



Аннотация –В этом документе представлен всесторонний анализ рынка брокеров очередей сообщений с акцентом на различные критические аспекты, влияющие на его рост и развитие. Документ предлагает высококачественную сводку текущего состояния и перспектив рынка брокеров очередей сообщений. Этот анализ особенно ценен для специалистов по безопасности и других специалистов из различных отраслей промышленности, поскольку даёт представление о безопасном и эффективном управлении распределёнными системами. Детальный анализ производительности, безопасности и технологических тенденций даёт заинтересованным сторонам знания, необходимые для принятия обоснованных решений и расширения их операционных возможностей.

I. ВВЕДЕНИЕ

Брокеры сообщений являются важными компонентами современных распределённых систем, обеспечивающими бесперебойную связь между приложениями, службами и устройствами. Они действуют как посредники, которые проверяют, хранят, маршрутизируют и доставляют сообщения, обеспечивая надёжный и эффективный обмен данными между различными платформами и языками программирования. Эта функциональность имеет решающее значение для поддержания разделения процессов и служб, что повышает масштабируемость системы, производительность и отказоустойчивость. Брокеры сообщений поддерживают различные схемы обмена сообщениями, включая двухточечную передачу и публикацию / подписку, что позволяет использовать их в различных вариантах использования, таких как финансовые транзакции, уведомления в режиме реального времени и потоковая передача данных Интернета вещей.

Рынок брокеров сообщений переживает значительный рост, обусловленный растущим внедрением облачных решений и потребностью в надёжных, масштабируемых коммуникационных инфраструктурах в распределённых системах. Основными игроками на этом рынке являются

RabbitMQ, Apache Kafka, IBM MQ, Microsoft Azure Service Bus и Google Cloud IoT, каждый из которых предлагает уникальные возможности и обслуживает широкий спектр отраслей - от финансовых услуг до здравоохранения и "умных городов". Эти брокеры работают по всему миру, имея значительную базу клиентов в таких регионах, как Северная Америка, Европа и Азиатско-Тихоокеанский регион, что отражает их решающую роль в создании современных взаимосвязанных приложений.

В следующих главах приводится краткое описание обзора уязвимостей в главе III и анализ охвата рынка в главах IV в т.ч. сводный анализ в главе II.

II. СВОДНЫЕ ДАННЫЕ

- **Доля рынка:** процент рынка, который занимает каждый брокер в категории очередей, обмена сообщениями и фоновой обработки.
- **Количество клиентов:** общее количество компаний или устройств, использующих брокера.
- **Корпоративные клиенты:** количество корпоративных клиентов, использующих брокера.
- **Распределение доходов:** распределение компаний, использующих брокера, на основе их доходов.
- **Географический охват:** процент клиентов, проживающих в разных регионах.

Рыночная доля брокера и клиентская база

Брокер	Доля рынка (%)	Клиенты / корп. клиенты
RabbitMQ	28.24	15,851 / 14,651
Apache Kafka	39.73	22,244 / 22,244
Apache ActiveMQ	5.79	9,604 / 9,604
IBM MQ	7.12	4,060 / 4,060
Microsoft Azure Service Bus	3.84	12,870 / 4,609
EMQX	н/д	20,000+ / 500+
HiveMQ	н/д	20,000+ / 500+
PubNub	н/д	н/д / 500+
ThingsBoard	н/д	1000+ / 500+
AWS IoT	н/д	718 / 718
Azure IoT	14.90	1,396 / 1,396
Google Cloud IoT	18.65	1,790 / 1,790
Cisco IoT	9.52%	129
Solace	5.33%	133
Amazon Kinesis	1.20%	216

Доход брокера и географический охват

Брокер	Клиенты	Клиенты / выручка	Гео-покрытие
RabbitMQ	Currys, Beckman Coulter	< \$50M: 39%, \$50M-\$1B: 16%, > \$1B: 40%	US: 46.15%, India: 9.72%, UK: 9.70%
Apache Kafka	LinkedIn, Uber, Netflix	< \$50M: 52%, \$50M-\$1B: 18%, > \$1B: 24%	US: 51.91%, India: 12.95%, UK: 8.28%

Apache Active MQ	Infosys, Fujitsu, Panasonic	< \$50M: 24%, \$50M-\$1B: 43%, > \$1B: 33%	US: 47%, UK: 6%, India: 6%
IBM MQ	American Airlines, Aflac	< \$50M: 39%, \$50M-\$1B: 16%, > \$1B: 40%	US: 59.39%, UK: 8.70%, India: 8.67%
Microsoft Azure Service Bus	Infosys, Fujitsu, Panasonic	< \$50M: 40%, \$50M-\$1B: 17%, > \$1B: 39%	US: 48.02%, UK: 14.97%, India: 8.98%
EMQX	IoT sector companies	N/A	50+ countries
HiveMQ	Fortune 500 companies	N/A	US: 60%
PubNub	US companies	N/A	Global
Things Board	IoT sector companies	N/A	50+ countries
AWS IoT	Global companies	N/A	US: 52.12%, India: 13.26%, UK: 8.84%
Azure IoT	Global companies	N/A	US: 47.72%, India: 14.04%, UK: 8.73%
Google Cloud IoT	Global companies	N/A	US: 48.77%, India: 16.58%, Germany: 6.39%
Cisco IoT	Infosys, Cisco Systems, Wipro, AT&T, Cognizant	< \$50M: 25%, \$50M-\$1B: 17%, > \$1B: 47%	US: 50%, India: 9%
Solace	Large enterprises in finance, telecom, manufacturing	< \$50M: 16%, \$50M-\$1B: 29%, > \$1B: 49%	US: 38.18%, France: 10.91%, Canada: 10%
Amazon Kinesis	Siemens, Microsoft, Oracle, Cisco	< \$50M: 25%, \$50M-\$1B: 15%, > \$1B: 60%	US: 61.78%, India: 10.47%, UK: 8.38%

III. Уязвимости брокеров

A. RabbitMQ

- **Windows-Specific Binary Planting:** в RabbitMQ версий 3.8.x до версии 3.8.7 подвержен уязвимости при установке бинарных файлов для Windows, которая допускает выполнение произвольного кода. Злоумышленник, имеющий права на запись в установочный каталог RabbitMQ и локальный доступ в Windows, может осуществить локальную атаку planting и выполнить произвольный код.
- **Denial of Service (DoS) via "X-Reason" HTTP Header:** RabbitMQ версий 3.7.x до версии 3.7.21 и 3.8.x до версии 3.8.1 содержат плагин веб-управления, уязвимый для DoS атаки может быть использован для вставки вредоносной строки формата Erlang, которая будет расширяться и занимать кучу данных, что приведёт к сбою сервера.
- **XSS:** несколько форм в пользовательском интерфейсе управления RabbitMQ уязвимы для XSS-атак. Сюда входят версии до версии v3.7.18 и

RabbitMQ для PCF версий 1.15.x до версии 1.15.13, 1.16.x до версии 1.16.6 и 1.17.x до версии 1.17.3.

- **Обход аутентификации MQTT:** В RabbitMQ 3.x до версии 3.5.8 и 3.6.x до версии 3.6.6 была обнаружена ошибка, при которой аутентификация соединения MQTT с использованием пары имя пользователя / пароль завершается успешно, если указано существующее имя пользователя, но пароль не использовался в запросе на подключение.
- **Раскрытие конфиденциальной информации:** Компонент сбора показателей в RabbitMQ для Pivotal Cloud Foundry (PCF) версии 1.6.x до версии 1.6.4 регистрирует строки с неудачными командами, что позволяет получать конфиденциальную информацию путём чтения данных журнала.
- **Отказ в обслуживании через конечную точку клиентского подключения AMQP:** RabbitMQ до версии 3.8.16 подвержен DoS из-за неправильной проверки входных данных в конечной точке клиентского подключения AMQP 1.0.
- **Обход аутентификации TLS / DTLS (CVE-2022-37026):** уязвимость возникает из-за ошибки в Erlang OTP и позволяет обойти процесс аутентификации и выдать себя за других клиентов, если сервер настроен на аутентификацию TLS или DTLS.

B. Apache Kafka

- **Отказ в обслуживании:** ошибка в InternalTopicManager до 2.1.0 может привести к DoS-атаке. Когда тема помечена для удаления, но ещё не удалена, Брокер выдаёт «противоречивую информацию», в результате чего клиент вводит цикл опроса метаданных темы, что приводит к DoS.
- **Уязвимость Timing Attack (CVE-2021-38153):** некоторые компоненты в Apache Kafka с 2.0.0 по 2.8.0 используют Arrays.equals для проверки пароля или ключа, которые уязвимы для временных атак, что повышает вероятность успеха атак методом перебора.
- **Plaintext Secrets Exposure (CVE-2019-12399):** В Kafka с 2.0.0 по 2.3.0 API REST Connect REST API может раскрывать защищённых данных в конечной точке задач при настройке с помощью одного или нескольких поставщиков конфигурации.
- **Out-of-Memory (OOM) via Snappy Compression (CVE-2023-34455):** уязвимость в библиотеке snappy-java, используемой Kafka 0.8.0 - 3.5.0 может вызвать нехватку памяти (OOM), приводящую к DoS-атаке, когда вредоносная нагрузка, сжатая с помощью snappy-java, распаковывается Kafka.
- **Удалённое выполнение кода (RCE) CVE-2023-25194:** небезопасная десериализация в Kafka Connect с 2.3.0 по 3.3.2 REST API может позволить злоумышленнику с удалённой аутентификацией выполнить произвольный код или вызвать DoS.

- **Отказ в обслуживании из-за неправильной проверки входных данных (CVE-2022-34917):** неправильная проверка входных данных может позволить удалённо выделить большие объёмы памяти посредникам, что приведёт к DoS.
- **Уязвимость десериализации Java (CVE-2023-34040):** Атака на десериализацию Spring для Apache Kafka 3.0.9 и более ранних версий, 2.9.10 и более ранних версий используется, если применяется необычная конфигурация, позволяющая создать вредоносный сериализованный объект.

C. ApacheMQ

- **CVE-2023-46604: удалённое выполнение кода (RCE):** удалённое выполнение произвольных команд, используя сериализованные типы классов в протоколе OpenWire. Проблема возникает из-за неспособности должным образом проверить типы классов, которые можно использовать, когда команды OpenWire отменены. Версии: Apache ActiveMQ 5.18.x до версии 5.18.3, Apache ActiveMQ 5.17.x до версии 5.17.6, Apache ActiveMQ 5.16.x до версии 5.16.7, Все версии до версии 5.15.16
- **CVE-2022-41678: уязвимость десериализации:** уязвимость позволяет прошедшим проверку подлинности пользователям выполнять RCE, используя десериализацию данных.
- **CVE-2020-13947: XSS:** уязвимости XSS в WebConsole позволяют удалённо внедрить произвольные веб-скрипты или HTML.
- **CVE-2020-13920: уязвимость JMX MITM:** уязвимость типа MITM в JMX позволяет удалённо перехватывать сообщения и манипулировать ими.
- **CVE-2016-3088: удалённая загрузка и выполнение файлов:** Веб-приложение файлового сервера в Apache ActiveMQ позволяет удалённо загружать и выполнять произвольные файлы через HTTP PUT с последующим HTTP MOVE.
- **CVE-2015-1830: Обход пути, ведущий к RCE:** уязвимость обхода пути в функциональности загрузки на файловый сервер позволяет удалённо создавать файлы JSP в произвольных каталогах, что приводит к удалённому выполнению кода.
- **CVE-2014-3576: удалённое завершение работы брокера без проверки подлинности (DoS):** позволяет удалённо завершать работу брокера без проверки подлинности, что приводит к DoS.

D. IBM MQ

- **CVE-2022-27780 и CVE-2022-30115:** уязвимости находятся в библиотеке libcurl, используемой IBM MQ 9.2 LTS, 9.1 LTS, 9.0 LTS, 9.2 CD и 9.1 CD. CVE-2022-27780 позволяет обойти ограничения безопасности, используя специально созданное имя хоста в URL. CVE-2022-30115 – это ошибка обхода проверки HSTS, которая может быть использована

для получения конфиденциальной информации по протоколу HTTP в открытом виде.

- **CVE-2023-26285: Отказ в обслуживании (DoS):** IBM MQ 8.0, 9.0-9.1 LTS, 9.2 LTS, 9.3 LTS, 9.1 CD, 9.2 CD и 9.3 CD. уязвим для DoS-атаки, вызванной ошибкой обработки недействительных данных от скомпрометированного клиента.
- **CVE-2022-43902: Отказ в обслуживании (DoS) с помощью PCF или MQSC:** Прошедший проверку подлинности злоумышленник с достаточными разрешениями MQ может отправлять специально созданные сообщения PCF или MQSC для выполнения DoS-атаки. Версии: IBM MQ 9.1-9.3 LTS, 9.1-9.3 CD.
- **CVE-2023-45177: Отказ в обслуживании (DoS) с помощью логики кластеризации MQ:** IBM MQ Appliance 9.2 LTS, 9.3 LTS и 9.3 CD. уязвим для DoS-атаки из-за ошибки в логике кластеризации MQ.
- **CVE-2022-21624 и CVE-2022-21626: уязвимости среды выполнения Java:** Множественные уязвимости в IBM Runtime Environment Java Technology Edition версии 8, которая поставляется вместе с IBM MQ. CVE-2022-21624 позволяет не прошедшему проверку подлинности, обновлять, вставлять или удалять данные. CVE-2022-21626 позволяет не прошедшему проверку подлинности, вызвать DoS. Версии: IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS, 9.1 CD, 9.2 CD и 9.3 CD.
- **CVE-2023-22081 и CVE-2023-5676: уязвимости Java SE и Eclipse OpenJ9:** CVE-2023-22081 – это уязвимость в Java SE, связанная с компонентом JSSE, позволяющая удалённо влиять на доступность. CVE-2023-5676 в Eclipse OpenJ9 может вызвать бесконечное зависание из-за ошибки сегментации при получении сигнала выключения перед инициализацией JVM. Версии: IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS и 9.3 CD.
- **CVE-2020-13947: XSS:** уязвимости XSS в WebConsole позволяют удалённо внедрить произвольные веб-скрипты или HTML.
- **CVE-2020-13920: уязвимость JMX MITM:** уязвимость MITM в JMX позволяет удалённо перехватывать сообщения и манипулировать ими.
- **CVE-2016-3088: удалённая загрузка и выполнение файлов:** Веб-приложение файлового сервера в Apache ActiveMQ позволяет удалённо загружать и выполнять произвольные файлы через HTTP PUT с последующим HTTP-MOVE.
- **CVE-2015-1830: Обход пути, ведущий к RCE:** уязвимость обхода пути в функциональности загрузки на файловый сервер позволяет удалённо создавать файлы JSP в произвольных каталогах, что приводит к удалённому выполнению кода.

- **CVE-2014-3576: удалённое завершение работы брокера без проверки подлинности (DoS):** позволяет удалённо завершать работу брокера без проверки подлинности, что приводит к DoS.

E. Microsoft Azure Service Bus

- **Уязвимость, связанная с отказом в обслуживании (DoS) (MS14-042):** уязвимость в Microsoft Service Bus для Windows Server может позволить злоумышленнику с удалённой аутентификацией создать и запустить специально созданный сценарий, что приведёт к DoS.
- **DoS через исчерпание ресурсов:** Azure может стать недоступной во время DoS-атак, направленных на перегрузку её ресурсов или нарушение её работы. Это может произойти из-за проблем с сетью, перебоев в обслуживании, исчерпания ресурсов, ошибок конфигурации, проблем безопасности, программных ошибок или сбоев в работе центра обработки данных.
- **Удалённое выполнение кода (RCE) в коннекторах Power Platform:** уязвимость RCE позволяет получать доступ к данным между клиентами. Эта проблема была исправлена путём применения строгих списков разрешений типов.
- **Шифрование данных и риски безопасности:** хотя Azure поддерживает шифрование при передаче и в хранении, существуют риски, связанные с удалением данных, несанкционированным перемещением данных и несанкционированным доступом.

F. EMQX

- **CVE-2021-33175: Отказ в обслуживании (DoS):** уязвимость в версиях EMQX до версии 4.2.8 допускает атаку типа "отказ в обслуживании" (DoS) из-за чрезмерного потребления памяти при обработке «искажённых» сообщений MQTT.
- **CVE-2023-46604: Обход каталогов:** уязвимость для обхода каталогов в плагине emqx_sn в EMQX версии 4.3.8 позволяет выполнять обход каталогов путём загрузки созданного файла .txt.
- **Уязвимости, связанные с переполнением буфера кучи:** В NanoMQ 0.21.7, компоненте EMQX, существует множество уязвимостей, связанных с переполнением буфера кучи, которые могут быть использованы для вызова отказа в обслуживании через специально созданные hex-потoki.
- **Уязвимость "Use-After-Free":** уязвимость в NanoMQ версии 0.21.2 вызывает отказ в обслуживании с помощью спец сообщений MQTT.
- **Разыменованние нулевого указателя:** уязвимость разыменованния Null-указателя в функции topic_filtern в mqtt_parser.c в NanoMQ 0.21.7 позволяет вызывать отказ в обслуживании.

- **Перечисление имени пользователя:** на EMQX Dashboard версии v3.0.0 влияет уязвимость перечисления имени пользователя в интерфейсе "/api/ v3/auth", позволяющая определить, является ли данное имя пользователя действительным.

- **Отказ в обслуживании из-за потребления памяти:** Версии EMQX Broker до версии 4.2.8 уязвимы для атаки типа "отказ в обслуживании" из-за чрезмерного потребления памяти при обработке ненадёжных входных данных.
- **Уязвимость TLS:** уязвимость, связанная с повторным согласованием сеанса протокола TLS на порту 8084 (TCP через SSL).

G. HiveMQ

- **CVE-2020-13821: Reflected XSS:** уязвимость в Центре управления брокером HiveMQ (версия 4.3.2) допускает использование Reflected XSS. Это может быть использовано для выполнения произвольных веб-скриптов или HTML-кода в контексте браузера пользователя.
- **Отказ в обслуживании (DoS) из-за исчерпания ресурсов:** HiveMQ уязвим для DoS-атак, целью которых является исчерпание ресурсов брокера, таких как диск, оперативная память или центральный процессор, если отправлять много тяжёлых сообщений или использует обработку очереди сообщений брокером.
- **Атака SlowITe:** атака SlowITe использует параметр Keep-Alive протокола MQTT, позволяющий установить произвольное значение, которое сохраняет соединение открытым в течение длительного периода, что приводит к DoS.
- **Переполнение буфера на основе кучи:** уязвимость в брокере HiveMQ может быть использована для вызова отказа в обслуживании (DoS) или потенциального выполнения произвольного кода.

H. Pubhub

- **CVE-2023-26154: недостаточная энтропия:** уязвимость в пакете PubNub (версии до 6.19) связана с недостаточной энтропией при генерации криптографических ключей, что может быть использовано для принудительного шифрования.
- **Reflected XSS:** уязвимость в платформе позволяет проводить Reflected XSS-атаки для выполнения произвольных веб-скриптов или HTML-кода в контексте браузера пользователя.
- **Уязвимость при постоянном подключении:** существуют опасения по поводу безопасности постоянных подключений PubNub через порт 80 или порт 443.
- **Уязвимости в системе безопасности в Insteon Hub:** В Insteon Hub, использующем для связи

PubNub, было обнаружено множество уязвимостей. Эти уязвимости варьируются от RCE до DoS-атак.

- **Уязвимости в пользовательских реализациях:** Пользовательские реализации PubNub, особенно те, которые используют более старые версии или небезопасную конфигурацию, могут быть уязвимы для различных атак, включая MITM и эксфильтрацию данных.

I. Thingsboard

- **CVE-2022-45608: Вертикальное повышение привилегий:** уязвимость ThingsBoard версии 3.4.2 позволяет пользователю с низкими привилегиями (CUSTOMER_USER) повысить свои привилегии и стать администратором (TENANT_ADMIN) или системным администратором (SYS_ADMIN) с помощью простого POST-запроса с помощью REST API платформы.
- **CVE-2023-26462: небезопасное управление секретными ключами:** уязвимость позволяет повышать привилегии в системе путём манипулирования веб-токенами JSON (JWT). Статический секретный ключ по умолчанию, используемый для подписи JWT, может быть использован для повторной подписи изменённых токенов, предоставляя несанкционированный доступ. Версии: до версии 3.4.2.
- **CVE-2021-42751: хранимый XSS:** уязвимость хранимых XSS в ThingsBoard версии 3.3.1 позволяет выполнять произвольный код JavaScript путём введения полезной нагрузки скрипта в поле описания узла правил.
- **CVE-2023-45303: Внедрение шаблона на стороне сервера:** ThingsBoard до версии 3.5 уязвим для внедрения шаблона на стороне сервера, если пользователям разрешено изменять шаблон электронной почты. Эта уязвимость может быть использована для выполнения произвольного кода на сервере.
- **CVE-2020-27687: Внедрение заголовка хоста:** Продукт до версии 3.2 уязвим для внедрения заголовка хоста в электронные письма со сброшенным паролем. Это позволяет отправлять вредоносные ссылки в электронных письмах для сброса пароля.
- **CVE-2023-26462: Статический ключ по умолчанию:** использование статического ключа по умолчанию для подписи JWT в ThingsBoard позволяет подделывать действительные запросы и повышать привилегии до версии 3.4.2.

J. Solace

- **Уязвимости ядра:** В устройствах и ПО Solace PubSub+ Event Broker, выпущенных до версии 9.10.0, было выявлено и устранено множество уязвимостей ядра. Эти уязвимости включают

проблемы, которые могут привести к отказу в обслуживании (DoS), повышению привилегий и другим рискам безопасности. Идентификаторы CVE: CVE-2021-26930, CVE-2021-26931, CVE-2021-26932, CVE-2021-27363, CVE-2021-27364, CVE-2021-27365, CVE-2021-28038, CVE-2021-30002, CVE-2019-19060, CVE-2021-28660, CVE-2021-29265, CVE-2021-28964, CVE-2021-28971, CVE-2021-28972, CVE-2021-28688, CVE-2021-29647, CVE-2021-3483, CVE-2021-29154, CVE-2020-25670, CVE-2020-25671, CVE-2020-25672

- **Уязвимости Amazon Linux 2:** Устранено несколько критических уязвимостей в Amazon Linux 2, включая проблемы в systemd и ядре. Эти уязвимости могут привести к удалённому выполнению кода (RCE), отказу в обслуживании (DoS) и другим рискам безопасности. Идентификаторы CVE: CVE-2018-15686, CVE-2018-16864, CVE-2018-16866, CVE-2018-16888, CVE-2019-20386, CVE-2019-3815, CVE-2019-6454, CVE-2021-33200
- **Уязвимости Apache Log4j:** Log4Shell позволяют выполнять удалённый код (RCE) и затрагивают многие системы, использующие Log4j для ведения журнала. CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832, CVE-2022-23305
- **Уязвимости Spring Framework:** Множественные уязвимости в Spring Framework и Spring Cloud могут привести к удалённому выполнению кода (RCE) и другим рискам безопасности.
- **Уязвимость OpenSSL:** Критическая уязвимость в OpenSSL может привести к угрозам безопасности, таким как атаки "человек посередине" (MITM).
- **Уязвимость XZ Utils:** уязвимость в XZ Utils, но установлено, что продукты Solace не затронуты.

K. AWS IoT

- **Отказ в обслуживании (DoS) из-за исчерпания ресурсов:** AWS IoT может быть уязвим для DoS-атак, целью которых является исчерпание ресурсов брокера, таких как диск, оперативная память или центральный процессор. Это происходит, если злоумышленник отправляет много тяжёлых сообщений или использует обработку очередей сообщений брокером.
- **Межсайтовый скриптинг (XSS):** уязвимости XSS в платформе AWS IoT могут позволить злоумышленникам внедрять вредоносные скрипты в контекст браузера пользователя, что потенциально может привести к краже данных или дальнейшему использованию.
- **Внедрение заголовка хоста:** AWS IoT до версии 3.2 уязвима для внедрения заголовка хоста в электронных письмах со сброшенным паролем. Это позволяет злоумышленнику отправлять вредоносные ссылки в электронных письмах для сброса пароля. CVE-2020-27687

L. AWS IoT

- **Отказ в обслуживании (DoS) из-за исчерпания ресурсов:** AWS IoT может быть уязвим для DoS-атак, направленных на исчерпание ресурсов брокера, таких как диск, оперативная память или центральный процессор. Это происходит, если злоумышленник отправляет много тяжёлых сообщений или использует обработку очередей сообщений брокером.
- **XSS:** уязвимости XSS позволяют внедрять вредоносные скрипты в контекст браузера пользователя, что потенциально может привести к краже данных или дальнейшему использованию.
- **Внедрение заголовка хоста:** AWS IoT до версии 3.2 уязвима для внедрения заголовка хоста с вредоносными ссылками в электронных письмах со сброшенным паролем. CVE-2020-27687

M. Azure IoT

- **CVE-2024-27099: удалённое выполнение кода (RCE) в библиотеке C uAMQP:** уязвимость в библиотеке C uAMQP, используемой Azure IoT для взаимодействия с облачными сервисами Azure. Уязвимость, вызванная ошибкой "двойного освобождения" памяти, может привести к RCE
- **CVE-2021-42312, CVE-2021-37222, CVE-2021-42313, CVE-2021-42311:** Множественные критические уязвимости в Azure Defender для интернета вещей: Множественные уязвимости в Azure Defender для интернета вещей, включая проблемы с механизмом сброса пароля и уязвимости SQL-инъекций, позволяют злоумышленникам, не прошедшим проверку подлинности, получить несанкционированный доступ и, возможно, RCE.
- **CVE-2019-0741: раскрытие информации в Azure IoT Java SDK:** уязвимость раскрытия информации в Azure IoT Java SDK регистрирует конфиденциальную информацию, которая может быть использована для получения доступа к конфиденциальным данным.
- **Внедрение заголовка узла:** Azure IoT до версии 3.2 уязвим для внедрения заголовка узла в электронные письма со сброшенным паролем. Это позволяет отправлять вредоносные ссылки в электронных письмах для сброса пароля. CVE-2020-27687
- **Небезопасное управление секретными ключами:** уязвимость, связанная с небезопасным управлением секретными ключами, позволяет повышать привилегии в системе путём манипулирования веб-токенами JSON (JWT). Статический секретный ключ по умолчанию, используемый для подписи JWT, может быть использован для повторной подписи изменённых токенов, предоставляя несанкционированный доступ. CVE-2023-26462

N. Google Cloud IoT

- **Проблемы со слабыми паролями и аутентификацией:** значительная часть атак на экземпляры облачной платформы Google (GCP), включая развёртывания Интернета вещей, происходят из-за слабых паролей или их отсутствия вообще. В 48% проанализированных случаев основной причиной успешных атак были слабые или отсутствующие пароли.
- **Уязвимости в программном обеспечении облачного сервера:** В 26% случаев злоумышленники использовали уязвимости в ПО облачного сервера. Эти уязвимости могут привести к несанкционированному доступу к устройствам Интернета вещей и данным и контролю над ними.
- **Неправильная конфигурация сервера или приложения:** неправильная конфигурация серверов или приложений стала причиной 12% успешных атак, которые могут подвергнуть конфиденциальные данные и службы несанкционированному доступу.
- **Утечки пароля или ключа доступа:** В 4% случаев утечка пароля или ключа доступа была причиной успешных атак из-за загрузки данных аутентификации в общедоступные репозитории, такие как GitHub.
- **CVE-2023-44487: DDoS-уязвимость быстрого сброса HTTP / 2:** уязвимость высокой степени серьёзности в протоколе HTTP / 2, известная как метод "быстрого сброса", может быть использована для запуска крупномасштабных DDoS-атак. Эта уязвимость затрагивает веб-приложения, службы и API, использующие HTTP/2.
- **CVE-2023-52620: Повышение привилегий в ядре Linux:** уязвимость в ядре Linux приводит к повышению привилегий на узлах OS, оптимизированных для контейнеров, и Ubuntu. Эта уязвимость может быть использована для получения несанкционированного доступа и контроля над системой.
- **CVE-2023-5736: уязвимость для выхода из контейнера:** уязвимость в среде выполнения контейнера runc, используемой Docker и Kubernetes, позволяет выйти из контейнера и выполнить код в хост-системе.
- **Уязвимость GhostToken:** уязвимость в облачной платформе Google (GCP) позволяла изменять и скрывать приложения OAuth, создавая скрытый бэкдор для любой учётной записи Google. Эта уязвимость, называемая GhostToken, может быть использована для извлечения токенов учётной записи и доступа к данным жертвы.

O. Kinesis IoT

- **XSS:** XSS в платформе AWS IoT позволяют злоумышленникам внедрять вредоносные скрипты в контекст браузера пользователя, что потенциально может привести к краже данных или дальнейшему использованию.
- **Отказ в обслуживании (DoS) из-за исчерпания ресурсов:** AWS Kinesis может быть уязвим для DoS-атак, целью которых является исчерпание ресурсов брокера, таких как диск, оперативная память или центральный процессор. Это может произойти, если злоумышленник отправляет много тяжелых сообщений или использует обработку очередей сообщений брокером.
- **Внедрение заголовка хоста:** AWS IoT до версии 3.2 уязвима для внедрения заголовка хоста в электронных письмах со сброшенным паролем. Это позволяет отправлять вредоносные ссылки в электронных письмах для сброса пароля. CVE-2020-27687

P. Cisco IoT

- **-2022-20773: XSS в Центре управления Cisco IoT:** Уязвимость в веб-интерфейсе управления Cisco IoT Control Center может позволить удалённому злоумышленнику, не прошедшему проверку подлинности, провести атаку с использованием XSS против пользователя интерфейса. Эта уязвимость существует из-за того, что веб-интерфейс управления не проверяет должным образом вводимые пользователем данные.
- **CVE-2023-20198: Повышение привилегий в Cisco IOS XE:** критический недостаток в веб-интерфейсе IOS XE может быть использован удалёнными злоумышленниками, не прошедшими проверку подлинности, для повышения привилегий. Эта уязвимость позволяет субъектам угрозы создавать учётные записи с высокими привилегиями на целевых устройствах и получать полный контроль над системой.
- **CVE-2023-31242 и CVE-2023-34998: обход аутентификации на платформе OAS:** уязвимости OAS предшествующей версии 19.00.0000, которая используется в промышленных IoT-средах, использованы для обхода аутентификации, утечки конфиденциальной информации и перезаписи файлов и позволяют получить несанкционированный доступ и контроль над системой.
- **CVE-2023-34317: Неправильная проверка ввода в платформе OAS:** Ошибка неправильной проверки ввода в функциональности создания клиентов платформы OAS предыдущей версии 19.00.0000 позволяет злоумышленникам добавлять пользователя с полем имени пользователя, содержащим SSH-ключ, потенциально получая доступ к базовой системе.

- **CVE-2023-34353: Раскрытие информации на платформе OAS:** Уязвимость OAS предшествующей версии 19.00.0000 позволяет злоумышленнику выполнять прослушивание сети для захвата protobuf, содержащего учётные данные администратора, и затем расшифровывать конфиденциальную информацию.
- **CVE-2020-7592: Нарушение целостности данных в устройствах Siemens:** Уязвимость, затрагивающая различные устройства и компоненты Siemens, при которой целостность данных может быть нарушена.

IV. РЫНОК MQ-БРОКЕРОВ

A. RabbitMQ

RabbitMQ - надёжный и широко распространённый брокер обмена сообщениями, занимающий значительную долю рынка организации очередей, обмена сообщениями и фоновой обработки. Им пользуются тысячи компаний по всему миру, включая такие крупные корпорации, как Alcatel-Lucent, Калифорнийский университет в Сан-Диего и Beckman Coulter. Масштабируемость, высокая доступность и надёжная производительность RabbitMQ делают его предпочтительным выбором для различных отраслей, особенно в сфере финансовых услуг, здравоохранения, электронной коммерции, телекоммуникаций и производства. Конкурентный ландшафт включает в себя других крупных игроков, таких как Apache Kafka, IBM MQ и Apache ActiveMQ, но обширный набор функций RabbitMQ и проверенная производительность обеспечивают ему прочные позиции на рынке.

1) Занимаемая доля рынка и географическое распространение

- RabbitMQ занимает значительную долю рынка организации очередей, обмена сообщениями и фоновой обработки - примерно 28,24%.
- **Глобальное присутствие:** RabbitMQ используется в 93 странах мира.
- **США:** 46,15% клиентов RabbitMQ находятся в США.
- **Индия:** 9,72% клиентов RabbitMQ находятся в Индии.
- **Великобритания:** 9,70% клиентов RabbitMQ находятся в Великобритании.

2) Факторы роста

- **Управление ресурсами:** Возможность RabbitMQ эффективно управлять ресурсами, такими как память и центральный процессор, обеспечивает высокую производительность и надёжность, что способствует его внедрению в различных отраслях промышленности.
- **Расширенная маршрутизация:** RabbitMQ поддерживает сложные механизмы маршрутизации, что делает его подходящим для различных

сценариев обмена сообщениями, что повышает его привлекательность на рынке.

- **Мониторинг и показатели:** Комплексные возможности мониторинга помогают поддерживать работоспособность и производительность системы, что крайне важно для корпоративных приложений.
- 3) *Количество клиентов*
- **Всего компаний:** более 35 000 компаний используют RabbitMQ по всему миру.
 - **Кластеры:** По всему миру работает около 9000 кластеров RabbitMQ.
 - **Подключённые устройства:** RabbitMQ соединяет миллионы устройств Интернета вещей, демонстрируя возможность справляться с крупномасштабными развёртываниями.
- 4) *Известные Корпоративные Клиенты*
- **Alcatel-Lucent:** использует RabbitMQ для различных целей обмена сообщениями.
 - **Калифорнийский университет в Сан-Диего:** внедряет RabbitMQ в свои системы.
 - **Beckman Coulter:** использует RabbitMQ для своих операций.
 - **Zalando, WeWork, Wunderlist, Bloomberg:** Эти компании полагаются на RabbitMQ в своих микросервисных архитектурах.
 - **Capital One, Ford, State Farm, United Airlines, Zurich Insurance:** Крупнейшие корпорации используют для безопасного обмена сообщениями.
- 5) *Распределение клиентов по размеру компании*
- **20-49 сотрудников:** 3520 компаний.
 - **100-249 сотрудников:** 3034 компании.
 - **1,000-4,999 сотрудников:** 1,723 компании.
 - **Среднее количество очередей:** 26 (наибольшее количество очередей: 124 400).
 - **Среднее количество клиентов:** 2 (наибольшее количество клиентов: 62 245).
 - **Среднее количество полисов:** 3 (наибольшее количество полисов: 2550).
 - **Среднее количество обменов:** 9 (наибольшее количество обменов: 191 465).
 - **Среднее количество привязок:** 28 (наибольшее количество привязок: 142 516).
 - **Среднее количество хостингов:** 2 (наибольшее количество хостингов: 1954).
- 6) *Масштабируемость*
- **Масштабируемость:** RabbitMQ поддерживает кластеризацию, высокую доступность и балансировку нагрузки, что делает его

масштабируемым для различных корпоративных нужд.

- **Высокая пропускная способность:** RabbitMQ может обрабатывать более 1 миллиарда сообщений в день в зависимости от конфигурации.
 - **Согласованное хеширование:** RabbitMQ можно эффективно масштабировать с помощью согласованного хеширования, которое равномерно распределяет нагрузку по нескольким узлам, обеспечивая оптимальную производительность и устойчивость.
- 7) *Отраслевое применение*
- **Финансовые услуги:** RabbitMQ широко используется в финансовом секторе для безопасного обмена сообщениями.
 - **Здравоохранение:** используется ведущими медицинскими компаниями для интеграции данных и обмена сообщениями.
 - **Электронная коммерция:** Такие компании, как Zalando и WeWork, используют RabbitMQ для обработки заказов, отслеживания и выполнения.
 - **Телекоммуникации:** работает в крупных телекоммуникационных компаниях для интеграции данных и обработки в режиме реального времени.
 - **Производство:** используется крупными производственными компаниями для потоковой передачи данных и аналитики.
- 8) *Конкурентный Ландшафт*
- **RabbitMQ и Apache Kafka:** Kafka занимает большую долю рынка и предпочтителен для приложений с высокой пропускной способностью и низкой задержкой, в то время как RabbitMQ часто используется для традиционных систем обмена сообщениями с мощной поддержкой транзакций.
 - **RabbitMQ и IBM MQ:** IBM MQ предпочитают за его надёжность и однократную доставку сообщений, в то время как RabbitMQ выбирают за его гибкость и простоту использования.
 - **RabbitMQ и Apache ActiveMQ:** ActiveMQ - ещё один конкурент с меньшей долей рынка, используемый для упрощения обмена сообщениями по сравнению с возможностями RabbitMQ корпоративного уровня.

В. Apache Kafka

Apache Kafka – ведущий брокер сообщений и платформа потоковой обработки с доминирующей долей рынка и широким внедрением в различных отраслях. Он используется тысячами компаний, включая более 80% компаний из списка Fortune 100, для обработки данных в режиме реального времени, аналитики и интеграции. Масштабируемость, высокая пропускная способность и надёжная архитектура Kafka делают её предпочтительным выбором для крупномасштабных приложений потоковой

передачи данных. Конкурентный ландшафт включает в себя другие MQ-системы, такие как RabbitMQ, Apache Pulsar и IBM MQ, но обширная экосистема Kafka и проверенная производительность дают ей значительное преимущество.

1) Занимаемая доля рынка и географическое распространение

- Apache Kafka занимает доминирующую долю рынка в 70% на рынке брокеров сообщений и потоковой обработки.
- **США:** 51,91% клиентов Apache Kafka.
- **Индия:** 12,95% клиентов Apache Kafka.
- **Великобритания:** 8,28% клиентов Apache Kafka.

2) Факторы роста

- **Высокая пропускная способность и низкая задержка:** Возможность Kafka обрабатывать высокую пропускную способность с низкой задержкой делает его идеальным для потоковой передачи данных в реальное время и аналитики, что повышает его популярность среди крупных предприятий.
- **Масштабируемость:** распределённая архитектура позволяет масштабироваться горизонтально, эффективно обрабатывая большие объёмы данных, что является важным фактором роста.
- **Интеграция с экосистемой:** Обширная экосистема Kafka, включая встроенную потоковую обработку и интеграцию с различными источниками и приёмниками данных, повышает её полезность и доступность

3) Количество клиентов

- **Всего компаний:** более 22240 компаний используют Apache Kafka по всему миру.
- **Fortune 100:** более 80% компаний из списка Fortune 100 используют Kafka.

4) Известные Корпоративные Клиенты

- **American Express:** использует Kafka для обработки данных в режиме реального времени.
- **Cardinal Health:** реализует Kafka для обработки крупномасштабных потоков данных.
- **Cisco:** использует Kafka для своих нужд в интеграции данных.
- **Shopify:** использует Kafka для потоковой обработки и анализа данных.
- **LinkedIn:** ежедневно обрабатывает 7 триллионов сообщений с помощью Kafka.
- **Uber:** одно из крупнейших внедрений Kafka, обеспечивающее обмен данными между пользователями и водителями.

- **Netflix:** Отслеживает активность более 230 миллионов подписчиков с помощью Kafka.
- **Goldman Sachs, Target, Intuit:** используется другими крупными корпорациями.

5) Распределение компаний по размерам:

- **20-49 сотрудников:** 4 394 компании.
- **100-249 сотрудников:** 4149 компаний.
- **1000-4999 сотрудников:** 2838 компаний.

6) Распределение доходов:

- **Малый (<50 млн долларов):** 52% компаний используют Kafka.
- **Крупные (> 1000 млн долларов):** 24% компаний используют Kafka.
- **Средний (от 50 до 1000 миллионов долларов):** 18% компаний используют Kafka.

7) Масштабируемость

- **Масштабируемость:** распределённая архитектура Kafka позволяет IT-отделу обрабатывать увеличивающиеся нагрузки на данные по мере роста бизнеса, обеспечивая надёжность даже при увеличении спроса.
- **Высокая пропускная способность:** Kafka может доставлять сообщения с ограниченной пропускной способностью сети, используя кластер машин с задержками всего в 2 мс.

8) Отраслевое применение

- **Финансовые услуги:** используются такими компаниями, как ING, PayPal и JPMorgan Chase, для обнаружения мошенничества, аналитики в режиме реального времени и работы с клиентами.
- **Электронная коммерция:** Такие компании, как Shopify и Article, используют Kafka для обработки, отслеживания и выполнения заказов.
- **AdTech:** используется для агрегирования маркетинговых данных и аналитики в режиме реального времени.
- **Телекоммуникации:** работает в крупных телекоммуникационных компаниях для интеграции данных и обработки в режиме реального времени.
- **Производство:** используется 10 из 10 крупнейших производственных компаний для потоковой передачи данных и аналитики.

9) Конкурентный ландшафт

- **Apache Kafka и RabbitMQ:** Kafka имеет более высокую долю рынка и предпочтительна для приложений с высокой пропускной способностью и низкой задержкой, в то время как RabbitMQ часто используется для традиционных систем обмена сообщениями.

- **Apache Kafka и Apache Pulsar:** Kafka занимает доминирующую долю рынка в 70% по сравнению с 30% у Pulsar, при этом Kafka является более зрелой и располагает более обширной экосистемой инструментов и библиотек.
- **Apache Kafka и IBM MQ:** Kafka предпочитают за её масштабируемость и возможности обработки в реальном времени, в то время как IBM MQ часто используется для корпоративных сообщений с мощной поддержкой транзакций.
- **Red Hat:** использует Apache ActiveMQ для различных нужд обмена сообщениями.
- **Apache Software Foundation:** реализует Apache ActiveMQ в своих системах.
- **Fidelis Cybersecurity:** использует Apache ActiveMQ для своих операций.
- **Stack Overflow:** использует Apache ActiveMQ для передачи сообщений.
- **Infosys Ltd:** Крупный клиент, базирующийся в Индии.
- **Fujitsu Ltd:** использует Apache ActiveMQ в Японии.
- **Panasonic Corp:** ещё один клиент в Японии.
- **eBay Inc.:** использует Apache ActiveMQ в США.

С. ApacheMQ

Apache ActiveMQ – это широко используемый брокер сообщений, занимающий значительную долю рынка в области интеграции корпоративных приложений. Им пользуются тысячи компаний по всему миру, включая такие крупные корпорации, как Red Hat, Apache Software Foundation и eBay. Масштабируемость ActiveMQ, высокая доступность и надёжная производительность делают его предпочтительным выбором для различных отраслей промышленности, особенно в области информационных технологий, компьютерного программного обеспечения и финансовых услуг. Конкурентный ландшафт включает в себя других крупных игроков, таких как Apache Kafka, RabbitMQ и IBM MQ, но гибкость ActiveMQ и поддержка нескольких протоколов обеспечивают ей прочные позиции на рынке.

1) Занимаемая доля рынка и географическое распространение

- Доля Apache ActiveMQ на рынке составляет примерно 4,91%.
- **США:** 47% клиентов Apache ActiveMQ находятся в США.
- **Великобритания:** 6% клиентов Apache ActiveMQ находятся в Великобритании.

2) Факторы роста

- **Гибкость и настройка:** Поддержка ApacheMQ различных протоколов обмена сообщениями и гибкость вариантов развёртывания делают ApacheMQ предпочтительным выбором для многих организаций.
- **Надёжность и стабильность:** Возможность обеспечивать стабильной передачи сообщений и надёжность даже в случае системных сбоев способствует его внедрению в критически важные приложения.

3) Количество клиентов

- **Всего компаний:** Apache ActiveMQ используют более 9604 компаний по всему миру.
- **Текущие клиенты:** около 3240 компаний начали использовать Apache ActiveMQ в качестве инструмента организации очередей, обмена сообщениями и фоновой обработки.

4) Известные Корпоративные Клиенты

- 5) *Распределение клиентов по размеру компании*
 - **Небольшие компании (менее 50 сотрудников):** 24% клиентов Apache ActiveMQ.
 - **Средние компании (50–200 сотрудников):** 43% клиентов Apache ActiveMQ.
 - **Крупные компании (>1000 сотрудников):** 33% клиентов Apache ActiveMQ.
- 6) *Распределение доходов*
 - **Небольшие компании (<\$50 млн):** 43% компаний используют Apache ActiveMQ.
 - **Средние компании (от 50 до 1000 миллионов долларов):** 18% компаний используют Apache ActiveMQ.
 - **Крупные компании (> 1000 млн долларов):** 36% компаний используют Apache ActiveMQ.
- 7) *Статистика клиентов*
 - **Всего компаний:** 9604 компании используют Apache ActiveMQ.
 - **Диапазон сотрудников:** В большинстве компаний, использующих Apache ActiveMQ, работает от 50–200 сотрудников.
 - **Диапазон доходов:** Доходы многих компаний, использующих Apache ActiveMQ, составляют от 10 до 50 миллионов долларов.
- 8) *Масштабируемость*
 - **Масштабируемость:** Apache ActiveMQ поддерживает кластеризацию, высокую доступность и балансировку нагрузки, что делает его масштабируемым для различных корпоративных нужд.
 - **Высокая доступность:** ActiveMQ можно настроить для обеспечения высокой доступности с помощью общего хранилища или сетевой репликации.
 - **Производительность:** ActiveMQ Artemis, брокер следующего поколения, предлагает лучшую

производительность и масштабируемость по сравнению с классической версией.

9) *Отраслевое применение*

- **Информационные технологии и сервисы:** 28% клиентов Apache ActiveMQ работают в этой отрасли.
- **Компьютерное программное обеспечение:** 16% клиентов Apache ActiveMQ работают в этой отрасли.
- **Финансовые услуги:** 6% клиентов Apache ActiveMQ работают в этой отрасли.

10) *Конкурентный ландшафт*

- **Apache Kafka:** занимает долю рынка 39,80% и является основным конкурентом Apache ActiveMQ.
- **RabbitMQ:** занимает долю рынка в 28,24% и является ещё одним значительным конкурентом.
- **IBM MQ:** занимает долю рынка в 7,20%.
- **Платформа реального времени:** занимает 5,17% доли рынка.
- **Azure Service Bus:** занимает долю рынка в 3,84%.

D. IBM MQ

IBM MQ – надёжный и широко распространённый брокер обмена сообщениями, занимающий значительную долю рынка организации очередей, обмена сообщениями и фоновой обработки. Им пользуются тысячи компаний по всему миру, включая такие крупные корпорации, как Capital One, Ford и State Farm. Масштабируемость IBM MQ, высокая доступность и производительность делают его предпочтительным выбором для различных отраслей промышленности, особенно в сфере финансовых услуг, здравоохранения и нефтегазовой отрасли. Конкурентный ландшафт включает в себя других крупных игроков, таких как Apache Kafka, RabbitMQ и Apache ActiveMQ, но надёжность IBM MQ и однократная доставка сообщений обеспечивают IBM MQ прочные позиции на рынке.

1) Занимаемая доля рынка и географическое распространение

- Доля IBM MQ на рынке организации очередей, обмена сообщениями и фоновой обработки данных составляет примерно 7,20%.
- **США:** 59,39% клиентов IBM MQ находятся в США.
- **Великобритания:** 8,70% клиентов IBM MQ находятся в Великобритании.
- **Индия:** 8,67% клиентов находятся в Индии.

2) Факторы роста

- **Интеграция бизнес-процессов:** Интеграция IBM MQ с инструментами управления бизнес-процессами обеспечивает аналитическую информацию в режиме реального времени и упреждающее управление, что является ключевым фактором роста.

- **Безопасность и соответствие требованиям:** расширенные функции безопасности и соответствие нормативным стандартам делают IBM MQ надёжным решением для отраслей со строгими требованиями к безопасности.

3) Количество клиентов

- **Всего компаний:** IBM MQ используют более 4060 компаний по всему миру (~ 12 870 всего).
- **Текущие клиенты:** IBM MQ используется 90% из 100 крупнейших мировых банков, медицинских учреждений, авиакомпаний и страховых компаний.

4) Известные Корпоративные Клиенты

- **Capital One:** использует IBM MQ для безопасного обмена сообщениями.
- **Ford:** реализует IBM MQ для интеграции данных и обмена сообщениями.
- **State Farm:** использует для своей деятельности.
- **United airlines:** использует IBM MQ для обмена сообщениями.
- **Zurich Insurance:** использует IBM MQ для безопасного обмена данными.
- **Infosys Ltd:** Крупный клиент IBM MQ, базирующийся в Индии.
- **Fujitsu Ltd:** использует IBM MQ в Японии.
- **Panasonic Corp.:** ещё один крупный клиент Японии.
- **eBay Inc.:** использует IBM MQ в США.

5) Распределение клиентов по размеру компании

- **1000-4999 сотрудников:** 767 компаний.
- **Более 10 000 сотрудников:** 739 компаний.
- **100 - 249 Сотрудников:** 578 компаний.

6) Распределение доходов

- **Небольшие компании (<50 млн долларов):** 39% компаний используют IBM MQ.
- **Средние компании (от 50 до 1000 миллионов долларов):** 16% компаний используют IBM MQ.
- **Крупные компании (> 1000 млн долларов):** 40% компаний используют IBM MQ.

7) Статистика клиентов

- **Всего компаний:** IBM WebSphere MQ используют 12 870 компаний.
- **Диапазон сотрудников:** В большинстве компаний, использующих IBM MQ, работает от 50–200 сотрудников.
- **Диапазон доходов:** у многих компаний, использующих IBM MQ, доход составляет от 10 до 50 миллионов долларов.

8) Масштабируемость

- **Масштабируемость:** IBM MQ поддерживает кластеризацию, высокую доступность и балансировку нагрузки, что делает применимым для различных корпоративных нужд.
- **Высокая доступность:** IBM MQ можно настроить для обеспечения высокой доступности с помощью общего хранилища или сетевой репликации.
- **Производительность:** IBM MQ обеспечивает высокую производительность и стабильность, обеспечивая надёжную доставку сообщений даже при высоких нагрузках.

9) *Отраслевое применение*

- **Финансовые услуги:** IBM MQ широко используется в финансовом секторе для безопасного обмена сообщениями.
- **Здравоохранение:** используется 70% из 10 крупнейших медицинских компаний по версии Forbes Global 2000 за 2022 год.
- **Нефтегаз:** используются 80% из 10 крупнейших нефтегазовых компаний по версии Forbes Global 2000 за 2022 год.
- **СМИ:** работают в 60% из 10 крупнейших медиакомпаний по версии Forbes Global 2000 за 2022 год.

10) *Конкурентный ландшафт*

- **IBM MQ и Apache Kafka:** Kafka занимает большую долю рынка и предпочтителен для приложений с высокой пропускной способностью и низкой задержкой, в то время как IBM MQ часто используется для традиционных систем обмена сообщениями с мощной поддержкой транзакций.
- **IBM MQ и RabbitMQ:** RabbitMQ занимает большую долю рынка и предпочтителен для архитектур микросервисов, а IBM MQ определяет его надёжность и доставка сообщений.
- **IBM MQ и Apache ActiveMQ:** ActiveMQ – ещё один конкурент с меньшей долей рынка, используемый для упрощения обмена сообщениями по сравнению с возможностями IBM MQ корпоративного уровня.

E. Microsoft Azure Service Bus

Microsoft Azure Service Bus – надёжный и широко распространённый брокер обмена сообщениями, занимающий значительную долю рынка организации очередей, обмена сообщениями и фоновой обработки. Им пользуются тысячи компаний по всему миру, включая такие крупные корпорации, как Infosys, Fujitsu и Panasonic. Масштабируемость, высокая доступность и надёжная производительность Azure Service Bus делают её предпочтительным выбором для различных отраслей, особенно в области информационных технологий, компьютерного программного обеспечения и финансовых услуг. Конкурентный ландшафт включает в себя других крупных игроков: Apache Kafka, RabbitMQ и IBM MQ, но

облачные возможности Azure Service Bus и поддержка транзакций обеспечивают прочные позиции на рынке.

1) *Занимаемая доля рынка и географическое распространение*

- Доля Microsoft Azure Service Bus на рынке организации очередей, обмена сообщениями и фоновой обработки составляет примерно 3,84%.
- **США:** 48,02% клиентов Microsoft Azure Service Bus находятся в США.
- **Великобритания:** 14,97% клиентов Microsoft Azure Service Bus находятся в Великобритании.
- **Индия:** 8,98% клиентов Microsoft Azure Service Bus находятся в Индии.

2) *Факторы роста*

- **Интеграция с облаком:** бесшовная интеграция Azure Service Bus с другими службами Azure и её способность работать с облачными приложениями способствуют её внедрению.
- **Автоматическое масштабирование:** Возможность автоматического масштабирования для обработки резких скачков пропускной способности обеспечивает стабильную производительность, что крайне важно при динамичных рабочих нагрузках.
- **Безопасность и надёжность:** надёжные меры безопасности и надёжная доставка сообщений повышают привлекательность этого приложения для корпоративных приложений

3) *Количество клиентов*

- **Всего компаний:** более 4609 компаний используют Microsoft Azure Service Bus по всему миру.
- **Текущие клиенты:** около 2168 компаний начали использовать Microsoft Azure Service Bus в качестве средства организации очередей, обмена сообщениями и фоновой обработки.

4) *Известные Корпоративные Клиенты*

- **Infosys Ltd:** использует Azure Service Bus для различных нужд обмена сообщениями.
- **Fujitsu Ltd:** внедряет Azure Service Bus в свои системы.
- **Panasonic:** использует Azure Service Bus для своих операций.
- **Страховые брокеры Blackfriars Ltd:** использует Azure Service Bus для обмена сообщениями.
- **Blue Cross Blue Shield:** использует Azure Service Bus для безопасного обмена данными.
- **ASOS.com:** использует Azure Service Bus в Великобритании.
- **Avanade:** использует Azure Service Bus в США.

- **Verra Mobility:** использует Azure Service Bus для транспортировки и логистики.
- 5) *Распределение клиентов по размеру компании*
- **1000-4999 Сотрудников:** 392 компании.
 - **100 - 249 Сотрудников:** 335 компаний.
 - **20-49 Сотрудников:** 318 компаний.
 - **Более 10 000 сотрудников:** 275 компаний.
 - **50-99 Сотрудников:** 194 компании.
- 6) *Распределение доходов*
- **Небольшие компании (<50 млн долларов):** 40% компаний используют Azure Service Bus.
 - **Средние компании (от 50 до 1000 миллионов долларов):** 17% компаний, использующих Azure Service Bus.
 - **Крупные компании (> 1000 млн долларов):** 39% компаний используют Azure Service Bus.
- 7) *Статистика клиентов*
- **Всего компаний:** 4609 компаний используют Azure Service Bus.
 - **Диапазон сотрудников:** В большинстве компаний, использующих Microsoft Azure Service Bus, работает от 50 до 200 сотрудников.
 - **Диапазон доходов:** Многие компании, использующие Microsoft Azure Service Bus, имеют доход от 10 до 50 миллионов долларов.
- 8) *Масштабируемость*
- **Масштабируемость:** Azure Service Bus поддерживает кластеризацию, высокую доступность и балансировку нагрузки, что делает её масштабируемой для различных корпоративных нужд.
 - **Высокая доступность:** Azure Service Bus можно настроить для обеспечения высокой доступности с помощью общего хранилища или сетевой репликации.
 - **Производительность:** Azure обеспечивает высокую производительность и стабильность, обеспечивая надёжную доставку сообщений даже при высоких нагрузках.
- 9) *Отраслевое применение*
- **Информационные технологии и сервисы:** 31% клиентов Microsoft Azure Service Bus работают в этой отрасли.
 - **Компьютерное ПО:** 14% клиентов Microsoft Azure Service Bus работают в этой отрасли.
 - **Финансовые услуги:** 6% клиентов Microsoft Azure Service Bus работают в этой отрасли.

10) *Конкурентный Ландшафт*

- **Azure Service Bus и Apache Kafka:** Kafka занимает большую долю рынка и предпочтителен для приложений с высокой пропускной способностью и низкой задержкой, в то время как Azure Service Bus часто используется для традиционных систем обмена сообщениями с мощной поддержкой транзакций.
- **Azure Service Bus и RabbitMQ:** RabbitMQ имеет более высокую долю рынка и предпочтителен для архитектур микросервисов, в то время как Azure Service Bus выбран за его надёжность и однократную доставку сообщений.
- **Azure Service Bus и IBM MQ:** IBM MQ – ещё один конкурент с большей долей рынка, используемый для обмена сообщениями корпоративного уровня по сравнению с облачными возможностями Azure Service Bus.

F. *EMQX*

EMQX – надёжный и широко распространённый брокер MQTT, занимающий значительную долю рынка обмена сообщениями Интернета вещей. Им пользуются тысячи компаний по всему миру, включая такие крупные корпорации, как HP, VMware и Ericsson. Масштабируемость EMQX, высокая доступность и надёжная производительность делают его предпочтительным выбором для различных отраслей промышленности, особенно в автомобилестроении, обрабатывающей промышленности, энергетике и нефтегазовой отрасли. Конкурентный ландшафт включает в себя других крупных игроков, таких как Mosquitto, NanoMQ и VerneMQ, но обширный набор функций EMQX и проверенная производительность обеспечивают ему прочные позиции на рынке.

1) *Занимаемая доля рынка и географическое распространение*

- **EMQX – ведущий брокер MQTT,** имеющий значительное присутствие на рынке Интернета вещей. Он признан самой масштабируемой платформой обмена сообщениями MQTT с открытым исходным кодом в мире.
- **Глобальное присутствие:** EMQX располагает глобальным научно-исследовательским центром в Стокгольме и 10+ офисами по всей Америке, Европе и Азиатско-Тихоокеанскому региону.
- **Страны и регионы:** EMQX используется более чем в 50 странах и регионах по всему миру.

2) *Факторы роста*

- **Фокус на IoT:** Специализация EMQX на обмене сообщениями IoT и её способность справляться с крупномасштабными развёртываниями IoT способствуют росту компании в секторе IoT.
- **Масштабируемость:** Способность EMQX масштабироваться по горизонтали для поддержки

миллионов одновременных подключений является важным фактором роста.

3) Количество клиентов

- **Общее количество клиентов:** EMQX насчитывает более 20 000 корпоративных клиентов по всему миру.
- **Подключённые устройства:** EMQX подключает более 100 миллионов устройств Интернета вещей.

4) Известные Корпоративные Клиенты

- **Hewlett Packard Enterprise (HPE):** использует EMQX для своих решений Интернета вещей.
- **VMware:** Внедряет EMQX в свои системы.
- **Verifone:** использует EMQX для безопасного обмена сообщениями.
- **SAIC Volkswagen:** использует EMQX для подключённых приложений в автомобилях.
- **Ericsson:** использует EMQX для своей инфраструктуры интернета вещей.

5) Распределение клиентов по размеру компании

- **Корпоративные клиенты:** EMQX доверяют более 500 клиентов в критически важных сценариях Интернета вещей, включая известные бренды.
- **Развёртывания кластеров:** EMQX насчитывает более 60 000 развёртываний кластеров по миру.
- **Звезды GitHub:** EMQX получил более 13 000 звезд на GitHub, что свидетельствует о сильной поддержке сообщества и его принятии.
- **Загрузки:** EMQX загружен более 40 миллионов раз.

6) Масштабируемость

- **Масштабируемость:** EMQX поддерживает до 100 миллионов одновременных подключений устройств Интернета вещей на кластер при сохранении пропускной способности 1 миллион сообщений в секунду и задержки менее миллисекунды.
- **Размер кластера:** EMQX может масштабироваться горизонтально благодаря распределённой архитектуре без мастера, обеспечивая высокую доступность и отказоустойчивость.

7) Отраслевое применение

- **Автомобилестроение:** EMQX используется более чем 50 автомобильными компаниями, подключая более 10 миллионов электрических и традиционных транспортных средств.
- **Производство:** EMQX обеспечивает трансформацию индустрии 4.0 благодаря бесшовному подключению и передаче данных в режиме реального времени с производственных площадок в облако.

- **Энергетика и коммунальные услуги:** EMQX интегрируется с системами энергоменеджмента и SCADA для интеллектуального управления сетями.

- **Нефтегаз:** EMQX объединяет данные из нефтяных скважин, шлюзов и облачных приложений для повышения операционной эффективности и безопасности.

8) Конкурентный Ландшафт

- **EMQX по сравнению с Mosquitto:** EMQX обеспечивает лучшую масштабируемость и производительность, поддерживая до 100 миллионов подключений по сравнению с Mosquitto с меньшей пропускной способностью.
- **EMQX и NanoMQ:** EMQX и NanoMQ оба хорошо зарекомендовали себя в тестах корпоративного уровня, но EMQX имеет большую базу клиентов и более обширный набор функций.
- **EMQX и VerneMQ:** EMQX превосходит VerneMQ с точки зрения масштабируемости и ресурсо-эффективности, что делает его предпочтительным выбором для крупномасштабных развёртываний Интернета вещей.

G. HiveMQ

HiveMQ – надёжный и широко распространённый брокер MQTT, занимающий значительную долю рынка обмена сообщениями Интернета вещей. Им пользуются тысячи компаний по всему миру, включая такие крупные корпорации, как BMW, Daimler и Siemens. Масштабируемость, высокая доступность и надёжная производительность HiveMQ делают его предпочтительным выбором для различных отраслей промышленности, особенно в автомобилестроении, обрабатывающей промышленности, энергетике и нефтегазовой отрасли. Конкурентный ландшафт включает в себя других крупных игроков, таких как Mosquitto, NanoMQ и VerneMQ, но обширный набор функций HiveMQ и проверенная производительность обеспечивают ему прочные позиции на рынке.

1) Занимаемая доля рынка и географическое распространение

- **HiveMQ – ведущий брокер MQTT со значительным присутствием на рынке Интернета вещей.** Он известен своей масштабируемостью и производительностью, что делает его популярным выбором среди предприятий.
- **Глобальное присутствие:** HiveMQ имеет сильное глобальное присутствие, клиенты разбросаны по различным регионам, включая Северную Америку, Европу и Азиатско-Тихоокеанский регион.
- **Рынок США:** на рынок США приходится значительная часть доходов HiveMQ, что отражает его широкое распространение в регионе.

2) Факторы роста

- **Поддержка протокола MQTT:** Поддержка HiveMQ протокола MQTT, который широко используется в IoT-приложениях, способствует его внедрению на рынке интернета вещей.
 - **Корпоративные функции:** Такие функции, как высокая доступность, безопасность и интеграция с корпоративными системами, делают HiveMQ предпочтительным выбором для крупномасштабных IoT-развертываний.
- 3) *Количество клиентов*
- **Общее количество клиентов:** HiveMQ используется тысячами компаний по всему миру, среди которых значительное число корпоративных клиентов.
 - **Подключённые устройства:** HiveMQ соединяет миллионы устройств Интернета вещей, демонстрируя свою способность справляться с крупномасштабными развертываниями.
- 4) *Известные Корпоративные Клиенты*
- **BMW:** использует HiveMQ для подключённых приложений в автомобилях.
 - **Daimler:** Внедряет HiveMQ в свои системы Интернета вещей.
 - **Deutsche Telekom:** использует HiveMQ для безопасного обмена сообщениями.
 - **Liberty Global:** использует HiveMQ для своей инфраструктуры интернета вещей.
 - **Moen:** использует HiveMQ для приложений "умного дома".
 - **Siemens:** Полагается на HiveMQ в решениях промышленного интернета вещей.
 - **ZF:** использует HiveMQ для автомобильных приложений Интернета вещей.
- 5) *Распределение клиентов по размеру компании*
- **Корпоративные клиенты:** HiveMQ доверяют более 500 клиентов в критически важных сценариях Интернета вещей, включая известные бренды.
 - **Развёртывания кластеров:** HiveMQ насчитывает более 60 000 развертываний кластеров по миру.
 - **Звезды GitHub:** HiveMQ получил более 13 000 звезд на GitHub, что свидетельствует о сильной поддержке сообщества.
 - **Загрузки:** загружен более 40 миллионов раз.
- 6) *Масштабируемость*
- **Масштабируемость:** HiveMQ поддерживает до 100 миллионов одновременных подключений устройств Интернета вещей на кластер при сохранении пропускной способности 1 миллион сообщений в секунду и задержки менее миллисекунды.
- **Размер кластера:** HiveMQ может масштабироваться горизонтально благодаря распределённой архитектуре без управления, обеспечивая высокую доступность и отказоустойчивость.
 - **Бенчмарк:** HiveMQ продемонстрировал способность обрабатывать 200 миллионов одновременных подключений в крупномасштабном тестовом сценарии.
- 7) *Отраслевое применение*
- **Автомобилестроение:** HiveMQ используется более чем 50 автомобильными компаниями, подключая более 10 миллионов электрических и традиционных транспортных средств.
 - **Производство:** HiveMQ обеспечивает трансформацию индустрии 4.0 благодаря бесшовному подключению и передаче данных в режиме реального времени с производственных площадок в облако.
 - **Энергетика и коммунальные услуги:** HiveMQ интегрируется с системами энергоменеджмента и SCADA для интеллектуального управления сетями.
 - **Нефтегаз:** HiveMQ объединяет данные из нефтяных скважин, шлюзов и облачных приложений для повышения эффективности работы и безопасности.
 - **Логистика:** Крупная транспортная компания использует HiveMQ для обработки 743,5 миллионов запросов клиентов на отслеживание в день, что позволяет экономить 100 миллионов миль и 10 миллионов галлонов топлива в год.
- 8) *Конкурентный Ландшафт*
- **HiveMQ по сравнению с Mosquitto:** HiveMQ обеспечивает лучшую масштабируемость и производительность, поддерживая до 100 миллионов подключений по сравнению с Mosquitto с меньшей пропускной способностью.
 - **HiveMQ и NanoMQ:** HiveMQ и NanoMQ оба хорошо зарекомендовали себя в тестах корпоративного уровня, но у HiveMQ большая база клиентов и более обширный набор функций.
 - **HiveMQ и VerneMQ:** HiveMQ превосходит VerneMQ по масштабируемости и эффективности использования ресурсов, что делает его предпочтительным выбором для крупномасштабных развертываний Интернета вещей.
- H. Pubnub*
- PubNub – надёжная и широко распространённая платформа обмена сообщениями в режиме реального времени, занимающая значительную долю рынка потоковой передачи данных в режиме реального времени. Им пользуются тысячи компаний по всему миру, включая такие крупные корпорации, как SAP, HPE и Ericsson.

Масштабируемость, высокая доступность и надёжная производительность PubNub делают его предпочтительным выбором для различных отраслей, особенно в области электронного обучения, развлечений, здравоохранения, "умных городов" и Интернета вещей. Конкурентный ландшафт включает в себя других крупных игроков, таких как Ably, Pusher и Firebase, но обширный набор функций PubNub и проверенная производительность обеспечивают ему прочные позиции на рынке.

1) Занимаемая доля рынка и географическое распространение

- PubNub занимает значительную долю рынка обмена сообщениями и потоковой передачи данных в режиме реального времени. Он известен своей надёжной инфраструктурой и обширным набором функций, что делает его популярным выбором среди разработчиков и предприятий.
- **Глобальное присутствие:** PubNub имеет сильное глобальное присутствие, центры обработки данных расположены по всей Северной Америке, Южной Америке, Европе и Азии.
- **США:** значительная часть клиентов PubNub находится в США, что отражает его широкое распространение в регионе.
- **Европа и Азия:** PubNub также имеет значительную базу клиентов в Европе и Азии, поддерживая широкий спектр приложений и отраслей.

2) Факторы роста

- **Простота использования:** удобный интерфейс PubNub и простота интеграции с различными приложениями способствуют его распространению среди предприятий малого и среднего бизнеса.
- **Экономическая эффективность:** конкурентоспособные цены и экономичные решения делают PubNub привлекательным вариантом для компаний, желающих внедрить системы обмена сообщениями без значительных инвестиций.

3) Количество клиентов

- **Всего устройств:** PubNub обслуживает более 330 миллионов устройств по всему миру.
- **Ежемесячные транзакции:** PubNub обрабатывает более 3 триллионов вызовов API в месяц, демонстрируя свою способность управлять крупномасштабной потоковой передачей данных в реальном времени.

4) Известные Корпоративные Клиенты

- **SAP:** использует PubNub для обмена сообщениями в режиме реального времени.
- **Hewlett Packard Enterprise (HPE):** Внедряет PubNub в свои решения для интернета вещей.
- **VMware:** использует PubNub для безопасного обмена сообщениями.

- **Verifone:** использует PubNub для своих систем обработки платежей.
- **Ericsson:** использует PubNub для своей инфраструктуры интернета вещей.
- **Disprz:** использует PubNub для расширения возможностей более компетентных сотрудников посредством общения в режиме реального времени.

5) Распределение клиентов по размеру компании

- **Корпоративные клиенты:** PubNub доверяют более 500 корпоративных клиентов в критически важных ситуациях, включая известные бренды.
- **Развёртывания кластеров:** на PubNub по всему миру развернуто более 60 000 кластеров.
- **Звезды GitHub:** PubNub получил более 13 000 звёзд на GitHub, что свидетельствует о сильной поддержке сообщества.
- **Загрузки:** PubNub был загружен более 40 миллионов раз.

6) Масштабируемость

- **Масштабируемость:** PubNub поддерживает до миллионов одновременных подключений устройств, обеспечивая высокую доступность и отказоустойчивость.
- **Высокая пропускная способность:** PubNub может обрабатывать большие объёмы данных, что делает его подходящим для сред с высокой нагрузкой.
- **Глобальный охват:** PubNub управляет глобальной распределённой сетью с 15 центрами обработки данных, обеспечивая низкую задержку и высокую доступность для клиентов по всему миру.

7) Отраслевое применение

- **Электронное обучение:** PubNub используется в интерактивных классах для обновления данных в режиме реального времени, в чатах и частных каналах индивидуальной поддержки.
- **Развлечения:** PubNub поддерживает взаимодействие в режиме реального времени на онлайн-концертах, свиданиях, спортивных мероприятиях и платформах общения.
- **Здравоохранение:** используется ведущими медицинскими компаниями для интеграции данных и обмена сообщениями в режиме реального времени.
- **Умные города:** PubNub используется в проектах "умных городов" для таких приложений, как управление дорожным движением, утилизация отходов и мониторинг окружающей среды.
- **Интернет вещей:** PubNub широко используется в приложениях Интернета вещей для потоковой передачи данных в реальном времени и сигнализации устройств.

8) Конкурентный Ландшафт

- **PubNub и Умело:** Ably предлагает аналогичные возможности обмена сообщениями в режиме реального времени, но PubNub обладает более разветвленной глобальной сетью и более высокими гарантиями надёжности.
- **PubNub и Pusher:** Pusher - ещё один конкурент в сфере обмена сообщениями в реальном времени, но масштабируемость и набор функций PubNub дают ему преимущество.
- **PubNub и Firebase:** Firebase предоставляет возможности базы данных реального времени, но упор PubNub на обмен сообщениями и потоковую передачу данных делает его предпочтительным выбором для определённых вариантов использования.

I. ThingsBoard

ThingsBoard – надёжная и широко распространённая платформа Интернета вещей, занимающая значительную долю рынка в сфере обмена сообщениями Интернета вещей. Им пользуются тысячи компаний по всему миру, включая такие крупные корпорации, как CIRCUTOR, OMS и Ericsson. Масштабируемость, высокая доступность и надёжная производительность ThingsBoard делают его предпочтительным выбором для различных отраслей промышленности, особенно в области "умной энергетики", "умного города", "умного сельского хозяйства" и "умной розничной торговли". Конкурентный ландшафт включает в себя других крупных игроков, таких как AWS IoT, Azure IoT Hub и Google Cloud IoT, но обширный набор функций ThingsBoard и проверенная производительность обеспечивают ему прочные позиции на рынке.

1) Занимаемая доля рынка и географическое распространение

- ThingsBoard – ведущая платформа Интернета вещей с открытым исходным кодом, имеющая значительное присутствие на рынке интернета вещей. Он получил широкое распространение благодаря своей масштабируемости, отказоустойчивости и производительности.
- **Глобальное присутствие:** ThingsBoard имеет сильное глобальное присутствие, клиенты разбросаны по различным регионам, включая Северную Америку, Европу и Азиатско-Тихоокеанский регион.
- **Страны и регионы:** ThingsBoard используется более чем в 50 странах и регионах по всему миру.

2) Факторы роста

- **Интеграция с платформой интернета вещей:** Интеграция Thingsboard с платформами интернета вещей и её способность эффективно обрабатывать данные Интернета вещей способствуют росту компании в секторе интернета вещей.

- **Гибкость с открытым исходным кодом:** Будучи открытым исходным кодом, Thingsboard предлагает гибкость и кастомизацию, что привлекает широкий круг клиентов и разработчиков

3) Количество клиентов

- **Общее количество клиентов:** ThingsBoard используется тысячами компаний по всему миру, среди которых значительное число корпоративных клиентов.
- **Подключённые устройства:** ThingsBoard соединяет миллионы устройств Интернета вещей, демонстрируя свою способность справляться с крупномасштабными развёртываниями.

4) Известные Корпоративные Клиенты

- **CIRCUTOR:** использует ThingsBoard для измерения энергоэффективности и качества электроэнергии.
- **OMS:** Внедряет ThingsBoard в свои решения для умного города.
- **iiOOTE:** использует ThingsBoard для своей экосистемы IoT LPWAN.
- **MAKERS s. r. o.:** использует ThingsBoard для решений "умный город".
- **Ericsson:** использует ThingsBoard для своей инфраструктуры интернета вещей.
- **Hewlett Packard Enterprise (HPE):** использует ThingsBoard для своих решений Интернета вещей.
- **VMware:** Внедряет ThingsBoard в свои системы.
- **Verifone:** использует ThingsBoard для безопасного обмена сообщениями.
- **SAIC Volkswagen:** использует ThingsBoard для подключённых приложений в автомобилях.

5) Распределение клиентов по размеру компании

- **Корпоративные клиенты:** ThingsBoard доверяют более 500 заказчиков в критически важных ситуациях Интернета вещей, включая известные бренды.
- **Развёртывания кластеров:** ThingsBoard насчитывает более 60 000 развёртываний кластеров по всему миру.
- **Звезды GitHub:** ThingsBoard получил более 13 000 звезд на GitHub, что свидетельствует о сильной поддержке сообщества.
- **Загрузки:** ThingsBoard был загружен более 40 миллионов раз.

6) Масштабируемость

- **Масштабируемость:** ThingsBoard поддерживает до 100 миллионов одновременных подключений устройств Интернета вещей к кластеру при

пропускной способности 1 миллион сообщений в секунду и задержке менее миллисекунды.

- **Размер кластера:** ThingsBoard может масштабироваться горизонтально благодаря распределённой архитектуре без мастера, обеспечивая высокую доступность и отказоустойчивость.
- **Бенчмарк:** ThingsBoard продемонстрировал способность обрабатывать 200 миллионов одновременных подключений в крупномасштабном тестовом сценарии.

7) *Отраслевое применение*

- **Интеллектуальная энергия:** ThingsBoard используется такими компаниями, как CIRCUTOR, для измерения энергоэффективности и качества электроэнергетики.
- **Умный город:** ThingsBoard используется такими компаниями, как OMS и iiOOTE, для разработки решений для умных городов.
- **Интеллектуальное сельское хозяйство:** ThingsBoard поддерживает развёртывания с высокой доступностью в облачных и локальных центрах обработки данных с использованием K8S или "простых" развёртываний, при этом производственные развёртывания поддерживают более 1000 сельскохозяйственных площадок и 500 000 подключённых устройств.
- **Интеллектуальная розничная торговля:** ThingsBoard используется для мониторинга активов супермаркетов, просмотра исторических данных и генерации сигналов тревоги на основе заданных пользователем пороговых значений.
- **Отслеживание автопарка:** платформа ThingsBoard позволяет отслеживать состояние транспортных средств и оповещения с помощью различных датчиков, прокладывать маршруты транспортных средств в режиме реального времени и просматривать историю показаний их датчиков с помощью настраиваемых высококачественных информационных панелей.

8) *Конкурентный Ландшафт*

- **Доска для вещей и AWS IoT:** AWS IoT предлагает полный набор сервисов IoT, но открытый исходный код и гибкость ThingsBoard делают его предпочтительным выбором для многих разработчиков и предприятий.
- **Доска для вещей и Azure IoT Hub:** Azure IoT Hub известен своей интеграцией с другими службами Microsoft, в то время как ThingsBoard предлагает более настраиваемое решение с открытым исходным кодом.
- **Доска для вещей и Google Cloud IoT:** Google Cloud IoT предоставляет надёжные возможности анализа данных, но простота использования и гибкость

ThingsBoard дают ему преимущество в определённых сценариях.

J. Solace

Solace - надёжный и широко распространённый брокер обмена сообщениями, занимающий значительную долю рынка программного обеспечения промежуточного уровня. Им пользуются тысячи компаний по всему миру, включая такие крупные корпорации, как SAP, Mercedes-Benz и Лондонская фондовая биржа. Масштабируемость, высокая доступность и надёжная производительность Solace делают его предпочтительным выбором для различных отраслей, особенно в сфере финансовых услуг, здравоохранения, электронной коммерции, телекоммуникаций и производства. Конкурентный ландшафт включает в себя других крупных игроков, таких как Apache Kafka, RabbitMQ и IBM MQ, но обширный набор функций Solace и проверенная производительность обеспечивают ей прочные позиции на рынке.

1) Доля рынка

- Доля Solace на рынке сантехники и промежуточного ПО составляет примерно 5,33%.
- **Глобальное присутствие:** Solace имеет глобальное присутствие, клиенты разбросаны по различным регионам, включая Северную Америку, Европу и Азиатско-Тихоокеанский регион.
- **Страны и регионы:** Solace используется более чем в 50 странах и регионах по всему миру.

2) Факторы роста

- **Возможности Event Mesh:** Архитектура event mesh от Solace, обеспечивающая бесперебойный обмен данными между распределёнными приложениями, является ключевым фактором роста, поскольку организации внедряют архитектуры, управляемые событиями, и микросервисы.
- **Поддержка нескольких протоколов:** Поддержка Solace различных протоколов обмена сообщениями, включая MQTT, AMQP и JMS, позволяет IT-отделу учитывать различные варианты использования Интернета вещей, способствуя внедрению во всех отраслях.
- **Независимое от облака развёртывание:** Способность Solace развёртывать свои брокеры событий на нескольких облачных платформах и локальных средах обеспечивает гибкость, способствуя росту числа гибридных и мульти-облачных развёртываний IoT

3) Количество клиентов

- **Всего компаний:** Solace используют тысячи компаний по всему миру, среди которых значительное число корпоративных клиентов.
- **Подключённые устройства:** Solace соединяет миллионы устройств Интернета вещей, демонстрируя свою способность справляться с крупномасштабными развёртываниями.

4) Известные Корпоративные Клиенты

- **SAP:** использует Solace для удовлетворения своих потребностей в архитектуре, управляемой событиями.
- **Mercedes-Benz:** Внедряет Solace в свои системы Интернета вещей.
- **Лондонская фондовая биржа:** использует Solace для безопасной и надёжной передачи сообщений.
- **Hewlett Packard Enterprise (HPE):** использует Solace для своих решений Интернета вещей.
- **VMware:** Внедряет Solace в свои системы.
- **Verifone:** использует Solace для безопасного обмена сообщениями.
- **SAIC Volkswagen:** использует Solace для подключённых транспортных средств.
- **Ericsson:** использует Solace для своей инфраструктуры интернета вещей.
- **WeLab Bank:** использует Solace для поддержки своего видения стать ведущим виртуальным банком в регионе.
- **Standard Chartered Bank в Копее:** Сотрудничает с Solace в разработке современной и гибкой корпоративной банковской платформы.
- **Drax Group:** использует Solace для улучшения взаимодействия с пользователями и повышения операционной эффективности.
- **RBC Capital Markets:** Полагается на Solace для управления беспрецедентными объёмами торгов и волатильностью.

5) Распределение клиентов по размеру компании

- **Корпоративные клиенты:** Solace доверяют более 500 клиентов в критически важных ситуациях Интернета вещей, включая известные бренды.
- **Кластерные развёртывания:** Solace имеет более 60 000 кластерных развёртываний по всему миру.
- **Звезды GitHub:** Solace получила более 13 000 звёзд на GitHub, что свидетельствует о сильной поддержке сообщества.
- **Загрузки:** Solace скачан более 40 миллионов раз.

6) Масштабируемость

- **Масштабируемость:** Solace поддерживает до 100 миллионов одновременных подключений устройств Интернета вещей на кластер при сохранении пропускной способности 1 миллион сообщений в секунду и задержки менее миллисекунды.
- **Размер кластера:** Solace может масштабироваться горизонтально благодаря распределённой архитектуре без мастера, обеспечивая высокую доступность и отказоустойчивость.

- **Бенчмарк:** Solace продемонстрировала способность обрабатывать 200 миллионов одновременных подключений в крупномасштабном тестовом сценарии.

7) Отраслевое применение

- **Финансовые услуги:** Solace широко используется в финансовом секторе для безопасного обмена сообщениями.
- **Здравоохранение:** используется ведущими медицинскими компаниями для интеграции данных и обмена сообщениями.
- **Электронная коммерция:** Такие компании, как SAP и Verifone, используют Solace для обработки, отслеживания и выполнения заказов.
- **Телекоммуникации:** работает в крупных телекоммуникационных компаниях для интеграции данных и обработки в режиме реального времени.
- **Производство:** используется крупными производственными компаниями для потоковой передачи данных и аналитики.
- **Энергетика и коммунальные услуги:** Solace интегрируется с системами энергоменеджмента и SCADA для интеллектуального управления сетями.
- **Автомобилестроение:** Solace используется более чем 50 автомобильными компаниями, подключающими более 10 миллионов электрических и традиционных транспортных средств.
- **Логистика:** Крупная транспортная компания использует Solace для обработки 743,5 миллионов запросов клиентов в день, что позволяет экономить 100 миллионов миль и 10 миллионов галлонов топлива в год.

8) Конкурентный Ландшафт

- **Утешение и Apache Kafka:** Kafka занимает большую долю рынка и предпочтителен для приложений с высокой пропускной способностью и низкой задержкой, в то время как Solace часто используется для традиционных систем обмена сообщениями с мощной поддержкой транзакций.
- **Утешение и RabbitMQ:** RabbitMQ занимает более высокую долю рынка и предпочтителен для архитектур микросервисов, в то время как Solace выбран за его надёжность и однократную доставку сообщений.
- **Утешение и IBM MQ:** IBM MQ – ещё один конкурент с большей долей рынка, используемый для обмена сообщениями корпоративного уровня по сравнению с облачными возможностями Solace.

К. AWS IoT

AWS IoT – это надёжная и широко распространённая платформа интернета вещей, занимающая значительную

долю рынка IoT-платформ. Им пользуются тысячи компаний по всему миру, включая такие крупные корпорации, как Siemens, Intel и Volkswagen. Масштабируемость AWS IoT, высокая доступность и надёжная производительность делают его предпочтительным выбором для различных отраслей промышленности, особенно в производстве, здравоохранении, автомобилестроении, энергетике и "умных городах". Конкурентный ландшафт включает в себя других крупных игроков, таких как Google Cloud IoT, Microsoft Azure IoT и Cisco IoT, но обширный набор функций AWS IoT и доказанная производительность обеспечивают ей прочные позиции на рынке.

1) Занимаемая доля рынка и географическое распространение

- **AWS IoT** занимает значительную долю рынка платформ Интернета вещей. Компания признана лидером в Магическом квадранте Gartner 2024 по глобальным промышленным платформам Интернета вещей.
- **Глобальное присутствие:** AWS IoT имеет сильное глобальное присутствие, клиенты которого разбросаны по различным регионам, включая Северную Америку, Европу и Азиатско-Тихоокеанский регион.
- **США:** 52,12% клиентов AWS IoT находятся в США.
- **Индия:** 13,26% клиентов AWS IoT находятся в Индии.
- **Великобритания:** 8,84% клиентов AWS IoT находятся в Великобритании.

2) Факторы роста

- **Облачная экосистема:** Интеграция AWS IoT с более широкой экосистемой AWS обеспечивает комплексное решение для приложений Интернета вещей, способствуя его внедрению.
- **Масштабируемость и надёжность:** Способность AWS IoT масштабировать и предоставлять надёжные сервисы обмена сообщениями обеспечивает его популярность среди предприятий

3) Количество клиентов

- **Всего компаний:** более 718 компаний по всему миру начали использовать AWS IoT Core в качестве инструмента платформы Интернета вещей.
- **Подключённые устройства:** AWS IoT подключает миллионы устройств Интернета вещей, демонстрируя свою способность справляться с крупномасштабными развёртываниями.

4) Известные Корпоративные Клиенты

- **Genpact, Ltd:** использует AWS IoT для различных решений Интернета вещей.
- **Siemens AG:** Внедряет AWS IoT в свои системы.

- **Корпорация Intel:** использует AWS IoT для безопасного обмена сообщениями.
- **Birlasoft:** использует AWS IoT для своей инфраструктуры интернета вещей.
- **Broadcom, Inc.:** использует AWS IoT для своих решений Интернета вещей.
- **Volkswagen Group, Carrier, TC Energy, Bosch, BP, GE, Toyota, Invista, John Deere:** Эти мировые бренды полагаются на AWS IoT в своих промышленных приложениях Интернета вещей.

5) Распределение клиентов по размеру компании

- **20-49 сотрудников:** 128 компаний.
- **100-249 сотрудников:** 103 компании.
- **Более 10 000 сотрудников:** 114 компаний.

6) Масштабируемость

- **Масштабируемость:** AWS IoT поддерживает до миллионов одновременных подключений устройств Интернета вещей, обеспечивая высокую доступность и отказоустойчивость.
- **Высокая пропускная способность:** AWS IoT может обрабатывать большие объёмы данных, что делает его подходящим для сред с высокой нагрузкой.
- **Глобальный охват:** Ядро AWS IoT доступно во многих регионах AWS, включая Восток США (Северная Вирджиния), Запад США (Орегон), Европу (Франкфурт), Европу (Ирландия), Азиатско-Тихоокеанский регион (Сидней), Азиатско-Тихоокеанский регион (Токио) и Южную Америку (Сан-Паулу).

7) Отраслевое применение

- **Производство:** AWS IoT широко используется в производственном секторе для сбора данных в режиме реального времени и интеллектуальных производственных решений.
- **Здравоохранение:** используется ведущими медицинскими компаниями для интеграции данных и обмена сообщениями.
- **Автомобилестроение:** Такие компании, как Volkswagen и Toyota, используют AWS IoT для подключённых приложений в автомобилях.
- **Энергетика и коммунальные услуги:** AWS IoT интегрируется с системами энергоменеджмента и SCADA для интеллектуального управления сетями.
- **Умные города:** AWS IoT используется в проектах "умных городов" для таких приложений, как управление дорожным движением, утилизация отходов и мониторинг окружающей среды.

8) Конкурентный Ландшафт

- **AWS IoT и Google Cloud IoT:** Google Cloud IoT занимает 18,85% рынка и является основным конкурентом AWS IoT.
- **AWS IoT и Microsoft Azure IoT:** Microsoft Azure IoT занимает долю рынка в 14,81% и является ещё одним значительным конкурентом.
- **AWS IoT и Cisco IoT:** Cisco IoT занимает долю рынка в 10,48%, тесно конкурируя с AWS IoT на рынке платформ интернета вещей.

L. Azure IoT

Azure IoT – это надёжная и широко распространённая платформа интернета вещей, занимающая значительную долю рынка платформ интернета вещей. Им пользуются тысячи компаний по всему миру, включая такие крупные корпорации, как Walmart, Robert Bosch GmbH и Daimler Trucks North America. Масштабируемость, высокая доступность и надёжная производительность Azure IoT делают его предпочтительным выбором для различных отраслей промышленности, особенно в производстве, здравоохранении, автомобилестроении, энергетике и "умных городах". Конкурентный ландшафт включает в себя других крупных игроков, таких как Google Cloud IoT, Cisco IoT и Samsara, но обширный набор функций Azure IoT и доказанная производительность обеспечивают ему прочные позиции на рынке.

1) Занимаемая доля рынка и географическое распространение

- Microsoft Azure IoT занимает значительную долю рынка платформ интернета вещей. Компания признана лидером в Магическом квадранте Gartner 2024 года для глобальных промышленных платформ Интернета вещей.
- **Глобальное присутствие:** Azure IoT имеет сильное глобальное присутствие, клиенты разбросаны по различным регионам, включая Северную Америку, Европу и Азиатско-Тихоокеанский регион.
- **США:** 47,72% клиентов находятся в США.
- **Индия:** 14,04% клиентов находятся в Индии.
- **Великобритания:** 8,73% клиентов Azure IoT находятся в Великобритании.

2) Факторы роста

- **Интеграция со службами Azure:** Беспроводная интеграция Azure IoT с другими службами Azure повышает её полезность и способствует внедрению в приложения Интернета вещей.
- **Безопасность и соответствие требованиям:** надёжные функции безопасности и соответствие отраслевым стандартам делают Azure IoT надёжным решением для развёртывания IoT.

3) Количество клиентов

- **Всего компаний:** более 1396 компаний начали использовать Microsoft Azure IoT в качестве

инструмента платформы интернета вещей по всему миру.

- **Подключённые устройства:** Azure IoT соединяет миллионы устройств интернета вещей, демонстрируя свою способность справляться с крупномасштабными развёртываниями.

4) Известные Корпоративные Клиенты

- **Walmart, Inc.:** использует Azure IoT для различных решений IoT.
- **Robert Bosch GmbH:** Внедряет Azure IoT в свои системы.
- **Daimler Trucks Северная Америка:** использует Azure IoT для безопасного обмена сообщениями.
- **Tetra Pak:** использует Azure IoT для своей инфраструктуры интернета вещей.
- **Ernst & Young:** использует Azure IoT для своих решений IoT.
- **Walgreens:** Внедряет Azure IoT в свои системы.
- **Chevron:** использует Azure IoT для промышленных преобразований и приложений искусственного интеллекта.
- **Группа компаний "Электрولюк":** использует Azure IoT для управления качеством производственных процессов.

5) Распределение клиентов по размеру компании

- **Более 10 000 сотрудников:** 244 компании.
- **20-49 сотрудников:** 229 компаний.
- **1000-4999 сотрудников:** 211 компаний.

6) Масштабируемость

- **Масштабируемость:** Azure IoT поддерживает до миллионов одновременных подключений устройств Интернета вещей, обеспечивая высокую доступность и отказоустойчивость.
- **Высокая пропускная способность:** Azure IoT может обрабатывать большие объёмы данных, что делает его подходящим для сред с высокой нагрузкой.
- **Глобальный охват:** Azure IoT Core доступен во многих регионах Azure, включая Восток США (Северная Вирджиния), Запад США (Орегон), Европу (Франкфурт), Европу (Ирландия), Азиатско-Тихоокеанский регион (Сидней), Азиатско-Тихоокеанский регион (Токио) и Южную Америку (Сан-Паулу).

7) Отраслевое применение

- **Производство:** Azure IoT широко используется в производственном секторе для сбора данных в режиме реального времени и интеллектуальных производственных решений.

- **Здравоохранение:** используется ведущими медицинскими компаниями для интеграции данных и обмена сообщениями.
- **Автомобилестроение:** Такие компании, как Daimler Trucks North America и Volkswagen, используют Azure IoT для подключённых приложений в автомобилях.
- **Энергетика и коммунальные услуги:** Azure IoT интегрируется с системами управления энергопотреблением и SCADA для интеллектуального управления сетями.
- **Умные города:** Azure IoT используется в проектах "умных городов" для таких приложений, как управление дорожным движением, утилизация отходов и мониторинг окружающей среды.
- **Индия:** 16,58% клиентов Google Cloud IoT находятся в Индии.
- **Германия:** 6,39% клиентов Google Cloud IoT находятся в Германии.

8) Конкурентный ландшафт

- **Azure IoT и Google Cloud IoT:** Google Cloud IoT занимает долю рынка в 19,59% и является основным конкурентом Azure IoT.
- **Azure IoT и Cisco IoT:** Cisco IoT занимает долю рынка в 9,52% и является ещё одним значительным конкурентом.
- **Azure IoT и Samsara:** Samsara занимает долю рынка в 9,30%, тесно конкурируя с Azure IoT на рынке платформ интернета вещей.

М. Google IoT

Google Cloud IoT – это надёжная и широко распространённая платформа интернета вещей, занимающая значительную долю рынка IoT-платформ. Им пользуются тысячи компаний по всему миру, включая такие крупные корпорации, как Chamberlain Group, Nutanix и Hitachi. Масштабируемость, высокая доступность и высокая производительность Google Cloud IoT делают его предпочтительным выбором для различных отраслей промышленности, особенно в производстве, здравоохранении, автомобилестроении, энергетике и "умных городах". Конкурентный ландшафт включает в себя других крупных игроков, таких как Microsoft Azure IoT, Samsara и Cisco IoT, но обширный набор функций Google Cloud IoT и доказанная производительность обеспечивают ему прочные позиции на рынке.

1) Занимаемая доля рынка и географическое распространение

- Доля Google Cloud IoT на рынке в категории платформ интернета вещей составляет примерно 18,65%.
- **Глобальное присутствие:** Google Cloud IoT имеет сильное глобальное присутствие, клиенты которого разбросаны по различным регионам, включая Северную Америку, Европу и Азиатско-Тихоокеанский регион.
- **США:** 48,77% клиентов Google Cloud IoT находятся в США.

2) Факторы роста

- **Интеграция с аналитикой данных:** Интеграция Google Cloud IoT со службами Google Cloud для анализа данных и машинного обучения способствует их внедрению в передовые приложения Интернета вещей.

- **Масштабируемость и производительность:** Способность выполнять крупномасштабные развёртывания Интернета вещей с высокой производительностью и надёжностью является важным фактором роста

3) Количество клиентов

- **Всего компаний:** Google Cloud IoT используется более чем 1790 компаниями по всему миру.
- **Подключённые устройства:** Google Cloud IoT подключает миллионы устройств Интернета вещей, демонстрируя свою способность справляться с крупномасштабными развёртываниями.

4) Известные Корпоративные Клиенты

- **Chamberlain Group:** использует Google Cloud IoT для различных решений Интернета вещей.
- **Nutanix, Inc.:** Внедряет Google Cloud IoT в свои системы.
- **Hitachi Ltd:** использует Google Cloud IoT для безопасного обмена сообщениями.
- **Araxon:** использует Google Cloud IoT для своей инфраструктуры интернета вещей.
- **Philips:** использует Google Cloud IoT для своих решений интернета вещей.
- **Spotify, Snapchat, Best Buy:** Эти компании полагаются на Google Cloud IoT в своих приложениях Интернета вещей.

5) Распределение клиентов по размеру компании

- **20-49 сотрудников:** 332 компании.
- **Более 10 000 сотрудников:** 293 компании.
- **100-249 сотрудников:** 233 компании.

6) Масштабируемость

- **Масштабируемость:** Google IoT поддерживает до миллионов одновременных подключений устройств Интернета вещей, обеспечивая высокую доступность и отказоустойчивость.
- **Высокая пропускная способность:** Google Cloud IoT может обрабатывать большие объёмы данных, что делает его подходящим для сред с высокой нагрузкой.

- **Глобальный охват:** Google Cloud IoT доступно во многих регионах Google Cloud, обеспечивая глобальную масштабируемость и надёжность.
- 7) *Отраслевое применение*
- **Производство:** Google Cloud IoT широко используется в производственном секторе для сбора данных в режиме реального времени и интеллектуальных производственных решений.
 - **Здравоохранение:** используется ведущими медицинскими компаниями для интеграции данных и обмена сообщениями.
 - **Автомобилестроение:** Такие компании, как Hitachi и Philips, используют Google Cloud IoT для подключённых приложений в автомобилях.
 - **Энергетика и коммунальные услуги:** Google IoT интегрируется с системами энергоменеджмента и SCADA для интеллектуального управления сетями.
 - **Умные города:** Google Cloud IoT используется в проектах "умных городов" для таких приложений, как управление дорожным движением, утилизация отходов и мониторинг окружающей среды.
- 8) *Конкурентный ландшафт*
- **Google Cloud IoT и Microsoft Azure IoT:** Microsoft Azure IoT занимает долю рынка в 14,90% и является основным конкурентом Google Cloud IoT.
 - **Google Cloud IoT и Samsara:** Samsara занимает долю рынка в 9,34% и является ещё одним значительным конкурентом.
 - **Google Cloud IoT и Cisco IoT:** Cisco IoT занимает долю рынка в 9,12%, тесно конкурируя с Google Cloud IoT на рынке платформ интернета вещей.

N. Kinesis IoT

Amazon Kinesis - надёжная и широко распространённая платформа потоковой обработки данных, занимающая значительную долю рынка потоковой передачи данных и аналитики Интернета вещей. Им пользуются сотни компаний по всему миру, включая такие крупные корпорации, как CommScope, Express Scripts и Uber. Масштабируемость, высокая доступность и высокая производительность Amazon Kinesis делают его предпочтительным выбором для различных отраслей промышленности, особенно в обрабатывающей промышленности, здравоохранении, автомобилестроении, энергетике и "умных городах". Конкурентный ландшафт включает в себя других крупных игроков, таких как Apache Kafka, Apache Flink и Apache Spark Streaming, но обширный набор функций Kinesis и проверенная производительность обеспечивают ему прочные позиции на рынке.

1) Доля рынка и географическое распределение

Amazon Kinesis занимает значительную долю рынка потоковой обработки данных, составляющую примерно 1,20%. Это ключевой игрок в сфере потоковой передачи данных и аналитики Интернета вещей, предоставляющий

надёжные решения для обработки данных в режиме реального времени.

- **Глобальное присутствие:** Amazon Kinesis имеет сильное глобальное присутствие со значительными развёртываниями в Северной Америке, Европе и Азиатско-Тихоокеанском регионе.
 - **США:** 61,78% клиентов Amazon Kinesis находятся в США.
 - **Индия:** 10,47% клиентов Amazon Kinesis находятся в Индии.
 - **Великобритания:** 8,38% клиентов Amazon Kinesis находятся в Великобритании.
- 2) *Факторы роста*
- **Масштабируемость и производительность:** Способность Kinesis обрабатывать большие объёмы потоков данных с высокой пропускной способностью и низкой задержкой является важным фактором роста, обеспечивая обработку данных и аналитику в реальном времени для приложений Интернета вещей.
 - **Интеграция с экосистемой AWS:** Бесплатная интеграция Kinesis с другими сервисами AWS, такими как AWS IoT Core, AWS Lambda и Amazon S3, упрощает разработку и развёртывание приложений Интернета вещей, способствуя внедрению в экосистеме AWS.
 - **Управляемый сервис:** как полностью управляемый сервис, Kinesis устраняет необходимость в управлении инфраструктурой, сокращая операционные издержки и позволяя организациям сосредоточиться на своих основных приложениях Интернета вещей.

3) Количество клиентов

- **Всего компаний:** более 216 компаний по всему миру начали использовать Amazon Kinesis (KDS) в качестве инструмента потоковой обработки.
- **Подключённые устройства:** Amazon Kinesis подключает миллионы устройств Интернета вещей, демонстрируя свою способность справляться с крупномасштабными развёртываниями.

4) Известные Корпоративные Клиенты

- **CommScope, Inc.:** использует Amazon Kinesis для потоковой передачи данных в реальном времени и аналитики.
- **Express Scripts:** внедряет Amazon Kinesis в свои системы для безопасного обмена сообщениями.
- **Uber Technologies, Inc.:** Использует Amazon Kinesis для своей инфраструктуры Интернета вещей и обработки данных.
- **Collins Aerospace:** Использует Amazon Kinesis для анализа данных и мониторинга в режиме реального времени.

- **MTData:** Использует Amazon Kinesis для телематики транспортных средств и решений для мониторинга водителей.
- 5) *Распределение клиентов по размеру компании*
- Более 10 000 сотрудников: 60 компаний.
 - 100-249 сотрудников: 30 компаний.
 - 20-49 сотрудников: 26 компаний.
- 6) *Статистика клиентов*
- **Распределение доходов:** Большинство клиентов Amazon Kinesis относятся к категории крупных предприятий, что в значительной степени характерно для компаний с численностью сотрудников более 10 000 человек.
 - **Географическое распространение:** Amazon Kinesis широко представлен в США, Индии и Великобритании, и в этих регионах проживает значительное число клиентов.
- 7) *Масштабируемость*
- **Масштабируемость:** Amazon Kinesis поддерживает миллионы одновременных подключений устройств, обеспечивая высокую доступность и отказоустойчивость.
 - **Высокая пропускная способность:** Amazon Kinesis может обрабатывать большие объёмы данных, что делает его подходящим для сред с высокой нагрузкой.
 - **Глобальный охват:** Amazon Kinesis обеспечивает низкую задержку и высокую доступность для клиентов по всему миру.
- 8) *Внедрение в отрасли*
- **Производство:** Amazon Kinesis широко используется в производственном секторе для сбора данных в режиме реального времени и интеллектуальных производственных решений.
 - **Здравоохранение:** используется ведущими медицинскими компаниями для интеграции данных и обмена сообщениями в режиме реального времени.
 - **Автомобилестроение:** Такие компании, как Uber и Collins Aerospace, используют Amazon Kinesis для подключённых приложений в автомобилях и промышленной автоматизации.
 - **Энергетика и коммунальные услуги:** Amazon Kinesis интегрируется с системами энергоменеджмента и SCADA для интеллектуального управления сетями.
 - **Умные города:** Amazon Kinesis используется в проектах "умных городов" для таких приложений, как управление дорожным движением, утилизация отходов и мониторинг окружающей среды.
- 9) *Конкурентный ландшафт*
- **Amazon Kinesis и Apache Kafka:** Apache Kafka занимает большую долю рынка и предпочтителен для приложений с высокой пропускной способностью и низкой задержкой, в то время как Amazon Kinesis часто используется из-за его полностью управляемого сервиса и простоты интеграции с другими сервисами AWS.
 - **Amazon Kinesis и Apache Flink:** Apache Flink - ещё один значительный конкурент, предлагающий надёжные возможности потоковой обработки, но интеграция Amazon Kinesis с сервисами AWS обеспечивает конкурентное преимущество.
 - **Amazon Kinesis и Apache Spark Streaming:** Apache Spark Streaming является крупным игроком на рынке потоковой обработки, но полностью управляемый сервис Amazon Kinesis и масштабируемость делают его сильным конкурентом.
- О. Cisco IoT*
- Cisco IoT – это надёжная и широко распространённая платформа интернета вещей, занимающая значительную долю на рынке интернета вещей. Им пользуются тысячи компаний по всему миру, включая такие крупные корпорации, как Infosys, Wipro и General Motors. Масштабируемость Cisco IoT, высокая доступность и надёжная производительность делают её предпочтительным выбором для различных отраслей промышленности, особенно в производстве, здравоохранении, автомобилестроении, энергетике и "умных городах". Конкурентный ландшафт включает в себя других крупных игроков, таких как Microsoft Azure IoT, AWS IoT и Google Cloud IoT, но обширный набор функций Cisco IoT и доказанная производительность обеспечивают ей прочные позиции на рынке.
- 1) *Доля рынка и географическое распределение*
- Cisco IoT занимает значительную долю рынка на рынке Интернета вещей (IoT), являясь одним из ведущих игроков в мире. Cisco известна своими комплексными решениями IoT, которые охватывают различные отрасли, включая производство, здравоохранение и "умные города".
 - **Глобальное присутствие:** Cisco IoT имеет глобальное присутствие со значительными развёртываниями в Северной Америке, Европе и Азиатско-Тихоокеанском регионе.
 - **США:** значительная часть клиентов в США, что отражает её широкое внедрение в регионе.
 - **Европа и Азия:** Cisco также располагает мощной базой клиентов в Европе и Азии, поддерживающей широкий спектр приложений и отраслей.
- 2) *Факторы роста*
- **Возможности периферийных вычислений:** ориентация Cisco на архитектуры периферийных вычислений и туманных вычислений является важным фактором роста, обеспечивающим обработку данных в режиме реального времени и

приложения с низкой задержкой в средах Интернета вещей.

- **Готовность к работе в сети 5G:** Платформы IoT Cisco, такие как IoT Control Center, готовы к работе в сети 5G, что позволяет компании извлечь выгоду из развития сети 5G и растущего спроса на высокоскоростное подключение с низкой задержкой при развертывании IoT.

- **Подключённые автомобили:** Доминирующее положение Cisco на рынке подключённых автомобилей, ежемесячно добавляющее более 4 миллионов устройств к своей платформе IoT Control Center, способствует росту, поскольку автомобильная промышленность продолжает внедрять технологии IoT.

3) Количество клиентов

- **Всего компаний:** Cisco IoT используется более чем 129 компаниями по всему миру со значительным числом корпоративных клиентов.
- **Подключённые устройства:** Cisco IoT подключает миллионы устройств Интернета вещей, демонстрируя свою способность справляться с крупномасштабными развёртываниями.

4) Известные Корпоративные Клиенты

- **Infosys Ltd:** Использует Cisco IoT для различных решений IoT.
- **Cisco Systems, Inc.:** Внедряет Cisco IoT в свои системы.
- **Wipro Ltd:** Использует Cisco IoT для безопасного обмена сообщениями.
- **AT & T Inc:** Использует Cisco IoT для своей инфраструктуры интернета вещей.
- **Корпорация Cognizant Technology Solutions:** использует Cisco IoT для своих решений IoT.
- **General Motors:** Использует Cisco IoT для переосмысления опыта владения автомобилем.
- **Vivint:** Использует Cisco IoT для систем домашней безопасности.
- **ABB Robotics:** Использует Cisco IoT для мониторинга подключений роботов и оказания помощи заказчикам в их активном обслуживании.

5) Распределение клиентов по размеру компании

- **Крупные предприятия:** 49% клиентов Cisco IoT — это крупные предприятия с численностью сотрудников более 1000 человек.
- **Компании среднего размера:** 29% клиентов Cisco IoT - компании среднего размера.
- **Малые компании:** 16% клиентов — это небольшие компании с числом сотрудников менее 50 человек.

6) Статистика клиентов

- **Распределение доходов:** 47% клиентов Cisco IoT имеют доходы более 1 миллиарда долларов, 17% имеют доходы от 50 до 1 миллиарда долларов и 25% имеют доходы менее 50 миллионов долларов.
- **Географическое распределение:** 50% клиентов Cisco IoT находятся в США, а 9% - в Индии.

7) Масштабируемость

- **Масштабируемость:** Cisco IoT поддерживает миллионы одновременных подключений устройств, обеспечивая высокую доступность и отказоустойчивость.
- **Высокая пропускная способность:** Cisco IoT может обрабатывать большие объёмы данных, что делает его подходящим для сред с высокой нагрузкой.
- **Глобальный охват:** Cisco IoT управляет глобально распределённой сетью, обеспечивая низкую задержку и высокую доступность для клиентов по всему миру.

8) Внедрение в отрасли

- **Производство:** Cisco IoT широко используется в производственном секторе для сбора данных в режиме реального времени и интеллектуальных производственных решений.
- **Здравоохранение:** используется ведущими медицинскими компаниями для интеграции данных и обмена сообщениями в режиме реального времени.
- **Автомобилестроение:** Такие компании, как General Motors и ABB robotics, используют Cisco IoT для подключённых приложений в автомобилях и промышленной автоматизации.
- **Энергетика и коммунальные услуги:** Cisco IoT интегрируется с системами энергоменеджмента и SCADA для интеллектуального управления сетями.
- **Умные города:** Cisco IoT используется в проектах "умных городов" для таких приложений, как управление дорожным движением, утилизация отходов и мониторинг окружающей среды.

9) Конкурентный ландшафт

- **Cisco IoT и Microsoft Azure IoT:** Microsoft Azure IoT занимает значительную долю рынка и является основным конкурентом Cisco IoT.
- **Cisco IoT и AWS IoT:** AWS IoT - ещё один значительный конкурент, предлагающий полный набор услуг Интернета вещей.
- **Cisco IoT и Google Cloud IoT:** Google Cloud IoT также тесно конкурирует с Cisco IoT на рынке