу P2P , музыкальное приложение, интерактивные образовательные и обучающие приложения, приложения для 3D-карт и т. д.

3. Персонализация контента с помощью машинного обучения.

Искусственный интеллект, в том числе машинное обучение, влияет на нашу повседневную деятельность в Интернете, даже если мы этого не замечаем. В этом и заключается главный смысл машинного обучения — изначально обеспечивать улучшенный опыт.

Машинное обучение — это способность программного обеспечения повышать производительность без прямого участия разработчиков. По сути, программное обеспечение анализирует поступающие данные, выявляет закономерности, принимает решения и совершенствует свою работу.

Airbnb, например, использовала машинное обучение для настройки результатов поиска для гостей, чтобы повысить шансы хозяина принять их запрос. Алгоритм машинного обучения анализирует решения о приеме запросов каждого хоста. В зависимости от этого результаты поиска в списках, которые с большей вероятностью будут приняты, ранжируются выше. A/B-тестирование показало увеличение конверсии на 3,75%. В результате все пользователи Airbnb теперь обрабатываются в соответствии с этим алгоритмом, что повышает удовлетворенность клиентов и увеличивает доход.

Инженеры Netflix пошли еще дальше. Чтобы использовать прогнозирующий подход к персонализации контента, они используют более продвинутые алгоритмы на основе машинного обучения, чтобы лучше удовлетворять потребности пользователей. В отличие от таргетинга на весь сегмент пользователей, каждый из пользователей идентифицируется конкретно. Алгоритмы предоставляют контент и результаты поиска на основе намерений пользователей, а не предыдущих запросов.

Прекрасные примеры, но есть намного больше! Включение естественного языка и распознавания изображений может улучшить взаимодействие с пользователем. Машинное восприятие позволяет компьютеру интерпретировать данные и принимать обоснованные решения. Машинное обучение используется в веб-приложениях в различных отраслях, таких как здравоохранение, финансы, образование, сельское хозяйство и т. д. Эта технология предлагает значительные улучшения, которых было бы трудно достичь без ИИ. Машинное обучение становится важной частью любого веб-сервиса. Важно также интегрировать его в свои услуги! Проанализируйте поведение посетителей вашего веб-сайта и скорректируйте отображаемый им контент. Ваши посетители никогда не узнают, что вы используете алгоритм, но их удовлетворение приведет к увеличению вовлеченности и конверсии!

4. Безопасность данных.

Чем больше данных обрабатывает веб-приложение, тем привлекательнее оно выглядит для киберпреступников. Они стремятся испортить ваши услуги и украсть данные ваших пользователей или внутреннюю информацию компании. Это может нанести большой вред вашей репутации и дорого вам обойтись.

Безопасность вашего веб-сервиса должна стать главным приоритетом. Итак, чтобы сохранить пользовательские данные в безопасности в 2022 году, следуйте этим 4 советам:

Никогда не пренебрегайте тестированием безопасности

Тестирование безопасности может проводиться на этапе разработки и может предотвратить утечку данных. Каждое изменение в вашем веб-приложении должно быть явно протестировано.

Используйте инструменты для мониторинга веб-сайтов

Алгоритм может постоянно отслеживать все запросы, а также обнаруживать и квалифицировать подозрительную активность. Своевременное уведомление позволяет вашей команде мгновенно реагировать и защищать веб-приложение.

Тщательно выбирайте сторонние сервисы

Программное обеспечение SaaS становится все более популярным, поскольку оно упрощает и ускоряет разработку приложений. Однако вы должны убедиться, что поставщик услуг, с которым вы решили работать, заслуживает доверия.

Шифрование конфиденциальных данных

Даже если злоумышленник доберется до вашей базы данных, он не сможет извлечь какую-либо пользу из хранящихся там конфиденциальных данных.

Наряду с этими советами мы подготовили некоторые из последних веб-тенденций 2022 года, чтобы обеспечить безопасность вашего приложения и данных. Здесь необходимо выделить 2 важнейших компонента:

ИИ для кибербезопасности

Машины становятся умнее. Хотя этот факт имеет как положительные, так и отрицательные стороны, в нашем докладе мы уделим внимание преимуществам, которые он несет.

Мы ожидаем, что в 2022 году технологии ИИ станут еще более полезными с точки зрения безопасности данных. У нас уже есть возможность наблюдать за самыми последними улучшениями: биометрические входы в систему с помощью ИИ, которые сканируют отпечатки пальцев или сетчатку глаза, — это не просто элементы научной фантастики. Веб-системы многих крупных компаний демонстрируют эти функции.

80% основателей телекоммуникационных компаний говорят, что они полагаются на ИИ для обеспечения кибербезопасности.

Угрозы и вредоносные действия легче обнаружить с помощью программного обеспечения для обеспечения безопасности на базе ИИ. По мере роста разнообразия вредоносных программ они становятся сильнее и опаснее. Поэтому сейчас крупные компании обучают свои системы искусственного интеллекта анализировать модели поведения в сети и немедленно реагировать на любые подозрительные действия.

«Искусственный интеллект становится советником; как доверенный советник, которому можно задавать вопросы… искусственный интеллект будет узнавать все больше и больше; когнитивные системы начнут узнавать больше по мере того, как мы их учим, но они будут там, и они не забудут, чему их учат, чтобы вы могли использовать эти знания и помочь вам принять более точное решение, когда вы смотрите на то, что происходит в вашей жизни. С точки зрения угрозы (безопасности)», — говорит Кевин Скапинец, вице-президент IBM по безопасности, описывая, как ИИ может повлиять на систему безопасности и спасти предприятие от потенциальных угроз.

Блокчейн для кибербезопасности

В течение нескольких лет биткойн и другие темы, связанные с блокчейном, занимали первые места в технических блогах и отчетах. В 2022 году мы бы рекомендовали присмотреться к нему как к инструменту безопасности веб-решений.

NASA внедрило технологию блокчейн для защиты данных и предотвращения кибератак на свои сервисы. Это хороший момент для начала: если влиятельные лидеры используют эту тенденцию для защиты своих организаций, почему вы игнорируете этот принцип?

Безопасность базы данных

Как только вы сохраните все свои данные в одном месте, хакерам будет очень удобно их украсть. Блокчейн — это децентрализованная база данных, что означает отсутствие единого органа или места для хранения данных. Каждый пользователь несет ответственность за проверку данных, и никакие изменения не могут быть внесены, если они не одобрены всеми.

Защищенный DNS.

Крупные компании страдают от DDoS-атак. Но есть лекарство: полная децентрализация DNS. Когда контент распространяется на множество узлов, злоумышленнику становится практически невозможно найти и использовать уязвимые точки, а также атаковать ваш домен.

Вообще говоря, каждый веб-тренд 2022 года достоин вашего внимания. Некоторые из них сохранятся в течение следующего десятилетия, а некоторые станут нормой всего за несколько месяцев. Поэтому не медлите с их внедрением как можно скорее.

Продолжение следует…