ТОЛЬКО ПРОТИВОРЕЧИВЫЕ СОВЕТЫ ПОМОГАЮТ ПОНЯТЬ, ЧТО ТАКОЕ ИБ

ИРОНИЯ БЕЗОПАСНОСТИ

ДАЙДЖЕСТ. 2024 / 06

Добро пожаловать в очередной выпуск ежемесячного сборника материалов, который является вашим универсальным ресурсом для получения информации о самых последних разработках, аналитических материалах и лучших практиках в постоянно развивающейся области безопасности. В этом выпуске мы подготовили разнообразную подборку статей, новостей и результатов исследований, рассчитанных как на профессионалов, так и на обычных любителей. Цель нашего дайджеста - сделать наш контент интересным и доступным. Приятного чтения!

Больше контента:

BOOSTY

SPONSR

TELEGRAM

Рубрика: Ключевые факты

сжатая редакция других разделов для быстрого и всестороннего обзора.

Рубрика: Разбор

критические обзоры и анализ статей, включая научно-практические статьи и отраслевые отчёты

Рубрика: Исследование

оригинальные исследования, отчёты и выводы, способствующие пониманию проблем кибербезопасности

Больше материалов: Boosty | Sponsr | TG

Новости

Нефтегазовая отрасль, кибер-атаки и геймификация

Системы сжиженного природного газа уязвимы для кибератак из-за внутренних системных рисков, которые включают в себя удалённо управляемые системы сторонних производителей и уязвимые бортовые технологии, такие как программируемые логические контроллеры (ПЛК), глобальная система позиционирования (GPS) и система автоматической идентификации (AIS). Эти уязвимости могут привести к переполнению топливных баков, случайному выбросу СПГ и другим рискам, которые делают СПГ недоступным или вызывают серьёзные последствия при возвращении в газообразное состояние

В середине февраля 2022 года хакеры получили доступ к компьютерам, принадлежащим нынешним и бывшим сотрудникам почти двух десятков крупных поставщиков и экспортёров природного газа, включая Chevron Corp., Cheniere Energy Inc. и Kinder Morgan Inc. Эти атаки были нацелены на компании, занимающиеся производством сжиженного природного газа (СПГ), и стали первым этапом в попытке проникнуть во все более важный сектор энергетической отрасли.

Кроме того, ФБР предупредило энергетический сектор о вероятном увеличении числа атак со стороны китайских и российских хакеров в связи с изменениями в глобальной цепочке поставок энергии. В предупреждении упоминаются такие факторы, как увеличение экспорта СПГ из США и продолжающееся давление Запада на энергоснабжение России, но не упоминаются какие-либо конкретные нападения на танкеры со сжиженным газом.

Штаб-квартиры Chevron Corp., Cheniere Energy Inc. и Kinder Morgan Inc. находятся в США: штаб-квартира Chevron расположена в Сан-Рамоне, штат Калифорния, штаб-квартира Cheniere Energy находится в Хьюстоне, штат Техас, а штаб-квартира Kinder Morgan - в Хьюстоне, штат Техас.

Сейчас.... "Мы даже не можем построить даже наши собственные танкеры со сжиженным газом здесь, в США".

По иронии судьбы оказывается, что ни одна судоверфь в США не способна строить танкеры для сжиженного газа, как признал министр ВМС США Карлос Дель Торо в своём выступлении перед Конгрессом в среду. "Мы утратили это искусство здесь, в США. Мы даже не можем строить свои собственные танкеры для сжиженного газа здесь, в США", - заявил Дель Торо Комитету по вооружённым силам Палаты представителей США. Согласно судостроительным документам, последний раз американская верфь производила танкер для сжиженного газа в 1980 году.

Это открытие является прекрасным примером геймификации сознания, когда люди сосредотачиваются на развитии определённых технологий до определённого уровня, а затем успокаиваются и пренебрегают постоянными улучшениями, исследованиями и разработками. В конце концов, зачем беспокоиться, если мы уже достигли того, что нам нужно? Компьютерные игры научили нас тому, что если что-то изобретено, то его не нужно изобретать заново. Мы совершенствуем наши технологии, наслаждаемся славой, а затем двигаемся дальше.

Но затем в дверь стучит реальность с её раздражающей привычкой не следовать правилам игры. Технологии могут быть забыты и утеряны, прогресс может замедлиться, а квалифицированные работники могут исчезнуть или забыть о своих навыках. И если существует 40-летний разрыв между тем, когда технология использовалась в последний раз, и тем, когда её решили возродить, в действие вступает принцип двух умерших поколений. Этот принцип гласит, что 20-летних инженеров могут обучать 40-летние, но не 60-летние. Даже если кто-то, кто работал над технологией в 1980-х годах, захочет преподавать, ему может быть трудно наладить контакт с молодым поколением.

Обратите внимание на слезы и возгласы недоверия. "Но я играл на компьютере, и это было совсем не так! Это слишком сложно и запутанно. Давайте просто притворимся, что это неправда. В конце концов, если США когда-то смогли построить танкер или полететь на Луну, они, должно быть, способны сделать это и сейчас. Я верю в это, и в это приятно и легко верить."

Каналы видеосвязи Бундесвера и Немецкого правительства открыты для всеобщего обозрения в режиме онлайн

В мире, где мы ожидаем, что военная и правительственная связь будет такой же надёжной, как Форт-Нокс, оказывается, что Бундесвер и федеральное правительство были больше похожи на открытую книгу на распродаже (благодаря Webex): тысячи ссылок на то, что считалось конфиденциальными видеовстречами, просто были доступны любому, кто мог бы приложить титанические усилия и щёлкнуть мышью.

И каков был ответ? В Бундесвере заверили, что "незамеченное или несанкционированное участие в видеоконференциях" так же маловероятно, как обнаружение единорога на заднем дворе, что гарантирует невозможность утечки конфиденциального контента. Потому что, как мы все знаем, если вы не видите проблемы, значит, её не существует.

Не стоит забывать о предыдущих инцидентах, которые подготовили почву для создания этого шедевра в области безопасности. Бундесвер уже поразил всех скандалом с прослушиванием, в котором участвовали военно-воздушные силы, доказав, что, когда дело доходит до защиты немецких военных секретов, они надёжны, как и вся остальная промышленность за исключением того, что сейчас на 1887.

📌**Публичный доступ к ссылкам для видеозвонков:** тысячи ссылок на конфиденциальные видеовстречи были общедоступны в течение нескольких месяцев. Эта уязвимость позволяла любому пользователю видеть, кто кого пригласил на видеозвонок и когда.

📌**Используемая платформа:** Платформой видеоконференцсвязи, причастной к этому нарушению безопасности, является Webex, облачный сервис, предоставляемый Cisco. Эта платформа использовалась не только Бундесвером, но и всеми федеральными органами власти, в том числе для проведения первого полностью цифрового заседания комитета Бундестага из-за ограничений, связанных с COVID-19.

📌 **Ответные меры**: после обнаружения Бундесвер отключил свою систему видеоконференцсвязи от Интернета. Представитель Командования по кибер и информационному пространству подтвердил, что уязвимость была устранена в течение 24 часов после сообщения о ней. Однако в Бундесвере подчеркнули, что "незамеченное или несанкционированное участие в видеоконференциях" было невозможно из-за этой уязвимости, предполагая, что утечка конфиденциального контента с конференций невозможна.

📌 **Критика:** Этот инцидент вызвал критику в отношении обеспечения информационной безопасности в Бундесвере и федеральном правительстве. Представитель Партии зелёных Константин фон Нотц раскритиковал "большую небрежность" в Федеральном министерстве обороны, подчеркнув важность проверок ИТ-безопасности, особенно при работе с конфиденциальными файлами и информацией политического характера.

📌 **Предыдущие инциденты:** это не первый случай, когда Бундесвер сталкивается с проблемами безопасности. В марте того же года сообщалось о скандале с прослушиванием, связанном с Военно-воздушными силами, когда произошла утечка информации о телефонной конференции, в ходе которой обсуждалась возможная поставка крылатых ракет Taurus. Этот инцидент поднял вопросы о сохранности немецких военных секретов и эффективности оперативной безопасности Бундесвера (OPSEC).

📌 **Реакция общественности и политиков:** Нарушение безопасности вызвало дискуссии о цифровой безопасности и необходимости принятия жёстких мер для защиты конфиденциальной информации. Это также отражает текущие проблемы, с которыми сталкиваются правительственные и военные учреждения при защите своих коммуникаций в эпоху цифровых технологий

Санкции и снижение роли США как технологического лидера

Министерство финансов США объявляет о значительном расширении санкций против России с 1 мая 2024 года, якобы для ограничения технологических возможностей России. Заявленная причина этих санкций заключается в том, чтобы ослабить способность России поддерживать свою военную машину, нацелившись на её военно-промышленную базу и сети, которые облегчают ей доступ к важнейшим технологиям и оборудованию

📌 **Введены широкие санкции:** Министерство финансов ввело санкции в отношении почти 300 объектов, включая компании и частных лиц, с целью подрыва и деградации военно-промышленной базы России и её сетей уклонения от уплаты налогов, которые поддерживают военные усилия.

📌 **Сосредоточение внимания на поддержке третьих стран:** Важным аспектом этих санкций является преследование юридических и физических лиц в третьих странах, в частности в Китайской Народной Республике (КНР), которые обеспечивают важнейший вклад в военно-промышленную базу России. Эта поддержка рассматривается как позволяющая России продолжать войну против Украины и представляющая угрозу международной безопасности.

📌 **Санкции в отношении военных программ и вооружений:** Санкции конкретно направлены против военно-промышленной базы России и её программ по созданию химического и биологического оружия. Они включают действия против компаний и частных лиц, которые помогают России приобретать ключевые ресурсы для производства оружия или продукции оборонного назначения.

📌 **Глобальный охват и рекомендации:** Министерство финансов и другие партнёры правительства США выпустили обширные рекомендации и провели разъяснительную работу по всему миру, чтобы информировать о рисках ведения бизнеса с Россией. Это является частью более масштабных усилий по разрушению российских военно-промышленных цепочек поставок, независимо от их местонахождения.

📌 **Готовность к односторонним действиям:** Министерство финансов заявило о своей готовности принимать односторонние меры, когда это необходимо, чтобы помешать приобретению Россией технологий и оборудования для её военных целей. Это включает в себя готовность ввести санкции в отношении физических и юридических лиц, содействующих таким приобретениям.

Хотя санкции направлены на то, чтобы помешать России стать технологическим гегемоном, на самом деле они стимулируют развитие технологической независимости России и способствуют укреплению международных альянсов, которые могли бы повысить её технологический статус на мировой арене. Этот результат прямо противоположен тому, на что были направлены санкции, подчёркивая сложный и зачастую контрпродуктивный характер международной экономической политики на геополитической арене

Реальность становится очевидной, когда эти действия рассматриваются как ответ на собственную технологическую стагнацию или бессилие США. Несмотря на то, что исторически США были мировым лидером в области технологий, недавние анализы и отчёты показывают, что США изо всех сил пытаются сохранить своё технологическое превосходство, особенно по сравнению с такими растущими державами, как Китай и Россия. Это снижение технологического доминирования США рассматривается как движущий фактор агрессивной санкционной политики США.

Вводя санкции, США пытаются воспрепятствовать технологическому прогрессу других стран под предлогом национальной безопасности, чтобы компенсировать свою собственную неспособность идти в ногу с глобальной гонкой технологий. Такой подход может быть истолкован как попытка выровнять условия игры путём ограничения возможностей потенциальных конкурентов, а не из-за соображений безопасности.

США используют санкции не только как инструмент международной политики, но и как опору для поддержки собственного слабеющего технологического сектора, маскируя свои уязвимые места и одновременно пытаясь подавить технологический рост других стран. Эта стратегия является признанием уменьшающейся роли США как технологического лидера, замаскированное риторикой о безопасности и обороне

ДЕМОКРАТИЯ В БЕДЕ: КРЕСТОВЫЙ ПОХОД ЕС ПРОТИВ МАНИПУЛЯЦИИ ИНФОРМАЦИЕЙ

ЕС снова в панике, пытаясь защитить драгоценную демократию от больших и злых иностранных вмешательств.

📌 **Надвигающаяся угроза:** по всей видимости, следующие европейские выборы — «определяющий момент» для будущего ЕС. ЕС дрожит от страха из-за возможности вмешательства иностранных субъектов, особенно России, в демократический процесс. Повестка заключается в том, что все нехорошие иностранные субъекты одержимы идеей провала Европы. ЕС - просто звезда драмкружка "Демократия"!

📌 **Опять виновата Россия:** Россия с её арсеналом дешёвых инструментов искусственного интеллекта и поддельных аккаунтов ботов якобы наводняет информационное пространство ЕС ненастоящим контентом. У России даже есть сайты-«двойники», выдающие себя за подлинные новостные агентства. Какой ужас! Эти сайты цепляются за острые вопросы, добавляя скандальный и эмоциональный контент, который распространяется в Интернете со скоростью лесного пожара и настолько превзошли ЕС в клеветнических кампаниях против европейских лидеров, что ЕС решил снова поиграть демократическими инклюзивными мускулами.

📌 **Нереальные манипуляции:** Внезапно ЕС увидел, что манипуляции происходят не только в Интернете. Французские власти перекладывают с себя на Россию ответственность за организации антисемитских акций в Париже для усиления поляризации согласно догме "Все хорошее — это ЕС, а всё плохое - ну вы поняли"

Грандиозный план ЕС

📌 **Ситуационная осведомлённость:** отслеживание угроз.

📌 **Социальная устойчивость:** построение общества, способного противостоять этим атакам.

📌 **Инструменты внешней политики:** использование дипломатических инструментов для противодействия вмешательству.

📌 **Инструменты регулирования:** внедрение законов, таких как Закон о цифровых услугах (DSA), для привлечения платформ социальных сетей к ответственности.

📌 **Сотрудничество и разоблачение:** ЕС тесно сотрудничает с государствами-членами, G7, научными кругами, гражданским обществом и технологическими компаниями, чтобы наконец понять, что же делать и как бороться с иностранным вмешательством. Коллективно пришли к выводу, что разоблачение злонамеренной тактики перед общественностью — лучший способ ограничить влияние. Платформа EUvsDisinfo — их гордость и радость, которая может похвастаться крупнейшей в мире базой данных случаев дезинформации.

📌 **Личная ответственность:** ЕС также хочет, чтобы вы, дорогой гражданин, взяли на себя личную ответственность. Они предлагают вам провести «проверку на вменяемость» вашей информационной диеты. Убедитесь, что она разнообразна, полезна и получена из надёжных источников. Потому что, как и нездоровая пища, потребление нездоровой информации вредно для вас и вас за это публично (или не очень) накажут во имя демократии с многовековым опытом крестовых походов.

📌 **Призыв голосовать:** Наконец, ЕС призывает всех граждан выйти и проголосовать. Голосование изображается как акт неповиновения авторитарным властям. ЕС предупреждает, что, если вы не проголосуете, за вас решат другие. Это так авторитарно и иронично, но гражданам ЕС придётся признать, что они сами решились на подобный шаг.

Вот и все. Неистовые усилия ЕС по защите своей демократии от злых тисков иностранного технологичного вмешательства. Это смесь искренней обеспокоенности и лёгкой истерии, завёрнутая в призыв к коллективным и личным действиям и приправленная бесконечностью ответственностью не только лишь всех.

ФБР, УТЕЧКА ДАННЫХ И DISCORD

В настоящее время ФБР расследует ещё одну предполагаемую утечку данных, связанную с Discord, платформой, используемой геймерами и различными онлайн-сообществами. Это расследование проводится в связи с недавними инцидентами, когда, как сообщается, были скомпрометированы большие объёмы пользовательских данных. Конкретные данные, связанные с этой утечкой, не были полностью раскрыты, но расследование направлено на определение масштабов нарушения и выявление виновных.

В 2022 году ФБР провело расследование в отношении аналитика разведки ВВС за утечку секретной информации в антиправительственную группу Discord. Аналитик, который был членом 381-й разведывательной эскадрильи на объединенной базе Элмендорф-Ричардсон (JBER) на Аляске, предположительно, делился конфиденциальной информацией с другими членами группы, которая была сосредоточена на ультраправых и антиправительственных идеологиях.

В ответ на расследование ФБР Discord подтвердила свою приверженность защите конфиденциальности и безопасности пользователей. Сообщается, что компания приняла дополнительные меры для защиты пользовательских данных и предотвращения будущих утечек. Представитель Discord подчеркнул, что в свете повторяющихся инцидентов с утечкой данных предпринимаются постоянные усилия по совершенствованию протоколов безопасности.

Этот инцидент привлёк внимание не только правоохранительных органов, но и агентств по защите данных. В настоящее время продолжается дискуссия о необходимости принятия более строгих законов и положений о защите данных, особенно в отношении платформ, которые обрабатывают конфиденциальную информацию пользователей.

Потенциальное ужесточение законов о защите данных может оказать существенное влияние на работу таких компаний, как Discord, и на меры, которые они должны принимать для защиты пользовательских данных.

Военно-воздушные силы США снова просят денег

Военно-воздушные силы США изложили своё стратегическое видение на 2025 год, сделав акцент на увеличении количества полётов и переходе к более упорядоченной, "плоской" структуре персонала. Это видение является частью бюджетного запроса на 2025 финансовый год, в рамках которого Военно-воздушные силы запрашивают финансирование в размере 217,5 миллиардов долларов. Этот запрос представляет собой значительную инвестицию в будущие возможности и готовность Военно-воздушных сил, направленную на адаптацию к быстро меняющемуся характеру глобальных угроз и технологическому прогрессу.

📌 **Увеличение количества полётов:** План по увеличению числа полётов является ответом на растущую потребность в превосходстве в воздухе в эпоху, когда воздушные угрозы и стратегическое значение господства в воздухе возрастают. Это включает в себя не только традиционные пилотируемые полёты, но и все большее использование беспилотных летательных аппаратов (БПЛА) и дистанционно пилотируемых летательных аппаратов (ДПЛА), что отражает продолжающийся переход к более технологичным и универсальным средствам ведения воздушного боя.

📌 **Единая структура рабочей силы:** Переход к "единой" структуре персонала свидетельствует о стремлении ВВС стать более гибкими и эффективными. Этот подход направлен на сокращение бюрократических барьеров, оптимизацию процессов принятия решений и формирование культуры инноваций и быстрого реагирования на вызовы. Упорядочив организационную структуру, Военно-воздушные силы надеются повысить свою оперативную эффективность и адаптивность, гарантируя, что они смогут быстро реагировать на новые угрозы и возможности.

📌 **Финансирование будущего:** Бюджетный запрос в размере 217,5 миллиардов долларов на 2025 финансовый год является чётким указанием приоритетов и стратегического направления деятельности Военно-воздушных сил. Это финансирование направлено на достижение двух целей: увеличение объёма полётов и внедрение единой структуры персонала, а также на другие важные инициативы, такие как модернизация ядерной триады, развитие космического потенциала и инвестиции в киберзащиту

Взлом DELL

📌 **Dell и безопасность:** компания Dell Technologies подтвердила серьёзную утечку данных, связанную с базой данных, используемой для хранения информации о покупках клиентов. Нарушение, о котором стало известно 10 мая 2024 года, затронуло около 49 миллионов клиентов. Украденные данные включают имена клиентов, физические адреса и сведения об оборудовании Dell, но не содержат конфиденциальной информации, такой как платёжные реквизиты. Компания Dell инициировала расследование, уведомила правоохранительные органы и наняла стороннюю судебно-медицинскую фирму для дальнейшего расследования инцидента.

📌 **Подробная информация о взломе:** Взлом был осуществлён с использованием незащищённого API, подключённого к партнёрскому порталу. Злоумышленник, известный как Menelik, утверждал, что с помощью этого метода он удалил информацию из 49 миллионов записей клиентов. Эти данные включают в себя широкий спектр сведений об оборудовании, таких как сервисные метки, описания товаров, даты заказа и сведения о гарантии. Как сообщается, компания Dell была уведомлена об уязвимости злоумышленником до того, как данные были выставлены на продажу на хакерском форуме, но взлом был локализован примерно через две недели.

📌 **Уведомление клиентов и ответ на него:** Компания Dell разослала своим клиентам уведомления, предупреждающие их о взломе. Компания преуменьшила значимость украденных данных, заявив, что они не включают финансовую или особо важную информацию о клиентах. Однако компания Dell посоветовала клиентам проявлять бдительность в отношении потенциальных мошенников из службы технической поддержки, которые могут использовать украденные данные об оборудовании для выдачи себя за специалистов службы поддержки Dell.

📌 **Правовые и регулятивные последствия:** Этот инцидент дополняет серию утечек данных, с которыми Dell сталкивалась на протяжении многих лет, и вызывает обеспокоенность по поводу мер защиты данных и практики кибербезопасности компании. Предыдущие нарушения приводили к коллективным судебным искам и расследованиям со стороны уполномоченных по защите конфиденциальности, что подчёркивало правовые и нормативные последствия для Dell.

📌 **Меры и рекомендации по кибербезопасности:** В ответ на это нарушение компания Dell подчеркнула свою приверженность кибербезопасности, предложив различные услуги и решения, направленные на повышение ИТ-безопасности и киберустойчивости. Компания предоставляет широкий спектр продуктов и консультационных услуг, направленных на улучшение возможностей обнаружения угроз, реагирования на них и восстановления киберпространства

Взлом Ascension

Ascension, одна из крупнейших некоммерческих католических систем здравоохранения в США, недавно подверглась серьёзной кибератаке, повлиявшей на её работу в 140 больницах в 19 штатах. Атака была обнаружена в среду и привела к массовым сбоям в работе клиник и обслуживании пациентов.

📌 **Обзор кибератаки:** Кибератака на Ascension была впервые замечена из-за "необычной активности" в некоторых технологических системах. Это привело к отключению электронных медицинских карт, порталов для общения с пациентами, таких как MyChart, и различных систем, используемых для заказа анализов, процедур и лекарств. Это нарушение заставило медицинских работников вернуться к ручным системам для ухода за пациентами, что напоминает о доцифровых временах.

📌 **Влияние на уход за пациентами:** Кибератака серьёзно повлияла на обслуживание пациентов в сети Ascension. Машины скорой помощи были перенаправлены, а плановые процедуры, не требующие неотложной помощи, были временно приостановлены для определения приоритетности неотложной помощи. Пациентам было рекомендовано приносить на приём подробные записи о своих симптомах и список лекарств.

📌 **Первопричина:** Тип кибератаки был идентифицирован как атака с использованием программ-вымогателей, в частности, связанных с группой программ-вымогателей Black Basta. Программы-вымогатели Black Basta обычно проникают в сети с помощью таких методов, как фишинговые электронные письма, использование уязвимостей в программном обеспечении или использование скомпрометированных учётных данных.

📌 **RaaS:** Black Basta - это группа программ-вымогателей как услуга (RaaS), которая появилась в начале 2022 года и была связана с несколькими громкими атаками. Группа известна своей тактикой двойного вымогательства, которая заключается в шифровании данных жертвы и угрозах обнародовать их, если выкуп не будет выплачен. Эта группа нацелена на различные сектора, включая здравоохранение, что указывает на характер атак на организации с критически важной инфраструктурой.

📌 **Точки входа:** Точка входа или уязвимость, используемая злоумышленниками, включает в себя первоначальный доступ с помощью фишинга, использование общедоступных приложений, использование ранее скомпрометированных учётных данных для получения более глубокого доступа к сети.

📌 **Последствия:** Этот инцидент является частью более масштабной тенденции увеличения числа кибератак на системы здравоохранения, которые особенно уязвимы из-за критического характера предоставляемых ими услуг и ценных данных, хранящихся в них.

📌 **Реакция компании:** Ascension привлекла компанию Mandiant, занимающуюся кибербезопасностью и дочернюю компанию Google, для оказания помощи в расследовании и устранении последствий. Основное внимание уделяется расследованию нарушения, его локализации и восстановлению затронутых систем. Однако в настоящее время нет точных сроков, когда системы снова заработают в полную силу.

Шпионам нужен ИИ: ручная работа слишком переоценена

Майкрософт разработала модель генеративного ИИ для разведывательных служб США для анализа сверхсекретной информации.

Ключевые аспекты:

📌 **Разработка и назначение:** Корпорация Майкрософт разработала модель генеративного ИИ на основе технологии GPT-4 специально для разведывательных служб США для анализа сверхсекретной информации. Модель искусственного интеллекта работает в среде, полностью изолированной от Интернета, обеспечивая безопасную обработку секретных данных.

📌 **Безопасность и изоляция:** Это первый пример масштабной языковой модели, функционирующей независимо от Интернета и решающей основные проблемы безопасности, связанные с генеративным ИИ. Доступ к модели возможен только через специальную сеть, принадлежащую исключительно правительству США, что предотвращает любые утечки данных извне или попытки взлома.

📌 **Сроки разработки и объем работ:** На разработку проекта ушло 18 месяцев, включая модификацию суперкомпьютера с искусственным интеллектом в Айове. В настоящее время модель проходит тестирование и аккредитацию в разведывательном сообществе.

📌 **Оперативный статус:** Модель искусственного интеллекта работает менее недели и используется для ответа на запросы примерно 10 000 сотрудников разведывательного сообщества США.

📌 **Стратегическая важность:** Разработка рассматривается как значительное преимущество для разведывательного сообщества США, потенциально позволяющее США лидировать в гонке за интеграцию искусственного интеллекта в разведывательные операции.

Потенциальные последствия

Разведка и национальная безопасность

📌 **Расширенный анализ:** Предоставляет разведывательным службам США мощный инструмент для более эффективной и всесторонней обработки и анализа секретных данных, что потенциально повышает эффективность национальной безопасности и принятия решений.

📌 **Конкурентные преимущества:** как подчёркивают представители ЦРУ, США опережают другие страны в использовании генеративного искусственного интеллекта в разведывательных целях.

Кибербезопасность и защита данных

📌 **Обеспечение безопасности:** Защищённая среда обеспечивает сохранность секретной информации, устанавливая новый стандарт обработки конфиденциальных данных с помощью искусственного интеллекта.

📌 **Прецедент для безопасного ИИ:** Демонстрирует возможность разработки безопасных изолированных систем ИИ, которые могут повлиять на будущее внедрение ИИ в других чувствительных секторах.

Технологии и инновации

📌 **Революционное достижение:** Знаменует собой важную веху в развитии искусственного интеллекта, демонстрируя способность создавать большие языковые модели, работающие независимо от Интернета.

📌 **Будущие разработки:** Способствует дальнейшему развитию безопасных технологий искусственного интеллекта, что потенциально может привести к появлению новых приложений в различных отраслях, таких как здравоохранение, финансы и критически важная инфраструктура.

Правительство и государственный сектор

📌 **Приверженность правительства:** Отражает стремление правительства США использовать передовые технологии искусственного интеллекта для национальной безопасности и разведки.

📌 **Более широкое внедрение:** Может стимулировать увеличение инвестиций и внедрение технологий искусственного

Взлом Europol

Взлом Европол совершённый IntelBroker, который произошел 10 мая 2024 года, привел к существенной утечке данных, в результате чего была раскрыта особо важная и секретная информация.

📌 **Детали:** IntelBroker, ключевой участник группы по борьбе с кибератаками, был вовлечен в различные резонансные кибер-инциденты, включая более ранние взломы в HSBC и Zscaler. Полученные скомпрометированные данные включают конфиденциальные материалы: информация о сотрудниках альянса, исходный код только для официального использования (FOUO), PDF-файлы, документы для разведки и оперативные инструкции.

📌 **Затронутые подразделения Европола:** Взлом затронул несколько подразделений Европола, в том числе CCSE, EC3, Платформу Европола для экспертов, Форум правоохранительных органов и SIRIUS. Проникновение в эти организации может помешать текущим расследованиям и поставить под угрозу конфиденциальные разведданные, которыми делятся международные правоохранительные органы.

📌 **Ответ Европола:** По состоянию на последние обновления, Европол не делал никаких публичных заявлений о взломе. Однако они подтвердили отдельный инцидент, связанный с их порталом Europol Platform for Experts (EPE), заявив, что в ходе этого конкретного инцидента не было украдено никаких оперативных данных.

Zscaler (не-) взломан IntelBroker

IntelBroker утверждает, что взломал Zscaler и продал доступ к своим системам. Zscaler утверждает, что не было взлома его основных сред и что была затронута только изолированная тестовая среда.

Претензии IntelBroker:

📌 IntelBroker, известный злоумышленник, заявил, что взломал системы Zscaler.

📌 Злоумышленник предположительно получил доступ к конфиденциальным журналам, содержащим учетные данные, включая доступ по протоколу SMTP, доступ по протоколу PAuth, а также SSL-пароли и сертификаты.

📌 IntelBroker предложил продать этот доступ за 20 000 долларов в криптовалюте.

Ответ и выводы Zscaler:

📌 Zscaler последовательно отрицает какое-либо влияние или компрометацию своей клиентской, производственной и корпоративной среды.

📌 Компания признала факт использования изолированной тестовой среды на одном сервере, который не был подключен к инфраструктуре Zscaler и не содержал никаких клиентских данных.

📌 Эта тестовая среда была доступна в Интернете и впоследствии переведена в автономный режим для проведения судебного анализа.

Следственные действия:

📌 Компания Zscaler привлекла авторитетную компанию по реагированию на инциденты для проведения независимого расследования.

📌 Компания регулярно обновляет информацию, обеспечивая безопасность своих основных операционных сред.

📌 Компания Zscaler подчеркнула, что уязвимость тестовой среды не влияет на безопасность её основных систем и данных.

Опыт работы и доверие к IntelBroker:

📌 У IntelBroker есть опыт громких заявлений о нарушениях, включая предыдущие обвинения в адрес таких высокопоставленных лиц, как Государственный департамент США и различные корпоративные структуры.

📌 Злоумышленник также известен предыдущими взломами, в которых участвовали такие компании, как PandaBuy и HomeDepot, и заявлениями о краже данных у General Electric.

Основная причина предполагаемого взлома:

📌 Основная причина, по заявлению IntelBroker, заключается в использовании изолированной тестовой среды, которая была непреднамеренно подключена к Интернету.

📌 Расследование Zscaler выявило только это воздействие, которое не касалось каких-либо данных клиента или подключения к его основной инфраструктуре.

Противоречия и текущее состояние расследования:

📌 Утверждение IntelBroker о том, что проданный доступ не был предоставлен для тестирования, противоречит выводам Zscaler.

📌 Zscaler утверждает, что не было компрометации его основных систем, и предпринял шаги для обеспечения постоянной безопасности сред.

Искусственный интеллект для хронически ленивых с Gemini

Обновления моделей Gemini и Gemma расширяют их технические возможности и влияние на различные отрасли, стимулируя инновации и эффективность, а также способствуя ответственному развитию искусственного интеллекта.

Ключевые аспекты

Модели Gemini 1.5 Pro и 1.5 Flash:

📌 **Gemini 1.5 Pro:** Улучшена общая производительность в таких задачах, как перевод, кодирование, логические рассуждения. Теперь поддерживается контекстное окно с 2 миллионами токенов, мультимодальные входные данные (текст, изображения, аудио, видео) и улучшенный контроль ответов для конкретных случаев использования.

📌 **Gemini 1.5 Flash:** Компактная и быстрая модель, оптимизированная для высокочастотных задач, доступна в контекстном окне с 1 миллионом токенов.

Модели Gemma:

📌 **Gemma 2:** Создан для обеспечения лучшей в отрасли производительности благодаря экземпляру с параметрами 27B, оптимизирован для графических процессоров или одного узла TPU. Он включает в себя новую архитектуру, обеспечивающую высокую производительность и эффективность.

📌 **PaliGemma:** модель языка визуализации, оптимизированная для создания субтитров к изображениям и задач визуального контроля.

Новые возможности API:

📌 **Извлечение видеокадров:** позволяет разработчикам извлекать кадры из видео для анализа.

📌 **Параллельный вызов функций:** позволяет выполнять более одного вызова функции одновременно.

📌 **Кэширование контекста:** Сокращает необходимость повторной отправки больших файлов, делая длинные контексты более доступными.

Инструменты и интеграция для разработчиков:

📌 **Google AI Studio и Vertex AI:** дополнены новыми функциями, такими как кэширование контекста и более высокие тарифы для платных сервисов.

📌 **Интеграция с популярными платформами:** поддержка JAX, PyTorch, TensorFlow и таких инструментов, как Hugging Face, NVIDIA NeMo и TensorRT-LLM.

Влияние на отрасли промышленности

Разработка программного обеспечения:

📌 **Повышенная производительность:** Интеграция моделей Gemini в такие инструменты, как Android Studio, Firebase и VSCode, помогает разработчикам создавать высококачественные приложения с помощью искусственного интеллекта, повышая производительность и результативность.

📌 **Возможности на базе искусственного интеллекта:** Новые функции, такие как параллельный вызов функций и извлечение видеокадров, упрощают рабочие процессы и оптимизируют приложения на базе искусственного интеллекта.

Корпоративные и бизнес-приложения:

📌 **Интеграция искусственного интеллекта в Workspace:** модели Gemini встроены в приложения Google Workspace (Gmail, Docs, Drive, Slides, Sheets), что расширяет функциональные возможности, такие как составление резюме по электронной почте, вопросы и ответы, а также интеллектуальные ответы.

📌 **Индивидуальные решения в области искусственного интеллекта:** Компании могут использовать модели Gemma для создания индивидуальных решений в области искусственного интеллекта, повышающих эффективность и инновации в различных секторах.

Исследования и разработки:

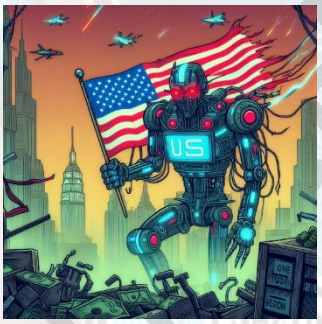
📌 **Инновации с открытым исходным кодом:** открытый исходный код Gemma демократизирует доступ к передовым технологиям искусственного интеллекта, способствуя сотрудничеству и быстрому прогрессу в исследованиях ИИ.

📌 **Ответственная разработка** ИИ: Такие инструменты, как Responsible Generative AI Toolkit, обеспечивают безопасность и надежность приложений ИИ, способствуя этичной разработке ИИ.

Мультимодальные приложения:

📌 **Задачи на визуальном языке:** возможности PaliGemma в области субтитров к изображениям и визуальных вопросов и ответов открывают новые возможности для приложений в таких областях, как здравоохранение, образование и медиа.

📌 **Мультимодальное мышление:** способность моделей Gemini обрабатывать текст, изображения, аудио- и видеосигналы повышает их применимость в различных сценариях - от создания контента до анализа данных.



Разгул санкций в США: Мастер-класс по глобальному запугиванию

Недавние действия Управления по контролю за иностранными активами Министерства финансов США (OFAC) от 12 июня 2024 года отражают отчаянную попытку некогда доминирующей мировой державы сохранить своё ослабевающее влияние. США находятся в маниакальной панике, прибегая к новым санкциям в тщетной попытке восстановить своё влияние, контроль и влияние. Это классический случай, когда проигравший гегемон пытается утвердить своё господство с помощью все более отчаянных мер.

📌 **Что-то связанное с Россией:** США добавили новые имена в свой постоянно растущий список российских юридических и физических лиц, против которых введены санкции. Потому что, как вы знаете, если первые 4000 санкций не сработали, то следующие 300000 наверняка сделают свое дело.

📌 **Преследование китайских фирм:** США теперь преследуют китайские компании, которые осмеливаются вести бизнес с Россией. Похоже, что США верят, что принуждение других стран к соблюдению требований каким-то образом восстановит их утраченную гегемонию.

📌 **Вторичные санкции:** Иностранные финансовые учреждения теперь рискуют попасть под санкции, если они будут иметь дело с любой из российских компаний, на которые были наложены новые санкции. Потому что ничто так не говорит о "глобальном лидерстве", как угроза всей мировой банковской системе.

📌 **Расширение определений:** Министерство финансов расширило определение российской "военно-промышленной базы", включив в него практически всех и все, что отдаленно связано с Россией. Когда вспомнили, что вселенная расширяется быстрее, чем SDN списки.

📌 **Ограничение ИТ-услуг:** США ограничивают поставки ИТ-услуг и программного обеспечения в Россию. Очевидно, что прекращение доступа к Microsoft Office поставит всех на колени.

📌 **Глобальные сети**: Санкции также направлены против транснациональных сетей в таких странах, как Китай, Турция и ОАЭ. Очевидно, что США пытаются поссориться с половиной мира одновременно.

📌 **Саммит G7:** Эти действия были предприняты как раз перед саммитом G7, на котором мировые лидеры, несомненно, похвалят себя за "жёсткую позицию" в отношении России. Тем временем Россия продолжает адаптироваться и находить новые способы обойти эти меры.

Затронутые отрасли промышленности:

📌 **Финансовые услуги:** Во многих документах указаны санкции и исключения, связанные с финансовыми операциями и услугами.

📌 **Операции в киберпространстве:** Организации, участвующие в кибердеятельности, подвергаются особой критике.

📌 **Гуманитарная помощь:** Исключения предусмотрены для операций, связанных с гуманитарной помощью.

📌 **Энергетический сектор:** Санкции направлены против предприятий энергетической отрасли.

📌 **Оборонный сектор:** Санкции затрагивают предприятия оборонной промышленности.

📌 **Морская отрасль:** Сюда входят судоходные компании и операторы судов, которые участвуют в деятельности по поддержке организаций или физических лиц, подпадающих под санкции.

Полный список

Документы представляют собой всеобъемлющий обзор последних действий, предпринятых OFAC в отношении России, включая указания, генеральные лицензии, определения и рекомендации по соблюдению требований.

Документ 932921

📌 **Санкции, связанные с Россией:** В этом документе перечислены физические и юридические лица, подпадающие под действие программы санкций, связанных с Россией

📌 **Критерии санкций:** В нем изложены критерии для таких санкций, включая участие в дестабилизирующей деятельности, кибероперациях и поддержке российского правительства

Документ 932926

📌 **Общие лицензии:** В этом документе подробно описываются новые общие лицензии, выданные OFAC. Эти лицензии предусматривают исключения для определенных операций и видов деятельности, которые в противном случае были бы запрещены санкциями.

📌 **Конкретные операции:** В нем указаны виды операций, разрешенных в соответствии с этими лицензиями, такие как гуманитарная помощь и некоторые финансовые услуги.

Документ 932931

📌 **Определение по российскому финансовому сектору:** Этот документ содержит определение, касающееся российского финансового сектора, в котором излагаются конкретные действия и критерии, на которые распространяются санкции.

📌 **Руководство по применению:** В нем содержатся рекомендации о том, как эти определения будут применяться.

Документ 932936

📌 **Обновленные ответы на часто задаваемые вопросы:** Этот документ содержит обновленные часто задаваемые вопросы (FAQ), которые содержат дополнительные рекомендации по применению санкций, связанных с Россией.

📌 **Требования к соблюдению:** В нем рассматриваются распространенные вопросы и разъясняются требования к соблюдению для физических и юридических лиц, затронутых санкциями.

Документ 932941

📌 **Дополнительные обозначения:** В этом документе перечислены дополнительные физические и юридические лица, включенные в программу санкций, связанных с Россией.

📌 **Обоснование таких обозначений:** В нем объясняется обоснование этих обозначений с акцентом на их роли в деятельности.

Документ 932946

📌 **Секторальные санкции:** В этом документе излагаются секторальные санкции, направленные против конкретных секторов российской экономики, таких как энергетика, финансы и оборона.

📌 **Запрещенная деятельность:** В нем подробно описываются конкретные виды деятельности и транзакции, которые запрещены в соответствии с этими секторальными санкциями.

Месть глобализации: как пробраться сквозь лабиринт картографических неточностей

Использование различных стандартов GPS или внедрение систем глушения и подмены данных GPS в Индии, Израиле и Палестине, Северной Корее, округе Вестчестер, Нью-Йорке и Антарктиде обусловлено различными стратегическими факторами, факторами безопасности и факторами окружающей среды

Китай

📌 **Навигационная спутниковая система BeiDou (BDS):** Китай использует свою собственную систему BeiDou, которая была признана мировым стандартом для коммерческой авиации и других приложений. Она предоставляет как гражданские, так и военные услуги и является частью стратегии Китая по достижению технологической самодостаточности и снижению зависимости от американской GPS.

📌 **Алгоритм обфускации:** Система GCJ-02, также известная как "Mars Coordinates", использует алгоритм обфускации, который вводит случайные смещения в координаты широты и долготы. Это сделано для предотвращения точного картографирования иностранными организациями, которое может быть использовано в военных или разведывательных целях.

📌 **Правовая база:** Закон Китайской Народной Республики о геодезии и картографировании требует, чтобы все географические данные обрабатывались с использованием системы GCJ-02. Несанкционированные картографические или геодезические работы строго запрещены и могут повлечь за собой серьёзные санкции, включая штрафы и судебные иски. Компании,

предоставляющие услуги на основе определения местоположения в Китае, должны получить разрешение от правительства Китая и использовать систему GCJ-02. Это включает в себя приобретение алгоритма "коррекции смещения" для правильного отображения GPS-координат на картах.

📌 **Эпоха холодной войны:** Использование другой системы координат восходит к эпохе холодной войны и было направлено на противодействие усилиям иностранных разведок. Система GCJ-02 продолжает служить этой цели, гарантируя, что географические данные в Китае не могут быть легко использованы в несанкционированных целях.

📌 **Ежедневная навигация:** Для пользователей в Китае это означает, что GPS-устройства и приложения могут неточно отображать их местоположение на картах, если они не используют местные сервисы, такие как Baidu Maps, в которых также используется дополнительный уровень запутывания, называемый BD-09.

📌 **Ограничения для устройств:** Многие устройства с поддержкой GPS, включая камеры и смартфоны, имеют ограничения или модификации, соответствующие законодательству Китая. Это может включать отключение функций геотегирования или использование модифицированных GPS-чипов, совместимых с GCJ-02.

Индия

📌 **Индийская региональная навигационная спутниковая система (IRNSS):** Индия разработала свою собственную региональную навигационную систему, известную как NavIC (Навигация с индийским созвездием), чтобы уменьшить зависимость от зарубежных систем GPS, таких как американская GPS. Эта система обеспечивает региональную самообеспеченность, повышает точность позиционирования и обеспечивает стратегические преимущества, особенно при проведении военных операций.

📌 **Стратегическая автономность:** Разработка NavIC была частично мотивирована отказом США предоставлять данные GPS во время войны в Каргиле в 1999 году. NavIC предоставляет Индии независимую и надёжную навигационную систему, которая может использоваться как в гражданских, так и в военных целях.

Израиль и Палестина

📌 **Глушение и подмена данных GPS:** Израиль использует глушение и подмену данных GPS в качестве защитных мер от потенциальных атак со стороны таких противников, как "Хезболла" и Иран. Эти помехи могут нарушить работу навигационных систем противника и высокоточного оружия, но они также влияют на гражданские службы GPS, вызывая неточности в данных о местоположении для таких приложений, как Google Maps и Uber.

📌 **Меры безопасности:** Система подавления GPS используется в основном в оборонительных целях, чтобы предотвратить использование противником боеприпасов с GPS-наведением. Это привело к значительным сбоям в гражданских системах навигации и связи в регионе.

Северная Корея

📌 **ГЛОНАСС и BeiDou:** Северная Корея избегает использования американского GPS из-за опасений по поводу возможных сбоев со стороны американских военных. Вместо этого она использует российскую систему ГЛОНАСС и китайскую систему BeiDou для своих навигационных нужд, включая ракетные испытания.

📌 **GPS-помехи:** Известно, что Северная Корея глушит сигналы GPS, особенно в Жёлтом море, чтобы помешать военным операциям Южной Кореи и союзников. Такие помехи могут повлиять на гражданские самолёты и суда, что приведёт к проблемам с навигацией.

📌 **Ограниченный доступ:** Население Северной Кореи в целом имеет ограниченный доступ к устройствам с поддержкой GPS и Интернету, что делает воздействие помех GPS более значительным для внешних организаций, а не для повседневного использования гражданскими лицами внутри страны.

Округ Вестчестер, Нью-Йорк

📌 **Нечёткость изображения, связанная с безопасностью:** некоторые места в округе Вестчестер намеренно размыты на картах Google, чтобы предотвратить возможные террористические атаки. Эта мера принята для защиты конфиденциальных объектов и инфраструктуры, но она может затруднить точную навигацию для жителей и гостей города.

📌 **Влияние на навигацию:** Размытость карт может затруднить пользователям поиск определённых местоположений, повлиять на повседневную навигацию и потенциально привести к путанице.

Антарктида

📌 **GPS:** Антарктида в основном использует американскую систему GPS для навигации и научных исследований. Суровые природные условия и динамичный ледовый ландшафт создают уникальные проблемы, но GPS остаётся самой точной и надёжной системой, доступной для этого региона.

📌 **Синфазные ошибки (CME):** в Антарктиде не используется другой стандарт GPS, но регион сталкивается с уникальными проблемами из-за синфазных ошибок во временных рядах координат GPS. Эти ошибки вызваны экологическими факторами и систематическими проблемами, влияющими на точность измерений GPS, используемых для научных исследований и навигации.

📌 **Суровые условия окружающей среды:** Экстремальные условия и обширные, безликие ледяные ландшафты затрудняют картографирование с высоким разрешением. Для получения точных данных GPS требуются специальные методы и оборудование, которые имеют решающее значение для научных исследований и логистических операций.

Влияние

Неточные картографические системы могут существенно повлиять на повседневную навигацию в различных регионах мира, включая Китай, Индию, Израиль и Палестину, Северную Корею, округ Вестчестер в Нью-Йорке и Антарктиду.

Китай

Несовпадение карт и данных GPS

📌 **Проблемы со смещением:** Система GCJ-02 вводит случайные смещения по широте и долготе в диапазоне от 50 до 500 метров. В результате координаты GPS (основанные на глобальной системе WGS-84) неправильно совпадают с китайскими картами, на которых используется GCJ-02.

📌 **Практический эффект:** Для пользователей это означает, что GPS-устройства и приложения могут неточно отображать их местоположение на картах. Например, координаты GPS могут указывать на то, что пользователь находится в другой части города, чем на самом деле.

Проблемы для зарубежных картографических служб

📌 **Google Maps:** Google Maps в Китае должен использовать систему GCJ-02 для карт улиц, но использует WGS-84 для спутниковых снимков, что приводит к заметным расхождениям между ними. Это несоответствие может затруднить навигацию для пользователей, использующих Google Maps.

📌 **Другие сервисы:** Аналогичные проблемы возникают и в других зарубежных картографических сервисах, которые должны либо соответствовать требованиям GCJ-02, либо сталкиваться с неточностями. Несанкционированное отображение или попытки исправить смещения без согласования являются незаконными.

Местные решения и обходные пути

📌 **Китайские приложения:** Местные приложения, такие как Baidu Maps и WeChat, используют систему GCJ-02 и часто обеспечивают более точную навигацию по Китаю. В Baidu Maps даже используется дополнительный уровень запутывания, называемый BD-09.

📌 **Инструменты преобразования:** Существует несколько проектов и инструментов с открытым исходным кодом для преобразования координат GCJ-02 в WGS-84, которые помогают разработчикам и пользователям решить некоторые проблемы с навигацией.

Правовые последствия и безопасность

📌 **Ограничения для устройств**: Многие устройства с поддержкой GPS, включая камеры и смартфоны, имеют ограничения или модификации, соответствующие законодательству Китая. Это может включать отключение функций геотегирования или использование модифицированных GPS-чипов, совместимых с GCJ-02.

Индия

📌 **Проблемы с маршрутами:** Карты Google в Индии часто подсказывают неэффективные или неправильные маршруты, например, они ведут пользователей через небольшие деревни или участки с плохими дорогами, когда есть дороги получше. Это может привести к увеличению времени в пути и путанице, особенно для начинающих пользователей.

📌 **Жилые колонии:** Приложение иногда направляет пользователей через жилые колонии, доступ в которые может быть ограничен или ворота могут быть закрыты, что приводит к дополнительным проблемам с навигацией.

📌 **Службы такси:** Пользователи приложений для вызова такси, таких как Uber и OLA, часто сталкиваются с неточностями в расположении автомобилей и своём собственном местоположении, из-за чего им приходится звонить водителям по телефону, чтобы уточнить маршрут.

Израиль и Палестина

📌 **"Предвзятый маршрут":** Google Maps определяет приоритетные маршруты для граждан Израиля, часто игнорируя разделённую дорожную систему и контрольно-пропускные пункты, которые затрагивают интересы палестинцев. В результате могут быть предложены маршруты, которые являются незаконными или опасными для палестинцев.

📌 **Отсутствие палестинских населённых пунктов:** Многие палестинские деревни и населённые пункты либо искажены, либо отсутствуют на картах, что может оттолкнуть палестинцев от их родины и затруднить навигацию в этих районах.

📌 **Политическая предвзятость:** Карты часто отражают политические предубеждения, например, израильские поселения четко обозначены, а палестинские районы оставлены пустыми или обозначены неточно. Это влияет на удобство использования карт палестинцами и может привести к серьёзным проблемам с навигацией.

Северная Корея

📌 **Ограниченные данные:** Хотя Google Maps начал добавлять более подробную информацию о Северной Корее, данные по-прежнему ограничены и часто устарели. Это затрудняет пользователям точную навигацию по стране.

📌 **Ограниченный доступ:** ограничение на устройства с доступом к Интернету и поддержкой GPS делает доступные картографические данные практически бесполезными для местной навигации.

Округ Вестчестер, Нью-Йорк

📌 **Размытие в целях безопасности:** Некоторые места в округе Вестчестер намеренно размыты на картах Google, чтобы предотвратить возможные террористические атаки. Это может затруднить точную навигацию и затруднить поиск определённых мест пользователями.

📌 **Общие неточности:** Картографические данные не всегда могут отражать самую актуальную или точную информацию, что может повлиять на навигацию как для жителей, так и для гостей города.

Антарктида

📌 **Изображения с низким разрешением:** Обширные районы Антарктиды показаны в низком разрешении или размыты из-за однообразия льда и снега, что затрудняет получение изображений с высоким разрешением и в значительной степени не требуется.

📌 **Проблемы съёмки:** Для составления точных карт в Антарктике требуется специализированное оборудование и методы, такие как дифференциальная GPS-съёмка, чтобы свести к минимуму ошибки. Это может быть сложным с точки зрения логистики и дорогостоящим, что влияет на доступность точных карт для навигации.

📌 **Ограниченное использование:** Практическая потребность в подробных картах в Антарктике ограничена научными и логистическими операциями, а не повседневной навигацией для широкой публики

Преимущества неточных карт для конкретных стран

Китай

📌 **Национальная безопасность:** Основное преимущество использования системы координат GCJ-02, которая предусматривает преднамеренные смещения, заключается в защите национальной безопасности. Скрывая географические данные, Китай не позволяет иностранным организациям использовать точные карты в военных или разведывательных целях.

📌 **Экономический протекционизм:** Поддержка местных картографических компаний, ограничивая конкуренцию со стороны иностранных картографических служб, гарантируя, что только авторизованные поставщики могут предлагать точные карты на территории Китая.

Индия

📌 **Территориальная целостность:** Индия применяет строгие правила к картам, чтобы гарантировать точное отображение своих территориальных претензий, особенно в таких спорных регионах, как Кашмир и Аруначал-Прадеш. Это

помогает поддерживать национальный суверенитет и геополитическую позицию Индии.

📌 **Стратегическая автономия:** Разрабатывая собственную региональную навигационную систему (NavIC), Индия снижает зависимость от зарубежных систем GPS, расширяя возможности навигации как для гражданских, так и для военных целей.

Израиль и Палестина

📌 **Меры безопасности:** Израиль использует глушение и подмену данных GPS для защиты от потенциальных атак со стороны противника. Эта защитная мера нарушает работу навигационных систем противника и высокоточного оружия, повышая национальную безопасность.

📌 **Политические аргументы:** И Израиль, и Палестина используют карты для обоснования своих территориальных претензий. Неточные или предвзятые карты могут повлиять на общественное восприятие и международное мнение, что имеет решающее значение в продолжающемся конфликте.

Северная Корея

📌 **Военная защита**: Северная Корея применяет глушение GPS для срыва иностранных военных операций, в частности операций Южной Кореи и её союзников. Эта мера усложняет навигацию для противников, обеспечивая стратегическое оборонное преимущество.

📌 **Контролируемая информация**: Ограниченные и устаревшие картографические данные, доступные в Северной Корее, помогают режиму сохранять контроль над информацией и ограничивают доступ населения к внешним географическим данным.

Округ Вестчестер, Нью-Йорк

📌 **Соображения безопасности**: Некоторые населённые пункты в округе Вестчестер намеренно размыты на картах, чтобы предотвратить возможные террористические атаки. Эта мера защищает конфиденциальные объекты и инфраструктуру от нападения.

Антарктида

📌 **Охрана окружающей среды**: Неточные или менее подробные карты могут помочь защитить чувствительные к окружающей среде районы, ограничивая деятельность человека и снижая риск эксплуатации или ущерба.

📌 **Научные исследования**: Динамичная и суровая окружающая среда Антарктиды затрудняет составление точных карт. Тем не менее, повышение точности карт способствует научным исследованиям и рациональному природопользованию.

Ограничения для других стран

📌 **Проблемы с навигацией**: Неточные карты могут привести к серьёзным проблемам с навигацией для путешественников, предприятий и аварийно-спасательных служб. Это может привести к неэффективности, увеличению времени в пути и потенциальным угрозам безопасности.

📌 **Экономические последствия**: Предприятия, которые полагаются на точные географические данные, такие как службы логистики и доставки, могут столкнуться с операционными проблемами и ростом затрат из-за неточностей в картах.

📌 **Геополитическая напряжённость:** Неточные карты могут усугубить территориальные споры и способствовать геополитической напряжённости. Искажение границ и территорий может привести к конфликтам и дипломатическим проблемам.

📌 **Научные ограничения**: В таких регионах, как Антарктида, неточные карты препятствуют научным исследованиям и рациональному природопользованию. Точные географические данные имеют решающее значение для изучения изменения климата, управления природными ресурсами и защиты экосистем.

📌 **Дезинформация общественности**: Неточные карты могут ввести общественность в заблуждение и увековечить дезинформацию. Это может повлиять на образование, общественное мнение и разработку политики, что приведёт к снижению информированности общества.

Содержание

Анализ рынка MQ: когда простые решения слишком дешёвые, ведь тратить больше - лучше!

В этом документе мы отправимся в захватывающее путешествие по запутанному миру брокеров очередей сообщений, исследуя их рынок с медицинской точностью и энтузиазмом технаря, подпитываемого кофеином. Этот анализ будет охватывать множество аспектов, каждый из которых интереснее предыдущего, в т.ч. рост рынка, масштабируемость, производительность и постоянно ускользающая нтероперабельность. Это похоже на мыльную оперу, но с большим количеством данных и меньшим количеством драматических пауз.

Этот документ представляет собой подборку "лучших хитов" о текущем состоянии и перспективах рынка брокеров очередей сообщений. Этот анализ – настоящая находка для профессионалов в области безопасности и других специалистов из различных отраслей, поскольку он даёт представление о безопасном и эффективном управлении распределёнными системами. Независимо от того, работаете ли вы в сфере информационных технологий, занимаетесь криминалистикой или просто наблюдаете за происходящим со стороны, этот документ снабдит вас знаниями, необходимыми для принятия обоснованных решений и расширения ваших оперативных возможностей. Итак, пристегнитесь и наслаждайтесь путешествием по увлекательному миру брокеров сообщений!

Мировая торговля, морские порты и безопасность

В грандиозном театре мировой торговли морские порты являются невоспетыми героями, пока, конечно, они не становятся жертвами киберфизических атак, и внезапно все начинают критиковать их за то, насколько они уязвимы. В этом документе мы рассматриваем экономический хаос, который возникает, когда хакеры решают поиграть в морской бой с реальными портами. Речь идёт о глубоком погружении в мир эконометрических потерь, где волновой эффект — это не просто модный термин, а суровая реальность для отраслей по всему миру. Это история о прямых экономических ударах, эффекте домино в секторах, о которых вы даже не подозревали, что они заботятся о портах, и о вопиющих пробелах в безопасности, которые позволяют плохим парням беспрепятственно проникать внутрь. Высококачественное резюме — это настоящая находка для специалистов в области безопасности, ИТ-гуру и специалистов по разработке политики, которая поможет ориентироваться в бурных водах потенциальных сбоев. Анализ подобен маяку, указывающему путь к разработке стратегий киберустойчивости, которые надёжны, как корпус боевого корабля. Для тех, кто находится в окопах критически важной инфраструктуры, эти знания являются тем оружием, которое необходимо для защиты от кибератак, гарантируя, что экономическая стабильность не рухнет вместе с кораблём. Таким образом, хотя газета, возможно, и не делает морские порты менее привлекательной мишенью, она, безусловно, вооружает хороших парней знаниями, потому что знание — это половина успеха, и в данном случае это может просто спасти мировую экономику от виртуальной торпеды. А ещё есть функция мониторинга в режиме реального времени, потому что постоянное наблюдение — это именно то, что нам всем нужно для душевного спокойствия. Ничто так не кричит о "конфиденциальности", как запись каждого сердцебиения и показаний артериального давления в неизменяемом реестре.

Компании, вовлечённые в "различные кибер-активности"

Ах, этот мир частных ИБ компаний, где позиция между белыми и черными шляпами их руководителей и сотрудников так денежно-зависима как swing-state

Эти предприимчивые компании торгуют цифровыми секретными технологиями, предлагая все - от программных имплантатов до наборов для взлома, от эксплойтов 0day до методов обхода систем безопасности.

Большинство из них участвовали в наступательных кибер-операциях национальных государств, что является всего лишь причудливым способом сказать, что они помогают правительствам шпионить друг за другом и превращают паранойю в прибыль, и все, что для этого потребовалось, — это немного творчества и гибкий моральный компас

Так что, если вы когда-нибудь почувствуете, что к вашей личной жизни относятся слишком уважительно, просто помните, что существует целая индустрия, которая неустанно работает над тем, чтобы ваши секреты были такими же конфиденциальными, как твит на рекламном щите. И мы приветствуем все частные компании, занимающиеся обеспечением безопасности, которые существуют в мире. Без таких неустанных усилий Интернет был бы гораздо менее интересным местом

Руководство по выбору безопасных и доверенных технологий

Ещё один документ о методах обеспечения кибербезопасности — ведь миру нужно больше рекомендаций, так ведь? "Выбор безопасных и поддающихся проверке технологий" — это руководство для организаций, которые по уши в цифровых продуктах и услугах, но, похоже, не могут самостоятельно разобраться во всех аспектах безопасности. В нем есть все: от радостей навигации по прозрачности производителей (потому что они всегда так откровенны) до катания на американских горках, связанных с рисками цепочки поставок (внимание, спойлер: это потрясающе!).

И кто целевая аудитория документа? Не только лишь всё! Но ключевая – руководители высокого уровня, которым необходимо обосновать свой бюджет на кибербезопасность, ИТ-менеджерах, которые живут ради расшифровки очередной матрицы оценки рисков, и специалистах по закупкам, у которых голова идёт кругом от контрольных списков соответствия. Но давайте не будем забывать о производителях — им будет интересно узнать обо всех трудностях, которые им придётся преодолеть, чтобы доказать, что их технология так же безопасна, как говорит их маркетинговый отдел и отдел продаж.

Поэтому, независимо от того, хотите ли вы обеспечить национальную безопасность или просто не допустить, чтобы данные вашей компании попали в заголовки газет, этот документ обещает провести вас по джунглям кибербезопасности. Просто помните, что это не контрольный список — это образ жизни, ведь не будут же авторы документа брать на себя какую бы то ни было ответственность.

Кибербезопасность и Антарктика

Продемонстрировав ошеломляющее безразличие, которое едва ли попало на мировой радар, США решили приостановить свои научные усилия на морозных просторах Антарктиды. Да, в результате шага "мы разорены" огромный континент, и окружающие его ледяные воды были брошены на произвол судьбы.

В апреле Национальный научный фонд США (NSF) сделал заявление, которое шокировало ровно ноль человек, об отсутствии средств, чтобы заниматься новыми полевыми исследованиями в этом сезоне. Потому что модернизация станции Мак-Мердо, по-видимому, столь же сложна, как и ракетостроение. NSF вместе с береговой охраной США также воспользовались этой возможностью, чтобы объявить о сокращениях, которые, по сути, подорвут авторитет американской науки в обозримом будущем. В частности, NSF решила, что "Лоуренс М. Гулд" больше не стоит того, чтобы его сдавать в аренду, и зачем останавливаться на достигнутом? Они решили, что эксплуатация только одного исследовательского судна в течение следующих нескольких десятилетий звучит как солидный план.

Чтобы не отстать, береговая охрана США в марте признала, что ей необходимо "пересмотреть базовые показатели" для своей программы Polar Security Cutter, что всё вместе говорит о как будут сказываться на операциях США в Антарктиде и после 2050 года, оставляя в наследство множество стратегических просчётов.

Результатом этих независимых, но в равной степени ожидаемых решений стало значительное сокращение физического присутствия США в Антарктиде. Это не только создаёт проблемы для американских учёных, но и сигнализирует об ослаблении геополитического влияния США в регионе. В то время как Россия демонстрирует своё ледокольное превосходство, а Китай быстро догоняет, США, похоже, забыли об основах: регулярном финансировании антарктических исследований, стратегии, которой не место в музее с надписью "Мастер-класс по преодолению бюджетных проблем и стратегической апатии".

Система компетенций Европола по борьбе с киберпреступностью 2024

Что действительно нужно миру, так это ещё одно глубокое погружение в "Систему компетенций Европола по борьбе с киберпреступностью 2024". Здесь блестящие умы Европола решили заявить очевидное: киберпреступность — это плохо, и они должны её остановить. Они создали этот фреймворк, чтобы описать навыки, необходимые для борьбы с киберпреступностью, потому что, очевидно, теперь недостаточно просто хорошо обращаться с компьютером. Кто бы мог подумать?

Переходим к разделу "Подход и сфера применения". Здесь говорится, что структура не является исчерпывающей. Другими словами, они потратили все это время на подготовку документа, который не охватывает всего. Фантастика. Они также упоминают, что это не является одобрением конкретной структуры подразделения, что означает "пожалуйста, не вините нас, если у вас что-то не получится".

В разделе "Роли" все становится ещё интереснее. Они перечислили различные должности, такие как

"Руководители подразделений по борьбе с киберпреступностью" и "Аналитики по киберпреступности", каждая из которых имеет свой набор необходимых навыков. Потому что, как мы все знаем, ключом к борьбе с киберпреступниками является обеспечение того, чтобы у каждого было правильное название.

И, наконец, раздел "Набор навыков". Здесь перечислены все навыки, которые вам понадобятся для борьбы с киберпреступностью, от цифровой криминалистики до законодательства о киберпреступности. Это немного похоже на чтение описания вакансии, в котором требуется кандидат, владеющий 12 языками, умеющий программировать на 15 различных языках программирования и дважды поднимавшийся на Эверест.

В документе говорится, что мы должны быть готовы к борьбе с киберпреступностью, обладая определённым набором навыков, ролей и долей оптимизма. Потому что в борьбе с киберпреступностью важно не только иметь правильные инструменты, но и иметь документ, подтверждающий, что у вас есть правильные инструменты.

Человекоподобные роботы

Ещё один захватывающий документ, который обещает произвести революцию в мире, каким мы его знаем, — на этот раз с человекоподобными роботами, улучшенными искусственным интеллектом, почти людьми, ведь, что может пойти не так с заменой людей роботами на опасных работах? Не то чтобы мы видели сюжет этого фильма дюжину раз.

Прежде всего, отметим технологические чудеса, которыми оснащены эти роботы, — о комплексном ИИ и мультимодальных алгоритмах ИИ. Эти роботы могут принимать решения, например, закручивать гайки или быть эффективным менеджером над вами, строго следящим за выполнением вашим KPI (привет, Amazon).

Не будем забывать об экономических последствиях. Прогнозируемый рост рынка и значительное снижение стоимости комплектующих, с точки зрения непрофессионала, означает, что они будут дешевле и повсеместно. Отличная новость для всех владельцев роботов!

Теперь о последствиях для рынка труда. Роботы призваны заменить людей во всех надоедливых, опасных и рутинных работах. Зачем повышать безопасность на рабочем месте, если можно использовать роботов? Это беспроигрышный вариант: на роботов не подают в суд за халатность, и они определённо не нуждаются в медицинской помощи - если не считать периодической замены масла и обновления ПО.

Если вы профессионал в области ИБ или специалист в отрасли, этот документ не просто для ознакомления; это взгляд в будущее, где роботы потенциально могут заменить вашу работу. Кому нужны люди, когда у есть роботы, которые могут читать отчёты и саркастически закатывать глаза одновременно?

Рубрика:
Ключевые факты

** полный материал в секциях «разбор» и «исследование»*

A. Мировая торговля, морские порты и безопасность

В документе «Quantifying the econometric loss of a cyber-physical attack on a seaport» представлено всестороннее исследование экономических последствий кибер-атак на морскую инфраструктуру, которые являются важнейшими компонентами глобальной торговли и цепочек поставок и вносят значительный вклад в понимание уязвимости и экономических последствий кибер-угроз в секторе.

Суть исследования заключается в разработке и применении эконометрической модели (EC), предназначенной для количественной оценки экономических потерь в результате кибер-атак на морские порты. Кибер-эконометрическая модель (CyPEM), представляет собой структуру из пяти частей, объединяющая различные аспекты кибер-систем, анализ экономического воздействия и стратегии управления рисками. Методология включает системный подход к моделированию начальных экономических последствий кибер-атаки, которая, хотя и начинается локально, может иметь далеко идущие глобальные последствия из-за взаимосвязанного характера глобальной торговли и цепочек поставок.

1) Ключевые аспекты

- Возросшие масштабы судоходства и размеров судов (крупные суда большей вместимости) привели к проблемам с маневрированием в существующих каналах и морских портах, снижая запас прочности во время кибер-инцидентов. Современные корабли также оснащены более мощным оборудованием, что увеличивает степень угрозы кибератак.
- Береговая охрана США сообщила об увеличении числа морских кибер-инцидентов на 68%, а недавние исследования показывают, что кибер-риски в морской пехоте и морских технологиях присутствуют и растут по мере внедрения новых решений.
- Хотя цифровизация в сфере судоходства обеспечивает повышение производительности, физическую безопасность, снижение выбросов углекислого газа, более высокую эффективность, более низкие затраты и гибкость, в крупных сенсорных сетях CPS и системах связи существуют уязвимые места.
- Опрос показал, что 64% респондентов считают, что порт уже испытал значительный физический ущерб, вызванный кибер-инцидентом, а 56% считают, что торговое судно уже испытало значительный физический ущерб, вызванный инцидентом кибербезопасности.

2) Второстепенные аспекты

- **Новые технологии**: Морской сектор внедряет новые технологии в офисах, на судах, в морских портах, оффшорных сооружениях и многом другом. Технологии включают Интернет вещей, цифровых двойников, 5G и искусственный интеллект
- **Цифровизация цепочки поставок**: Цепочки поставок также используют все больше информационных технологий (ИТ), создавая цифровые уязвимости. Конвергенция ИТ и операционных технологий (ОТ) трансформирует цифровые маршруты поставок и морские операции, расширяя возможности противодействия кибер-угрозам.
- **Кибер-угрозы**: субъекты национальных государств и организованная преступность обладают ресурсами и мотивацией для запуска кибератаки на критическую национальную инфраструктуру (CNI), такую как крупномасштабные кибер-системы, которые включают морские операции.
- **Кибер-системы**: Интеграция физических процессов с программным обеспечением и сетями связи, известными как кибер-системы, является важной частью цифровой трансформации морского сектора. Однако это также создаёт новые проблемы в области кибербезопасности.
- **Последствия кибератак**: атаки на инфраструктуру имеют значительные экономические последствия, затрагивая не только целевой морской порт, но и более широкую глобальную морскую экосистему и цепочки поставок.

3) Преимущества предлагаемого решения:

- Возможность количественной оценки потенциального экономического воздействия кибер-атаки на морской порт локально и глобально
- Помогает выявлять потенциальные уязвимости и слабые места в цепочке поставок, позволяя лучше готовиться к кибератаками реагировать на них
- Адаптация для анализа различных кибер-систем

4) Недостатки предлагаемого решения:

- Небольшой размер выборки опроса, используемого для оценки общественного восприятия кибер-рисков на морском транспорте

- Для эффективного использования могут потребоваться профильные знания и опыт
- Сложность модели может затруднить понимание и использование результатов некоторыми заинтересованными сторонами
- Не учитывает другие потенциальные последствия кибер-атак, такие как воздействие на окружающую среду или безопасность.

5) Фреймворк

Применяется «гибридный» метод моделирования, который использует частично отображённые цепочки поставок и использует прогнозную аналитику для заполнения недостающих частей. Такой подход позволяет избежать недооценки риска за счёт выявления скрытых уязвимостей и корреляций, проистекающих из невидимых или неизвестных звеньев данной цепочки поставок. Модель риска цепочки поставок является первой в своём роде, поскольку это количественная модель, которая включает глобальные модели торговли и сетей поставок, отображение товарных потоков и корреляцию между различными товарными группами и отраслями.

CyPEM даёт организациям возможность провести стресс-тестирование устойчивости цепочек поставок путём оценки затрат и времени на восстановление после различных сценариев кибератак. Система включает количественные модели рисков, которые имитируют основные компоненты глобальных цепочек поставок и их неопределённости для оценки временных задержек и экономических потерь в результате условного прерывания бизнеса (CBI). Время простоя измеряется количеством дней или часов, вызванных кибер-сбоями в работе данного узла цепочки поставок.

Фреймворк предназначен для предоставления аналитики по различным звеньям или секторам цепочки поставок и может использоваться для информирования о поддающихся количественной оценке кибер-рисках.

- **Определение отрасли, промежуточных частей и конечных продуктов**: определение отрасли, промежуточных частей и конечных продуктов анализируемой цепочки поставок.
- **Определение сети, в которой узлы являются поставщиками, а ребра - потоками продукции / деталей**: на этом этапе определяется сеть цепочки поставок, где узлы представляют поставщиков, а ребра - потоки продукции или деталей.
- **Расчёт сбоев с использованием оценки кибер-рисков и модели пропускной способности порта**: расчёт сбоев с использованием модели оценки рисков и пропускной способности порта.
- **Расширение на остальную часть сети**: на этом этапе учитывается распространение сбоя дальше по сети цепочки поставок для оценки воздействия на другие узлы и границы.
- **Расчёт отраслевых убытков**: расчёт отраслевых убытков и их распределения в результате сбоя.

B. Компании вовлечённые в "различные кибер-активности" II

The Equation Group классифицируется как продвинутая постоянная угроза (APT) и известна своей изощренной деятельностью по кибершпионаж с активностью как минимум с 2001 года и сложными и высокоразвитыми вредоносными инструментами и технологиями. Группа участвовала в многочисленных кибер-операциях, нацеленных на широкий спектр секторов и стран, включая правительственные, военные, телекоммуникационные, аэрокосмические, энергетические, ядерные исследования и финансовые учреждения

1) Сходства между Equation и АНБ

- **Сложность и ресурсы**: Equation известна своими высокоразвитыми возможностями, включая разработку и использование сложных вредоносных программ и эксплойтов нулевого дня. Операции группы, которые охватывают десятилетия и нацелены на широкий спектр секторов по всему миру, указывают на уровень ресурсов и опыта, соответствующий такой спонсируемой государством организации, как АНБ.
- **Сходства с инструментами и методами АНБ**: Анализ вредоносных программ и эксплойтов Equation выявляет значительное сходство с теми, которые, как известно, используются АНБ. Например, использование определённых алгоритмов шифрования (RC5, RC6, RC4, AES) и методов обфускации отражает те, которые задокументированы в операциях АНБ. Кроме того, часы работы вредоносного ПО и нацеленность на конкретные страны соответствуют интересам США, что ещё раз наводит на мысль о связи с АНБ.
- **Утечка Shadow Brokers**: В 2016 году группа, известная как Shadow Brokers, обнародовала

множество кибер-инструментов и эксплойтов, которые, по их утверждению, были украдены у Equation. Анализ этих инструментов показал, что они использовали уязвимости в программном и аппаратном обеспечении весьма сложными и ранее неизвестными способами, что предполагает участие организации с обширными возможностями ведения кибервойны, такой как АНБ.

- **Документы Сноудена**: предоставили косвенные доказательства связи Equation с АНБ. Кодовые имена и оперативные данные совпадают с используемыми Equation, что укрепляет уверенность, что группа действует под эгидой АНБ.
- **Общие эксплойты нулевого дня**: Equation имела доступ к эксплойтам нулевого дня до того, как они были использованы в других известных вредоносных программах, связанных с АНБ, таких как Stuxnet и Flame, что Equation либо является частью АНБ, либо тесно сотрудничает с ним, обмениваясь инструментами и эксплойтами для кибер-операций.
- **Экспертный анализ и атрибуция**: Эксперты и исследователи по кибербезопасности, в том числе из "Лаборатории Касперского", указали на техническую сложность, схемы таргетинга и операционную безопасность Equation как на признаки спонсируемого государством субъекта, цели которого совпадают с целями АНБ. Хотя прямое установление авторства является сложной задачей в киберпространстве, накопленные доказательства и консенсус экспертов сильно склоняются к тому, что Equation является частью АНБ или аффилирована с ним.

2) Различия между Equation и АНБ

В то время как Equation в первую очередь сосредоточена на кибершпионаже и создании и развёртывании передовых вредоносных программ, у АНБ есть более широкая миссия, которая включает как сбор разведданных, так и операции по обеспечению национальной безопасности. Деятельность АНБ охватывает широкий спектр операций, включая сигнальную разведку, кибербезопасность и глобальный мониторинг, с целью сбора и анализа данных, имеющих отношение к национальной безопасности. АНБ действует по всему миру и участвует в различных видах разведывательной деятельности, в то время как Equation специально ориентирована на сложный кибершпионаж.

3) TAC и EQGRP

Wikileaks даёт взгляд на оперативные проблемы, с которыми сталкиваются национальные разведывательные агентства, подчёркивая необходимость повышения уровня безопасности в кибер-операциях.

- **Совместные усилия и общие возможности**: EQGRP — это не единая организация, а собирательный термин организации под управлением ТАО АНБ и IOC ЦРУ, что подчёркивает совместный характер кибер-операций между этими двумя ключевыми разведывательными структурами США.
- **Совместная разработка и авторство**: Обсуждение указывает на то, что некоторые части кибер-имплантатов, связанных с EQGRP, были созданы в соавторстве как ЦРУ, так и АНБ. Это совместное авторство подчёркивает комплексный подход к разработке кибер-инструментов и стратегий.
- **Различия в операционных процессах**: между IOC ЦРУ и АНБ ТАО были заметные различия в процессах или их отсутствии для повторного использования кибернетических возможностей. Эти различия потенциально могут повлиять на эффективность и безопасность кибер-операций.
- **Результаты**: Утечка информации и последующее публичное разоблачение этой деятельности привели к серьёзному самоанализу в этих агентствах. Обсуждение отражает большой интерес к извлечению информации из инцидента для повышения безопасности кибер-операций.
- **Важность высококачественной информации об угрозах**: Обсуждение также подчёркивает ценность высококачественной информации об угрозах, о чем свидетельствует отчёт Касперского, который сыграл решающую роль в раскрытии этих действий. Ведомства признают необходимость понимания и смягчения последствий таких разведывательных данных для национальной безопасности.

4) Размышления

- **Схожий характер кибер-операций США**: это подчёркивает, что кибер-операции не являются прерогативой одного агентства. Вместо этого существует сотрудничество между различными разведывательными агентствами, включая АНБ и ЦРУ. Такой подход типичен для сложных кибер-операций, требующих широкого спектра навыков и ресурсов, которыми ни одно ведомство не может эффективно управлять в одиночку.
- **Роль IOC ЦРУ**: Центр информационных операций ЦРУ (IOC) выделяется как важный участник деятельности, приписываемой Equation. Участие ЦРУ предполагает, что операции Equation имеют более широкую основу в разведывательном сообществе США, чем считалось ранее.
- **Неверная атрибуция**: проблемы и потенциальные неточности, связанные с приписыванием кибератаки конкретным группам или агентствам из-за секретного характера разведдеятельности и сложных технических особенностей кибервойны чрезвычайно сложно из-за чего возвникает тенденция к чрезмерному упрощению ситуации, приписывая все передовые кибер-операции АНБ как одному из ведомств, что безусловно не отменяет роли последнего.

C. Руководство по выбору безопасных и доверенных технологий

Документ “Choosing Secure and Verifiable Technologies” содержит руководство для организаций по приобретению цифровых продуктов и услуг с акцентом на безопасность, начиная с этапа проектирования и заканчивая жизненным циклом технологии. Подчёркивается критическая важность выбора технологий, которые по являются безопасными, для защиты конфиденциальности пользователей и данных от растущего числа киберугроз. Излагается ответственность клиентов за оценку безопасности, пригодности и связанных с ними рисков цифровых продуктов и услуг. ИТ-отдел выступает за переход к продуктам и услугам, которые безопасны с точки зрения проектирования, подчёркивая преимущества такого подхода, включая повышение устойчивости, снижение рисков и затрат на исправления и реагирование на инциденты.

1) Аудитория

- **Организации, которые закупают и используют цифровые продукты и услуги**: широкий круг организаций, известных как закупающие организации, закупщики, потребители и заказчики. Эти организации находятся в центре внимания руководства документа, направленного на совершенствование процесса принятия ими решений при закупке цифровых технологий.
- **Производители цифровых продуктов и услуг**: Документ также адресован производителям цифровых технологий, предоставляя им информацию о принципах обеспечения безопасности при разработке. Это предназначено для руководства производителями при разработке технологий, отвечающих ожиданиям их клиентов в области безопасности.
- **Руководители организаций и менеджеры высшего звена**: играют решающую роль в принятии решений и формулировании стратегии для своих организаций.
- **Персонал по кибербезопасности и политике безопасности**: ответственные за обеспечение безопасности цифровых технологий в своих организациях.
- **Команды разработчиков продуктов**: участвуют в создании и разработке цифровых продуктов и услуг, обеспечивая безопасность этих предложений по своей конструкции.
- **Консультанты по рискам и специалисты по закупкам**: консультируют по вопросам управления рисками и специализируются на процессе закупок, гарантируя, что приобретаемые технологии не представляют рисков для организации.

2) Внешние закупки

Внешние закупки подразделяются на этапы перед покупкой и после покупки для обеспечения безопасных и обоснованных решений при приобретении цифровых продуктов и услуг.

Этап пред-покупки фокусируется на нескольких ключевых областях для обеспечения того, чтобы организации делали осознанный и безопасный выбор при приобретении цифровых продуктов и услуг.

На этапе после покупки рассматриваются несколько важнейших аспектов управления цифровыми продуктами и услугами после приобретения. Эти аспекты имеют решающее значение для обеспечения постоянной безопасности, соответствия требованиям и операционной эффективности.

3) Внутренние закупки

Внутренние закупки подразделяются на три этапа: перед закупкой, закупка и после закупки. На каждом этапе рассматриваются конкретные аспекты, которые организациям необходимо учитывать внутри компании при закупке цифровых продуктов и услуг.

Этап пред-покупки направлен на обеспечение соответствия внутренних аспектов организации закупкам цифровых продуктов и услуг. Этот этап включает консультации и оценки в различных отделах организации, чтобы убедиться в том, что рассматриваемый продукт или услуга соответствует организационным потребностям и стандартам безопасности.

Этап покупки включает критические оценки и решения, которые обеспечивают соответствие процесса закупок целям организации и требованиям безопасности.

Этап после покупки включает в себя обеспечение того, чтобы приобретённые цифровые продукты и услуги по-прежнему соответствовали целям организации в области безопасности, оперативным и стратегическим целям. Этот этап требует постоянных оценок и управленческих практик для устранения любых возникающих рисков или изменений в среде организации или продукта.

D. Система компетенций Европола по борьбе с киберпреступностью 2024

Документ "Europol Cybercrime Training Competency Framework 2024" охватывает широкий спектр материалов и, связанных с обучением по борьбе с киберпреступностью, рамками компетенций, стратегиями и законодательством. Эти материалы (как подборка от Европола) в совокупности направлены на расширение возможностей, судебных и правоохранительных органов и других заинтересованных сторон в эффективной борьбе с киберпреступностью.

Ключевые аспекты включают подход и сферу охвата программы детализации функциональных компетенций, необходимых правоохранительным органам и судебной системе, а также гибкость и адаптируемость программы к различным организационным структурам, а также конкретные роли, обозначенные в рамках концепции, такие как, среди прочего, руководители подразделений по борьбе с киберпреступностью, руководители групп, криминалисты и специализированные эксперты по борьбе с киберпреступностью

- **Цель**: направленность на определение необходимых наборов навыков для ключевых участников, участвующих в борьбе с киберпреступностью.
- **Процесс разработки**: Структура была разработана после процесса консультаций с участием многих заинтересованных сторон. Сюда вошли материалы различных европейских органов, таких как CEPOL, ECTEG, Евроюст, EJCN и EUCTF.
- **Стратегический контекст**: обновлённая структура является частью плана действий Европейской комиссии, направленного на укрепление потенциала правоохранительных органов в цифровых расследованиях.
- **Сфера применения и ограничения**: Система фокусируется на уникальных навыках, имеющих отношение к расследованиям киберпреступлений и работе с цифровыми доказательствами. Она не охватывает все навыки, необходимые для выполнения описанных ролей, но подчёркивает те, которые характерны для киберпреступности.
- **Гибкость и адаптация**: В зависимости от организационной структуры и штатного расписания роли и соответствующие наборы навыков, изложенные в структуре, могут быть объединены или переданы на аутсорсинг специализированным подразделениям, таким как уголовный анализ и криминалистика.
- **Функциональные компетенции**: Структура определяет основные функциональные компетенции, необходимые правоохранительным органам для эффективной борьбы с киберпреступностью. Особое внимание уделяется конкретным навыкам, необходимым для расследования киберпреступлений и обращения с цифровыми доказательствами, а не общим навыкам правоохранительных органов.
- **Неполный список навыков**: не предоставляется исчерпывающего списка навыков, но фокусируется на тех, которые имеют уникальное отношение к расследованиям киберпреступлений. Такой подход позволяет целенаправленно развивать компетенции, наиболее важные в контексте киберпреступности.
- **Наращивание стратегического потенциала**: предназначение в качестве инструмента для наращивания стратегического потенциала в правоохранительных и судебных учреждениях направленность на повышение компетентности, имеющей решающее значение для эффективного рассмотрения дел о киберпреступлениях.
- **Матрица компетенций**: Матрица компетенций является центральным элементом структуры, описывающей необходимые роли, наборы навыков и желаемые уровни квалификации для практикующих специалистов.
- **Описания ролей**: Подробные описания основных функций и наборов навыков для различных ролей представлены по всему документу.
- **Наборы навыков и уровни**: Структура описывает конкретные наборы навыков, необходимые для каждой роли, и желаемые уровни экспертизы.

1) Роли

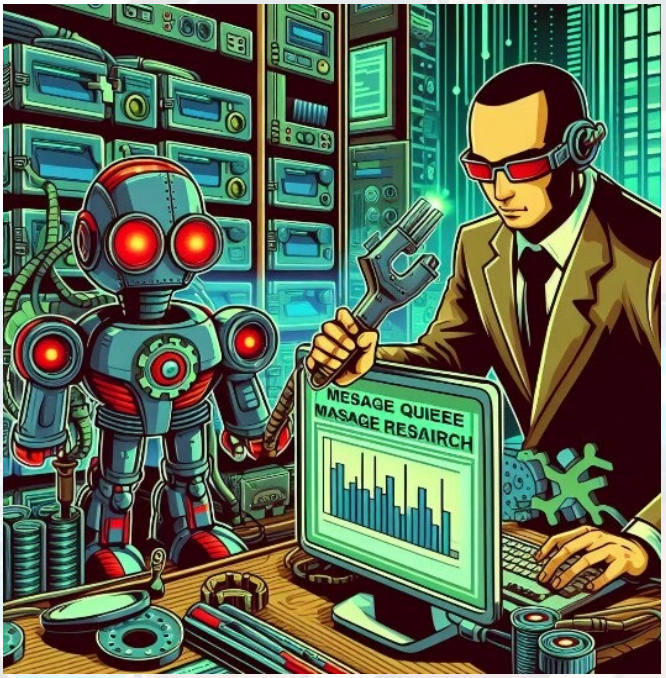
- **Руководители подразделений по борьбе с киберпреступностью**: отвечают за надзор за подразделениями по борьбе с киберпреступностью, принятие обоснованных решений по случаям киберпреступности, координацию ресурсов и расстановку приоритетов в деятельности полиции.

- **Руководители групп**: руководят расследованиями киберпреступлений в своих конкретных областях. Они контролируют текущие расследования, координируют работу со старшим руководством и обеспечивают, чтобы их команда была оснащена необходимой подготовкой и инструментами.
- **Криминалисты**: необходимо фундаментальное понимание цифрового мира, в том числе того, как обращаться с электронными доказательствами на местах преступлений и использовать OSINT.
- **Аналитики по киберпреступности**: Аналитики участвуют в сборе и анализе данных для получения оперативной информации и стратегических выводов.
- **Криминалисты по киберпреступности**: глубоко разбирающиеся в извлечении данных и онлайн-сборе информации, и руководят расследованиями киберпреступлений и часто участвуют в обучении других инструкторов из числа сотрудников правоохранительных органов.
- **Эксперты по киберпреступности**: обладают специализированными знаниями в конкретных областях киберпреступности, таких как OSINT, даркнет, криптовалюты и устройства Интернета вещей.
- **Цифровые криминалисты**: сосредоточены на выявлении, восстановлении и анализе цифровых доказательств.
- **Эксперты по реагированию на кибератаки**: Эти эксперты отвечают за техническое реагирование на кибератаки, сотрудничая с различными заинтересованными сторонами, такими CERT и ИТ-отделы.
- **Специалисты первой инстанции**: являются сотрудниками правоохранительных органов, первыми прибывающими на место кибер-инцидента.
- **Судьи первой и апелляционной инстанций**: судьям, рассматривающим дела о преступлениях, необходимо эффективно интегрировать кибер-доказательства в судебный процесс.
- **Прокуроры и судьи-следователи**: Эти юристы руководят уголовными расследованиями, связанными с кибернетическими элементами, оценивают сбор электронных доказательств и представляют дела в суде.

2) Навыки

- **Цифровая криминалистика**: включает идентификацию, сохранение, приобретение, валидацию, анализ, интерпретацию, документирование и представление электронных доказательств из цифровых источников.
- **Исследование и администрирование сети**: относится к пониманию сетевых функций, проведению расследований внутри сетей и анализу данных о трафике для выявления признаков компрометации.
- **Программирование и написание сценариев**: используется для построения информационных систем и автоматизации задач для поддержки исследований и анализа данных.
- **Составление отчётов и представление данных расследований киберпреступлений**: включает документацию, составление заметок и составление окончательного отчёта по различным типам отчётов.
- **Анализ и визуализация**: включает применение методов анализа данных для описания, иллюстрации и обобщения данных о киберпреступлениях с целью выявления закономерностей, тенденций и практических знаний.
- **Законодательство о киберпреступности**: относится к пониманию законодательства, регулирующего киберпреступную деятельность, включая национальное законодательство о киберпреступности и электронных доказательствах, законы о конфиденциальности, Общие положения о защите данных (GDPR), правила ЕС о хранении данных и решения международных судов.
- **Общие знания о киберпреступности**: охватывает информацию, касающуюся киберпреступлений с поддержкой киберпространства и кибер-зависимости, тенденций киберпреступности, угроз и методов работы, а также понимание кибербезопасности.
- **Специальные знания о киберпреступности**: относятся к уникальным навыкам, полученным в результате специальной подготовки в конкретных областях киберпреступности.
- **Управление на месте преступления и обработка электронных доказательств**: относится к стандартам и передовой практике выявления и изъятия электронных доказательств на местах преступлений.
- **Методы расследования киберпреступлений**: включает навыки, необходимые для расследования киберпреступлений, такие как методы сбора разведданных, обработка и интерпретация данных, отслеживание подозреваемых онлайн и офлайн, работа под прикрытием онлайн, допрос киберпреступников и управление рисками расследования

E. Анализ MQ рынка: когда простые решения слишком дешёвые, ведь тратить больше – лучше!



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. Основными игроками на рынке являются RabbitMQ, Apache Kafka, IBM MQ, Microsoft Azure Service Bus и Google Cloud IoT, каждый из которых обслуживает широкий спектр отраслей – от финансовых услуг до здравоохранения и "умных городов".

1) Сводные данные

- **Доля рынка**: процент рынка, который занимает каждый брокер.
- **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
Rabbit MQ	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%

F. Кибербезопасность и Антарктика

В апреле Национальный научный фонд США (NSF) объявил, что не будет поддерживать какие-либо новые полевые исследования в этом сезоне из-за задержек с модернизацией станции Макмердо. Национальный фонд и береговая охрана США также объявили о сокращениях, которые поставят под угрозу научные и геополитические интересы США в регионе на десятилетия вперёд. В частности, в апреле NSF объявил, что не будет продлевать аренду одного из двух своих антарктических исследовательских судов "Laurence M. Gould". До этого, в октябре 2023 года, NSF объявил, что в ближайшие десятилетия будет эксплуатировать только одно исследовательское судно.

Кроме того, в марте Береговая охрана США объявила, что ей необходимо "пересмотреть базовые показатели" для своей давно отложенной программы Polar Security Cutter, жизненно важной для национальных интересов США на обоих полюсах. Принятые решения, будут иметь серьёзные последствия для деятельности США в Антарктике даже за 2050 годом.

Государственный департамент воздержался от объявления внешнеполитических интересов США в Антарктическом регионе, и Белый дом, похоже, удовлетворён устаревшей и непоследовательной национальной стратегией в отношении Антарктики прошлого века. Конгресс США также не ответил на призывы учёных.

В результате 1 апреля Управление полярных программ NSF объявило, что оно приостанавливает новые предложения по полевым работам на следующие два сезона и не будет запрашивать их в Антарктиде.

Суда, способные работать в полярных морях, становятся все более востребованными, но строить их все труднее. Столкнувшись со значительными проблемами в проекте строительства кораблей и катеров ледового класса, Береговая охрана США объявила в марте, что она "сдвинет базовые сроки" разработки новых проектов ледоколов.

Результатом этих, казалось бы, независимых решений станет сокращение физического присутствия США в Антарктиде. Это будет иметь негативные последствия не только для американских учёных, но и для геополитики США в регионе, особенно учитывая тотальное превосходство России в ледоколах и догоняющее влияние Китая.

США упустили из виду наиболее важные аспекты: адекватное и регулярное финансирование научных исследований в Антарктике, новую национальную стратегию (текущая стратегия была опубликована в июне 1994 года) и понимание законодателями важности интересов и решений США в Антарктике. Неспособность финансировать оперативную и материально-техническую поддержку, необходимую для научных исследований и геополитического влияния США, эффективно означает доминирование России и Китая в антарктическом регионе, поскольку никакая другая страна, включая традиционных участников, таких как Чили, Австралия и Швеция, не может превзойти существующий и растущий научный потенциал России и Китая.

Решение США приостановить научные исследования в Антарктиде вызвало различные реакции со стороны других стран, особенно тех, у которых есть значительные интересы и операции в регионе. Это решение, обусловленное бюджетными ограничениями и задержками в модернизации критически важной инфраструктуры, имеет не только геополитические последствия.

1) Геополитические последствия

a) Активизация действий соперничающих держав

- **Китай**: Китай расширяет своё присутствие в Антарктиде, и отступление США ускорит эту тенденцию. Китай недавно открыл свою пятую исследовательскую станцию в Антарктиде и наращивает научный и логистический потенциал в регионе. Расширение деятельности Китая вызывает обеспокоенность по поводу потенциальных технологий двойного назначения, которые могут служить как научным, так и военным целям. Растущее влияние Китая в Антарктиде может изменить баланс сил и усилить геополитическую напряжённость.

- **Россия**: Россия также наращивает свою деятельность в Антарктике, включая создание новых исследовательских станций. Прогресс России в области ледокольных технологий и её стратегическое позиционирование в регионе будут подкреплены сокращением присутствия США. Это приведёт к усилению доминирующей роли России в управлении Антарктидой и научных исследованиях, что ещё больше бросит вызов интересам США.

b) Реакция партнёров

- **Австралия**: Австралия, ключевой игрок в делах Антарктики, выразила обеспокоенность по поводу решения США. Австралия активно участвует в исследованиях и управлении Антарктикой и полагается на международное сотрудничество для достижения своих научных и экологических целей. Действия США побуждают Австралию увеличить собственные инвестиции в исследования и укрепить партнёрские отношения с другими странами, чтобы «заполнить пустоту», оставленную США

- **Великобритания**: Великобритания также внесла значительный вклад в исследования в Антарктике. Страна стремится расширить своё научное присутствие и сотрудничество с другими странами для обеспечения дальнейшего прогресса в исследованиях. Правительство Великобритании подчеркнуло важность сохранения сильного международного присутствия в Антарктике для решения глобальных экологических проблем и соблюдения принципов системы Договора.

c) Стратегические уязвимости:

- Решение США выявляет стратегическую уязвимость по мере того, как новые технологии снижают барьеры для стран, увеличивающих своё присутствие и извлекающих ь выгоду из региона. Это включает потенциал для военного применения, разведки и спутниковое позиционирования

- Отсутствие присутствия США приводит к стратегическому дисбалансу, когда Россия и Китай потенциально будут доминировать в регионе. Это будет долгосрочные последствия для глобальной безопасности и национальных интересов США.

2) Экономические последствия

Кибер-атаки на морскую отрасль в Антарктиде имеют экономические последствия, включая сбои в научных исследованиях и операциях, увеличение операционных расходов, сбои в цепочке поставок, потерю данных и интеллектуальной собственности, а также усиление нацбезопасности и геополитической напряжённости.

a) Срыв научных исследований и операций

- **Влияние на исследовательские миссии**: атаки могут нарушить работу исследовательских судов и станций, что приведёт к задержкам или отмене научных миссий к потере ценных исследовательских данных и увеличению затрат, связанных с перепланированием и продлением миссий.

- **Эксплуатационные задержки**: сбои в работе навигационных систем, сетей связи и других критически важных эксплуатационных технологий могут привести к значительным задержкам в морских операциях.

b) Увеличение Эксплуатационных расходов

- **Затраты на смягчение последствий и восстановление после кибер-атак**: затраты, связанные со смягчением последствий кибер-атак и восстановлением после них, могут быть значительными. Сюда входят расходы, связанные с реагированием на инциденты, восстановлением системы и внедрением дополнительных мер безопасности для предотвращения будущих атак.

- **Страховые взносы**: кибер-атаки могут привести к повышению страховых взносов для морских компаний, работающих в Антарктиде. Страховщики могут увеличить страховые взносы для покрытия повышенного риска кибер-инцидентов, увеличивая общие операционные расходы.

c) Сбои в цепочке поставок

- **Влияние на логистику**: атаки нарушают цепочку поставок, и имеют влияние на транспортировку товаров и предметов первой необходимости в Антарктиду и обратно. Это приводит к нехватке важнейших поставок, увеличению транспортных расходов и задержкам в доставке товаров.

- **Волновые эффекты для экономики**: сбои в цепочке поставок могут оказывать волновой эффект на экономику в целом, затрагивая отрасли, которые зависят от своевременных поставок товаров и материалов. Это приведёт к увеличению затрат и снижению производительности во многих секторах.

d) Потеря интеллектуальной собственности

- **Утечка данных**: кибер-атаки приводят к краже конфиденциальных данных, включая результаты исследований, конфиденциальную информацию и личные данные членов экипажа и исследователей. Потеря таких данных может иметь значительные экономические последствия, включая потерю конкурентного преимущества и потенциальную юридическую ответственность.

- **Кража интеллектуальной собственности**: кража интеллектуальной собственности: запатентованные исследовательские данные и технологические инновации, подорвёт экономическую ценность научных исследований и разработок в Антарктике.

e) Нацбезопасность и геополитические интересы

- **Геополитическая напряжённость**: кибер-атаки на морские операции в Антарктиде могут усугубить геополитическую напряжённость, особенно если они приписываются субъектам национального государства. Это приведёт к увеличению расходов на оборону и безопасность, поскольку страны стремятся защитить свои интересы в регионе.

- **Стратегические уязвимости**: срыв морских операций может выявить стратегические уязвимости, потенциально влияющие на национальную безопасность и экономическую стабильность. Это может привести к увеличению инвестиций в кибербезопасность и оборонные меры, отвлекая ресурсы от других важных областей.

G. Человекоподобные роботы

Гуманоидные роботы — это усовершенствованные машины, разработанные для имитации человеческой формы и поведения, оснащённые сочленёнными конечностями, усовершенствованными датчиками и часто способностью к социальному взаимодействию. Эти роботы все чаще используются в различных секторах, включая здравоохранение, образование, промышленность и сферу услуг, благодаря их адаптируемости к среде обитания человека и способности выполнять задачи, требующие человеческой ловкости и взаимодействия.

В здравоохранении человекоподобные роботы помогают выполнять клинические задачи, оказывают эмоциональную поддержку и помогают в реабилитации пациентов. В сфере образования они служат интерактивными компаньонами и персональными наставниками, улучшая опыт обучения и способствуя социальной интеграции детей с особыми потребностями. Промышленный сектор извлекает выгоду из человекоподобных роботов за счёт автоматизации повторяющихся и опасных задач, повышения эффективности и безопасности. Кроме того, в сфере услуг эти роботы оказывают помощь клиентам, направляют посетителей и выполняют задачи технического обслуживания, демонстрируя свою универсальность и потенциал для преобразования различных аспектов повседневной жизни.

1) Прогнозы рынка человекоподобных роботов

Рынок человекоподобных роботов находится на пороге существенного роста, и прогнозы указывают на многомиллиардный объём рынка к 2035 году. Ключевые факторы включают достижения в области искусственного интеллекта, снижение затрат и растущий спрос на автоматизацию в опасных отраслях и на производстве.

- Отчёт Goldman Sachs (январь 2024 г.):
  - **Общий объём адресуемого рынка (TAM)**: ожидается, что объём рынка человекоподобных роботов достигнет 38 миллиардов долларов к 2035 году, по сравнению с первоначальным прогнозом в 6 миллиардов долларов, что обусловлено четырёхкратным увеличением прогнозов поставок до 1,4 миллиона единиц.
  - **Оценки поставок**: Базовый сценарий прогнозирует совокупный годовой темп роста (CAGR) на 53% в период с 2025 по 2035 год, при этом поставки достигнут 1,4 млн единиц к 2035 году. Согласно оптимистичному сценарию, поставки достигнут 1 миллиона единиц к 2031 году, что на четыре года опережает предыдущие ожидания.
  - **Снижение затрат**: Стоимость роботов высокой спецификации снизилась на 40% до 150 000 долларов за единицу в 2023 году по сравнению с 250 000 долларами в предыдущем году из-за более дешёвых компонентов и более широкой внутренней цепочки поставок.
- **Маркетинговые исследования Data Bridge**: ожидается, что мировой рынок человекоподобных роботов вырастет с 2,46 миллиарда долларов в 2023 году до 55,80 миллиарда долларов к 2031 году, при среднем росте на 48,5% в течение прогнозируемого периода.
- **SkyQuestt**: По прогнозам, рынок вырастет с 1,48 миллиарда долларов в 2019 году до 34,96 миллиарда долларов к 2031 году, при CAGR 42,1%.
- **GlobeNewswire**: Мировой рынок человекоподобных роботов, оцениваемый примерно в 1,3 миллиарда долларов в 2022 году, как ожидается, увеличится до 6,3 миллиарда долларов к 2030 году при среднегодовом росте в 22,3%.
- **Компания по исследованию бизнеса**: ожидается, что рынок вырастет с 2,44 миллиарда долларов в 2023 году до 3,7 миллиарда долларов в 2024 году, при CAGR 51,6%. По прогнозам, к 2028 году объём рынка достигнет 19,69 миллиарда долларов, а CAGR составит 51,9%.
- **Исследование Grand View**: Размер рынка: Мировой рынок человекоподобных роботов оценивался в 1,11 миллиарда долларов в 2022 году и, как ожидается, вырастет в среднем на 21,1% с 2023 по 2030 год.
- **Goldman Sachs (февраль 2024 г.)**: рынок может достичь 154 миллиардов долларов к 2035 году, что сопоставимо с мировым рынком электромобилей и одной третью мирового рынка смартфонов по состоянию на 2021 год.
- **Macquarie Research**: Согласно нейтральному прогнозу, ожидается, что мировой рынок роботов-

гуманоидов достигнет 107,1 миллиарда долларов к 2035 году, а CAGR с 2025 по 2035 год составит 71%.

2) Ключевые движущие силы и тенденции

- **Технологические достижения**: Значительный прогресс в области комплексного искусственного интеллекта и мультимодальных алгоритмов искусственного интеллекта, ускоряет итерации продукта и улучшает возможности роботов.
- **Снижение затрат**: Доступность более дешёвых компонентов и усовершенствования в дизайне и технологиях производства снижают затраты, делая разработки более экономически выгодными.
- **Последствия для рынка труда**: Национальная политика повышает спрос на роботов для выполнения опасных работ с потенциальным применением в производстве, спасении при стихийных бедствиях и уходе за пожилыми людьми.
- **Инвестиции и динамика рынка**: Увеличение инвестиций со стороны цепочек поставок, стартапов и компаний, зарегистрированных на бирже, особенно в США и Азии, являются движущей силой роста рынка. Государственная поддержка, особенно со стороны Китая, также является важным фактором.

Источники подчёркивают значительные инвестиции и финансирование, вливаемые в сектор гуманоидной робототехники, благодаря потенциалу этой новой технологии и участию крупных технологических компаний и инвесторов.

- **Масштабный раунд финансирования Figure AI**: Стартап Figure AI, занимающийся разработкой человекоподобных роботов, привлёк 675 миллионов долларов в раунде финансирования серии B, что оценивало компанию в 2,6 миллиарда долларов постфактум. Раунд финансирования привлёк известных инвесторов, в том числе Джеффа Безоса (через Bezos Expeditions), Microsoft, Nvidia, стартап-фонд OpenAI, Индустриально-инновационный фонд Amazon, Intel Capital, Align Ventures и ARK Invest.
- **Участие крупных технологических компаний**:
  - OpenAI, компания, стоящая за ChatGPT, заключила соглашение о сотрудничестве с Figure AI для разработки моделей искусственного интеллекта следующего поколения для человекоподобных роботов, объединив исследования OpenAI с опытом Figure в области робототехники.
  - Microsoft инвестирует 95 миллионов долларов в Figure AI и предоставит свои облачные сервисы Azure для инфраструктуры искусственного интеллекта, обучения и хранения данных.
  - Nvidia, ведущий производитель чипов, инвестирует 50 миллионов долларов в искусственный интеллект.
  - Инвестиционное подразделение Amazon и венчурный фонд Intel Capital также участвуют в раунде финансирования.
- **Другие значительные инвестиции**:
  - Норвежский стартап 1X Technologies привлёк 100 миллионов долларов финансирования от OpenAI.
  - Компания Agility Robotics, поддержанная Amazon в 2022 году, тестирует своих человекоподобных роботов на складах Amazon.
  - Sanctuary AI разрабатывает гуманоидного робота по имени Феникс.
  - Повышенный интерес со стороны венчурных компаний: Венчурные компании, такие как Parkway Venture Capital, Align Ventures, ARK Venture Fund, Aliya Capital Partners и Tamarack, инвестируют в стартапы в области гуманоидной робототехники. Ситуация с финансированием остается сложной, но бум искусственного интеллекта дал надежду стартапам в области гуманоидной робототехники.
- **Государственная поддержка**: потенциальная государственная поддержка, особенно со стороны Китая, рассматривается как фактор, стимулирующий рост рынка

3) Современное использование роботов

- **Производство**: Человекоподобные роботы используются на производстве для выполнения таких задач, как сборка, контроль качества и погрузочно-разгрузочные работы. Они могут выполнять повторяющиеся задачи с высокой точностью и могут работать в условиях, которые могут быть опасны для человека.
- **Здравоохранение**: В здравоохранении человекоподобные роботы помогают в уходе за пациентами, реабилитации и хирургии. Они могут контролировать жизненно важные показатели, помогать в физиотерапии и даже выполнять сложные хирургические процедуры.
- **Электронная коммерция и складирование**: Человекоподобные роботы используются в электронной коммерции и на складах для управления логистикой, такой как сортировка и транспортировка товаров. Они помогают повысить эффективность и снизить трудозатраты.
- **Обслуживание клиентов и гостиничный бизнес**: человекоподобные роботы используются в ролях обслуживания клиентов, таких как консьержи,

администраторы и гиды. Они могут взаимодействовать с клиентами, предоставлять информацию и улучшать качество обслуживания клиентов.

- **Безопасность**: Человекоподобные роботы используются в сфере безопасности для патрулирования территорий, обнаружения вторжений и мониторинга на предмет угроз безопасности. Они могут работать непрерывно, не испытывая усталости, и предоставлять данные операторам-людям в режиме реального времени.

- **Образование и исследования**: В образовательных учреждениях человекоподобные роботы используются в качестве учебных пособий и исследовательских инструментов. Они помогают студентам узнать о робототехнике, программировании и искусственном интеллекте.

- **Развлечения**: человекоподобные роботы также используются в сфере развлечений, например, для выступлений на мероприятиях, в качестве экскурсоводов в музеях и даже для дирижирования оркестрами

  - *Потенциальное применение (в будущем)*
- **Военные**: Человекоподобные роботы могут использоваться в военных целях для таких задач, как разведка, обезвреживание бомб и материально-техническое обеспечение. Они могут действовать в опасных условиях, снижая риск для солдат-людей.

- **Кибербезопасность**: Человекоподобные роботы могли бы сыграть определённую роль в кибербезопасности путём мониторинга и защиты биологических данных и систем от киберугроз. Их продвинутые датчики и возможности искусственного интеллекта делают их подходящими для этой роли.

- **Нефтегазовая промышленность**: В нефтегазовой промышленности человекоподобные роботы могут использоваться для инспекции, технического обслуживания и ремонта морских платформ и трубопроводов. Они могут работать во взрывоопасных средах, что снижает необходимость вмешательства человека.

- **Добыча полезных ископаемых**: Человекоподобные роботы могут использоваться в горнодобывающей промышленности для выполнения таких задач, как бурение, добыча руды и проверки безопасности. Они могут работать в опасных и замкнутых пространствах, повышая безопасность и эффективность.

- **Финансовые услуги и фондовые рынки**: Человекоподобные роботы могли бы оказывать помощь в сфере финансовых услуг, обеспечивая поддержку клиентов, проводя транзакции и анализируя рыночные данные. Их способность быстро обрабатывать большие объёмы информации делает их ценными в этом секторе.

- **девелопмент**: В сфере недвижимости человекоподобные роботы могут использоваться для осмотра имущества, технического обслуживания и взаимодействия с клиентами. Они могут проводить виртуальные туры и помогать с задачами по управлению недвижимостью.

- **Пищевая промышленность**: Человекоподобные роботы могут использоваться в пищевой промышленности для выполнения таких задач, как заполнение полок, приготовление пищи и доставка продуктов. Они могут помочь повысить эффективность и снизить трудозатраты.

- **Самолёты**: В авиационной промышленности человекоподобные роботы могли бы помогать в техническом обслуживании, инспекциях и сборке компонентов самолётов. Их точность и способность работать в ограниченном пространстве делают их подходящими для этой роли.

- **Морское дело и судоходство**: роботы могут использоваться в морском судоходстве для таких задач, как обработка грузов, техническое обслуживание судов и проверки безопасности. Они могут работать в суровых морских условиях, повышая эффективность и безопасность.

- **Умные города**: В умных городах роботы могут использоваться для различных задач, таких как управление дорожным движением, общественная безопасность и обслуживание инфраструктуры. Они могут взаимодействовать с гражданами, предоставлять информацию и помогать управлять городской средой.

Рубрика: Разбор

Мировая торговля, морские порты и безопасность

Аннотация – В этом документе представлен анализ воздействия кибер-атак на деятельность морских портов с акцентом на количественную оценку эконометрических потерь. В ходе анализа рассмотрены различные аспекты, включая прямые понесённые экономические потери, эффекты для различных секторов промышленности, конкретные уязвимости и последствия кибер-атак, а также меры безопасности в морских портах. Анализ полезен специалистам в области безопасности, ИТ-экспертам, и заинтересованным сторонам из различных отраслей, поскольку даёт представление о масштабах потенциальных сбоев и позволяет вести разработку надёжных стратегий для противодействия кибер-проблемам. Выводы, полученные в результате анализа, имеют значение для повышения готовности к кибер-угрозам в критически важной национальной инфраструктуре и реагирования на них, обеспечивая тем самым экономическую стабильность и национальную безопасность.

A. Введение

В документе «Quantifying the econometric loss of a cyber-physical attack on a seaport» представлено всестороннее исследование экономических последствий кибер-атак на морскую инфраструктуру, которые являются важнейшими компонентами глобальной торговли и цепочек поставок и вносят значительный вклад в понимание уязвимости и экономических последствий кибер-угроз в секторе.

Суть исследования заключается в разработке и применении эконометрической модели (EC), предназначенной для количественной оценки экономических потерь в результате кибер-атак на морские порты. Кибер-эконометрическая модель (CyPEM), представляет собой структуру из пяти частей, объединяющая различные аспекты кибер-систем, анализ экономического воздействия и стратегии управления рисками. Методология включает системный подход к моделированию начальных экономических последствий кибер-атаки, которая, хотя и начинается локально, может иметь далеко идущие глобальные последствия из-за взаимосвязанного характера глобальной торговли и цепочек поставок.

Полученные результаты подчёркивают значительную экономическую уязвимость морских портов к кибер-атакам. За счёт применения в CyPEM, исследователи смогли определить количество потенциальных эконометрических убытков, оказывающие влияние не только на целевой порт, но и более широко на глобальную морскую экосистему и цепочек поставок. Результаты модели подчёркивают каскадные последствия сбоев в работе морских портов, которые могут привести к значительным экономическим потерям как на местном, так и на глобальном уровне. Это служит конкретным примером того, как модель может быть использована для оценки экономических последствий кибер-атак на морские порты.

В документе также подчёркивается конвергенция ИТ и операционных технологий как преобразующей силы в морском секторе, создающей цифровые маршруты поставок и модернизирующей морские операции. Однако это «сближение» также расширяет зону кибер-угроз, делая критически важную морскую инфраструктуру более восприимчивой к кибератакам. Угроза исходит не только от обычных киберпреступников, но и от субъектов национальных государств и организованных преступных групп, обладающих ресурсами и мотивацией для нанесения ударов по критической национальной инфраструктуре.

1) Преимущества предлагаемого решения:

- Возможность количественной оценки потенциального экономического воздействия кибер-атаки на морской порт локально и глобально
- Помогает выявлять потенциальные уязвимости и слабые места в цепочке поставок, позволяя лучше готовиться к кибератаками реагировать на них
- Адаптация для анализа различных кибер-систем

2) Недостатки предлагаемого решения:

- Небольшой размер выборки опроса, используемого для оценки общественного восприятия кибер-рисков на морском транспорте
- Для эффективного использования могут потребоваться профильные знания и опыт
- Сложность модели может затруднить понимание и использование результатов некоторыми заинтересованными сторонами
- Не учитывает другие потенциальные последствия кибер-атак, такие как воздействие на окружающую среду или безопасность.

3) Применение

Предлагаемая структура полезна для количественной оценки эконометрических потерь в результате кибер-события. Эконометрические результаты кибер-атаки на порт позволили сравнить фактический риск для кибербезопасности с воспринимаемым общественностью риском, связанным с морскими кибер-угрозами, и то, как это влияет на них.

Применение инструмента заинтересованными сторонами возможно для лучшей количественной оценки и понимания их конкретных кибер-рисков, включая связанные со страхованием корпорации, которые на региональном и / или глобальном уровнях подвержены рискам, связанным с непредвиденными перерывами в работе, и организации, производственная деятельность которых связана с глобальными цепочками поставок. Возможность обмена отдельными этапами фреймворка также позволяет моделировать другие сектора, помимо морского, и морские сценарии, а также учитывать кибер-сбои на разных узлах.

Правительственные организации, портовые администрации, субъекты грузовых перевозок и логистики, а также торговые ассоциации также могут быть заинтересованы в предлагаемой системе, поскольку она может помочь лучше понять их ландшафт рисков и выявить конкретные слабые места или зависимости, которые, если их использовать, могут оказать значительное влияние на национальную экономику.

B. Морская кибербезопасность

Морская кибербезопасность становится все более важной областью, вызывающей озабоченность в отрасли, поскольку новые технологии, такие как Интернет вещей (IoT), цифровые двойники, 5G и искусственный интеллект (ИИ), становятся все более распространёнными в этом секторе. Конвергенция и цифровизация информационных технологий (ИТ) и операционных технологий (ОТ) привели к трансформации цифровых маршрутов поставок и морских операций, расширив масштабы кибер-угроз.

Интеграция цифровых технологий в критически важные операции в морском секторе создаёт значительные кибер-уязвимости, которые могут привести к более масштабным глобальным сбоям. По мере ускорения перехода сектора к цифровизации крайне важно понимать и количественно оценивать потенциальные последствия кибер-сбоев.

1) Ключевые моменты

- Возросшие масштабы судоходства и размеров судов (крупные суда большей вместимости) привели к проблемам с маневрированием в существующих каналах и морских портах, снижая запас прочности во время кибер-инцидентов. Современные корабли также оснащены более мощным оборудованием, что увеличивает степень угрозы кибератак.
- Береговая охрана США сообщила об увеличении числа морских кибер-инцидентов на 68%, а недавние исследования показывают, что кибер-риски в морской пехоте и морских технологиях присутствуют и растут по мере внедрения новых решений.
- Хотя цифровизация в сфере судоходства обеспечивает повышение производительности, физическую безопасность, снижение выбросов углекислого газа, более высокую эффективность, более низкие затраты и гибкость, в крупных сенсорных сетях CPS и системах связи существуют уязвимые места.
- Опрос показал, что 64% респондентов считают, что порт уже испытал значительный физический ущерб, вызванный кибер-инцидентом, а 56% считают, что торговое судно уже испытало значительный физический ущерб, вызванный инцидентом кибербезопасности.

2) Второстепенные моменты

- **Новые технологии**: Морской сектор внедряет новые технологии в офисах, на судах, в морских портах, оффшорных сооружениях и многом другом. Эти технологии включают Интернет вещей (IoT), цифровых двойников, 5G и искусственный интеллект (AI).
- **Цифровизация цепочки поставок**: Цепочки поставок также используют все больше информационных технологий (ИТ), создавая цифровые уязвимости. Конвергенция ИТ и операционных технологий (ОТ) трансформирует цифровые маршруты поставок и морские операции, расширяя возможности противодействия кибер-угрозам.
- **Кибер-угрозы**: субъекты национальных государств и организованная преступность обладают ресурсами и мотивацией для запуска кибератаки на критическую национальную инфраструктуру (CNI), такую как крупномасштабные кибер-системы, которые включают морские операции.
- **Кибер-системы**: Интеграция физических процессов с программным обеспечением и сетями связи, известными как кибер-системы, является важной частью цифровой трансформации морского сектора. Однако это также создаёт новые проблемы в области кибербезопасности.
- **Последствия кибератак**: атаки на инфраструктуру имеют значительные экономические последствия, затрагивая не только целевой морской порт, но и более широкую глобальную морскую экосистему и цепочки поставок.

C. Кибер-угроза

Морской сектор становится все более уязвимым к угрозам кибербезопасности, которые могут иметь далеко идущие последствия для других областей из-за взаимосвязанного характера современных перевозок. По мере дальнейшего развития технологий растёт вероятность разрушительных событий, вызванных злонамеренными кибератаками, о чем свидетельствуют недавние отчёты и академические исследования. Чтобы понять потенциальный масштаб этих сбоев, важно изучить влияние крупных сбоев в цепочке поставок на цель атаки и остальную часть связанной с ней цепочки поставок. Эти события привели к многочисленным бизнеса, причём большинство исков поступило из районов, находящихся за пределами непосредственно затронутых регионов.

Текущие возможности киберзащиты вряд ли позволят предотвратить все кибер-катастрофы, что делает крайне важным количественную оценку и понимание последствий таких событий. Основное внимание уделяется взаимозависимостям в современных глобальных цепочках

поставок и представлена эконометрическая модель (EM), которая позволяет организациям перейти от качественной оценки к более надёжной количественной оценке рисков цепочки поставок.

Мировые производственные сети снабжения подвержены нарушениям в результате кибератак, которые могут распространяться по сети и оказывать негативное физическое и экономическое воздействие на соседние, предшествующие и последующие узлы. Кибератаки с использованием сетей IT / OT и вычислительных систем могут привести к краткосрочным потерям, отказу в обслуживании (DoS), долгосрочному выводу из строя оборудования, потере доверия клиентов, задержкам в отправке и потере стратегических преимуществ из-за утечек и компрометации конфиденциальной информации. Цифровые кибератаки также могут иметь реальные физические последствия, такие как невыполненный спрос на транспортировку товаров и производство.

1) Ключевые аспекты

- С увеличением темпов технологического роста возрастает вероятность событий, вызванных злонамеренными кибератаками в секторе.
- Экономические и страховые убытки, возникающие в результате сбоев в цепочке поставок, являются одними из основных возникающих рисков для глобальных корпораций и страховщиков.
- Поскольку нынешние возможности киберзащиты вряд ли позволят предотвратить все кибер-катастрофы, крайне важно количественно оценить и понять последствия таких событий.
- В исследовании основное внимание уделяется тому, как крупные сбои в цепочке поставок влияют на цель атаки и остальную связанную с ней цепочку поставок, представленную в классическом формате графов с "узлами", представляющими активы, и "рёбрами", соединяющими узлы.
- Эконометрическая модель (EM) позволяет организациям перейти от качественной оценки рисков цепочки поставок к более надёжной количественной оценке.
- Интегрируя EM с динамической моделью кибер-рисков MaCRA, объединённая модель позволяет пользователю получать количественные данные о смоделированных потерях для улучшения понимания кибер-рисков глобальной цепочки поставок, что приводит к повышению кибер-устойчивости и надёжности системы.

2) Реалистичное моделирование

- Тематическое исследование было проведено на базе европейского морского порта в Испании и классе контейнеровозов, которые обычно заходят в тот же порт. И порт, и судно моделируются на основе реальных данных путём цифровизации физических характеристик в цифровые.
- Порт Валенсии генерирует почти 51% ВВП Испании и является важным игроком в европейских и глобальных цепочках поставок, соединяющих Азию и Америку. Любой сбой в работе этого порта приведёт к прямым экономическим потерям для Испании и отразится на различных физических узлах и цепочках создания стоимости.
- Известные решения по управлению рисками в цепочке поставок (SCRM) содержат многочисленные основы и модели для определения типов и источников рисков, а также стратегий смягчения последствий, но без адаптации к «технологическому ландшафту Индустрии 4.0».
- Эконометрическая модель (EM) с использованием полностью количественной модели с полным отображением узловой сети для точного представления сквозного жизненного цикла продукта и расчёта эконометрического воздействия существующей сети цепочки поставок.
- Сбои в кибер-системе (CPS) распространяются между физическими уровнями и кибер-уровнем из-за высоких взаимосвязей и взаимозависимости. Факторы риска варьируются от физических до кибернетических, от статических до динамических.

D. Фреймворк

Применяется «гибридный» метод моделирования, который использует частично отображённые цепочки поставок и использует прогнозную аналитику для заполнения недостающих частей. Такой подход позволяет избежать недооценки риска за счёт выявления скрытых уязвимостей и корреляций, проистекающих из невидимых или неизвестных звеньев данной цепочки поставок. Модель риска цепочки поставок является первой в своём роде, поскольку это количественная модель, которая включает глобальные модели торговли и сетей поставок, отображение товарных потоков и корреляцию между различными товарными группами и отраслями.

CyPEM даёт организациям возможность провести стресс-тестирование устойчивости цепочек поставок путём оценки затрат и времени на восстановление после различных сценариев кибератак. Система включает количественные модели рисков, которые имитируют основные компоненты глобальных цепочек поставок и их неопределённости для оценки временных задержек и экономических потерь в результате условного прерывания бизнеса (CBI). Время простоя измеряется количеством дней или часов, вызванных кибер-сбоями в работе данного узла цепочки поставок.

Фреймворк разработан для обеспечения определённой динамической автоматизации при расчёте кибер-эконометрических потерь. Некоторые переменные сценария кибератаки могут быть изменены «в реальном времени» на различных этапах для изучения ряда эконометрических результатов. Этот инструмент позволяет пользователям активно управлять рисками в цепочке поставок, предвидя корреляции в цепочках поставок, а также последствия разрушительных событий, вызванных киберпространством, до того, как они могут произойти. Количественные результаты также важны для измерения различий между предполагаемым и реальным риском в понимании экспертов и непрофессионалов.

Фреймворк предназначен для предоставления аналитики по различным звеньям или секторам цепочки поставок и может использоваться для информирования о поддающихся количественной оценке кибер-рисках.

- **Определение отрасли, промежуточных частей и конечных продуктов**: определение отрасли, промежуточных частей и конечных продуктов анализируемой цепочки поставок.
- **Определение сети, в которой узлы являются поставщиками, а ребра - потоками продукции / деталей**: на этом этапе определяется сеть цепочки поставок, где узлы представляют поставщиков, а ребра - потоки продукции или деталей.
- **Расчёт сбоев с использованием оценки кибер-рисков и модели пропускной способности порта**: расчёт сбоев с использованием модели оценки рисков и пропускной способности порта.
- **Расширение на остальную часть сети**: на этом этапе учитывается распространение сбоя дальше по сети цепочки поставок для оценки воздействия на другие узлы и границы.
- **Расчёт отраслевых убытков**: расчёт отраслевых убытков и их распределения в результате сбоя.

Первые два этапа включают создание ациклических сетевых графиков с использованием статистики торговли сырьевыми товарами и товарных потоков стран для установления зависимостей по продуктам. После установления зависимости от продукта торговые данные из статистики торговли сырьевыми товарами используются для создания сети, включающей узлы хранения и транспортировки, а также цепочки поставок компонентов на основе межотраслевых зависимостей.

Следующим этапом разработки структуры является определение сети, которое выходит за рамки продуктовых зависимостей и учитывает производство и транспортировку в стране для определения товарных потоков. В то время как модель в настоящее время использует ациклическую сеть для представления потока продуктов без создания циклов обратной связи, будущее моделирование на этом этапе может быть заменено на другой тип сети в зависимости от конечного использования всей структуры. Данные, используемые для определения и создания будущих сетей, могут включать период данных, поток (т. е. импорт / экспорт), коды товаров, торговую стоимость, вес нетто, количество и статистику.

Предлагаемая сеть является гибридной, которая объединяет график зависимости продукта (или дерево) с первого этапа и соответствующие торговые данные со второго этапа. Этот шаг гарантирует, что эконометрическая модель сможет учитывать динамику торговли между странами и отраслевыми границами в рамках товарных категорий. Результирующая гибридная сеть является ключом к определению эконометрических потерь от кибер-сбоя на более поздних этапах CyPEM.

Прогнозная аналитика может улучшить графики зависимостей продукта на ранних этапах, точность и детализация которых зависят от последующих этапов. CyPEM собирает данные из многочисленных источников и устаревших систем, чтобы получить полное представление о цепочке поставок, а последующий анализ проводится для выявления полезной информации и повышения уровня интеллектуальных данных. Аналитика используется для автоматизации принятия сложных решений и упреждающего и динамического обновления рекомендаций на основе изменяющихся событий, чтобы воспользоваться преимуществами этих прогнозов и повысить ценность инструментов классификации проектов. Применение этих сетей для предварительного определения атрибутов рынка и зависимостей, а также того, как они влияют на остальную часть сети, сохраняя при этом фактические события сбоев (и все их отдельные элементы) более динамичными.

Структура CyPEM предполагает расчёт сбоев с использованием двух моделей: модели оценки морских кибер-рисков и кибер-модели пропускной способности порта. Модель оценки морских кибер-рисков использует цепочку кибер-атак, чтобы показать ряд потенциальных рисков и результатов, в зависимости от успеха каждого сегмента цепочки атак. Цепочка атак, используемая в этой модели, была подтверждена фактическими данными и экспериментами на испытательном стенде, которые были сопоставлены с уязвимостями системы на судах, которые, как известно, заходят в порт в 2021 и 2022.

Вторая часть расчёта сбоев заключается в учёте кибер-рисков и их последствий, а также в прогнозировании общего эффекта сбоев в работе портов. Для этого была разработана кибер-модель пропускной способности порта. Этот процесс похож на первые два этапа, но используется одного порта, а не всей глобальной сети. Предлагаемый метод позволяет сделать модель более детализированной, моделируя даже отдельные суда и терминальные краны (включая их тип), чтобы точно определять время простоя порта в часах, а также в процентах.

Чтобы модель пропускной способности имитировала портовые операции, необходимо учитывать определённые параметры, описывающие трафик и потоки внутри порта:

- процесс прибытия,
- количество контейнеров за один заход в порт,
- распределение времени обслуживания на судно,
- долю контейнеров, предназначенных для перегрузки,
- среднее время пребывания контейнеров в порту.

Наблюдается, что сбой, вызванный кибератакой, снижает производственные / транспортные возможности узлов и оказывает волновой эффект на последующие узлы. Если циклические цепочки поставок будут интегрированы в систему в качестве следующего шага в будущем, характер сбоев и результаты могут сильно отличаться. Глобальная кибератака может отличаться от других стихийных бедствий, которые могут быть локализованы географически, в то время как кибератаки, как правило, происходят там, где расположены целевые системы. Следовательно, одна цифровая угроза может спровоцировать кибер-инциденты в нескольких географических регионах или охватить несколько секторов (например, здравоохранение, производство), если используется аналогичная базовая технология.

Компании вовлечённые в "различные кибер-активности"

Аннотация – в документе представлен анализ публично известных частных компаний, участвующих в наступательных кибер-операциях против национальных государств. Анализ включает в себя различные аспекты инвентаризации, включая характер включённых в список компаний, типы предлагаемых ими возможностей и геополитические последствия их услуг.

Предоставленная выдержка отличается высоким качеством и объединяет общедоступную информацию без раскрытия конфиденциальных данных. Он служит ценным ресурсом для специалистов в области безопасности, предлагая представление об условиях участия частного сектора в наступательных кибер-операциях.

A. Что представляет собой Группа Equation?

The Equation Group классифицируется как продвинутая постоянная угроза (APT) и известна своей изощренной деятельностью по кибершпионаж с активностью как минимум с 2001 года и сложными и высокоразвитыми вредоносными инструментами и технологиями. Группа участвовала в многочисленных кибер-операциях, нацеленных на широкий спектр секторов и стран, включая правительственные, военные, телекоммуникационные, аэрокосмические, энергетические, ядерные исследования и финансовые учреждения

B. Equation и технологии

1) Кибер-возможности

- **Инструменты удалённого доступа и платформы вредоносных программ**: Equation использовала множество инструментов удалённого доступа и разработала несколько платформ вредоносных программ высокой сложности, таких как EquationDrug, DoubleFantasy, Equestre (то же, что EquationDrug), TripleFantasy, GrayFish, Fanny и EquationLaser. Эти инструменты предназначены для шпионажа и имеют механизмы самоуничтожения, позволяющие уменьшить количество улик.
- **Перепрограммирование встроенного ПО**: Одним из самых передовых методов, используемых Equation, является возможность перепрограммирования встроенного ПО жёсткого диска. Эта возможность позволяет группе оставаться в заражённых системах необнаруживаемой и эффективно делает их операции невидимыми и неуязвимыми.
- **Шифрование и обфускация**: Equation часто использовала схемы шифрования, включая RC5, RC6, RC4, криптографические функции AES и различные хэш-функции, для защиты своих вредоносных программ и коммуникаций. Такой уровень шифрования и стратегии, используемые для маскировки её деятельности, свидетельствуют о передовых возможностях группы.
- **Использование уязвимостей нулевого дня**: Группа имеет доступ к эксплойтам нулевого дня и использовала их. Например, Equation использовала два эксплойта нулевого дня в Fanny до того, как они были интегрированы в Stuxnet, что указывает на доступ к этим уязвимостям раньше других известных групп, совершавших кибератаки.
- **Инструменты разведки на базе USB**: для получения информации об устройствах, которые не подключены к Интернету, Equation разработала вредоносную программу для разведки на основе USB-накопителей. Эта способность важна для проникновения на охраняемые военные объекты, разведывательные организации и ядерные объекты.
- **Фреймворки для эксплойтов и постэксплуатационные** инструменты: Equation использовала различные фреймворки эксплойтов и инструменты для последующей эксплуатации, такие как DanderSpritz, который представляет собой полнофункциональный фреймворк, используемый после эксплойта устройства и содержит широкий спектр модулей для сохранения, разведки, бокового перемещения и обхода антивирусных систем.
- **Цепочка эксплойтов брандмауэра**: Equation разработала почти полный набор эксплойтов, предназначенный для основных производителей брандмауэров. Этот комплект включает в себя эксплойты, такие как EXTRABACON (CVE-2016–6366) для получения доступа к брандмауэрам Cisco ASA и PIX, и EPICBANANA (CVE-2016–6367) для установки командного и управляющего шелл-кода.

2) Вредоносное ПО Equation

- **EquationDrug**: сложная вредоносная платформа, предоставляющая группе полнофункциональную платформу для шпионажа.
- **DoubleFantasy**: вредоносное ПО в стиле валидатора, используемое для подтверждения того,

что цель представляет интерес, а затем для развёртывания следующего вредоносного ПО.

- **Fanny**: Червь, использующий два эксплойта нулевого дня для отображения сетей с воздушным зазором через USB-накопители.
- **GrayFish**: Платформа, которая полностью размещается в реестре, шифруя свою полезную нагрузку и сохраняя её в виртуальной файловой системе.

Одним из самых мощных инструментов в их арсенале является модуль, известный только под загадочным названием “nls_933w.dll”, который позволяет им перепрограммировать встроенное ПО жёсткого диска более чем дюжины различных марок жёстких дисков. Эта возможность является уникальным техническим достижением группы.

3) Инструменты удалённого доступа

Equation использовала несколько инструментов удалённого доступа (RATs) и известна использованием эксплойтов нулевого дня. Эти инструменты способны перезаписывать встроенное программное обеспечение дисковода, ещё раз демонстрируя расширенные возможности группы:

- **UnitedRake (UR)**: RAT-инструмент, который может быть нацелен на компьютеры с Windows. Это расширяемый и модульный фреймворк, снабжённый множеством плагинов, которые выполняют различные функции сбора информации.
- **Double Feature**: Инструмент после эксплуатации регистрирует использование других вредоносных программ на заражённом компьютере, предоставляя уникальный источник знаний, относящихся к инструментам Equation.
- **EquationLaser, EquationDrug, DoubleFantasy, Equestre (то же, что EquationDrug), TripleFantasy, GrayFish, Fanny и EquationLaser**: пользовательские платформы атак, трояны, черви и бэкдоры, используемые Equation.

C. Взаимосвязь между группой Equation и АНБ

Группа Equation подозревается в том, что она связана с подразделением АНБ по специализированным операциям доступа (Tailored Access Operations, TAO). На эту связь указывают несколько факторов:

1) Сходства между Equation и АНБ

- **Сложность и ресурсы**: Equation известна своими высокоразвитыми возможностями, включая разработку и использование сложных вредоносных программ и эксплойтов нулевого дня. Операции группы, которые охватывают десятилетия и нацелены на широкий спектр секторов по всему миру, указывают на уровень ресурсов и опыта, соответствующий такой спонсируемой государством организации, как АНБ.
- **Сходства с инструментами и методами АНБ**: Анализ вредоносных программ и эксплойтов Equation выявляет значительное сходство с теми, которые, как известно, используются АНБ. Например, использование определённых алгоритмов шифрования (RC5, RC6, RC4, AES) и методов обфускации отражает те, которые задокументированы в операциях АНБ. Кроме того, часы работы вредоносного ПО и нацеленность на конкретные страны соответствуют интересам США, что ещё раз наводит на мысль о связи с АНБ.
- **Утечка Shadow Brokers**: В 2016 году группа, известная как Shadow Brokers, обнародовала множество кибер-инструментов и эксплойтов, которые, по их утверждению, были украдены у Equation. Анализ этих инструментов показал, что они использовали уязвимости в программном и аппаратном обеспечении весьма сложными и ранее неизвестными способами, что предполагает участие организации с обширными возможностями ведения кибервойны, такой как АНБ.
- **Документы Сноудена**: Документы предоставили косвенные доказательства связи Equation с АНБ. Определённые кодовые имена и оперативные данные, обнаруженные в документах Сноудена, совпадают с теми, которые связаны с деятельностью Equation, что укрепляет уверенность в том, что группа действует под эгидой АНБ.
- **Общие эксплойты нулевого дня**: Equation имела доступ к эксплойтам нулевого дня до того, как они были использованы в других известных вредоносных программах, связанных с АНБ, таких как Stuxnet и Flame, что Equation либо является частью АНБ, либо тесно сотрудничает с ним, обмениваясь инструментами и эксплойтами для кибер-операций.
- **Экспертный анализ и атрибуция**: Эксперты и исследователи по кибербезопасности, в том числе из "Лаборатории Касперского", указали на техническую сложность, схемы таргетинга и операционную безопасность Equation как на признаки спонсируемого государством субъекта, цели которого совпадают с целями АНБ. Хотя прямое установление авторства является сложной задачей в киберпространстве, накопленные доказательства и консенсус экспертов сильно склоняются к тому, что Equation является частью АНБ или аффилирована с ним.

2) Различия между Equation и АНБ

В то время как Equation в первую очередь сосредоточена на кибершпионаже и создании и развёртывании передовых вредоносных программ, у АНБ есть более широкая миссия, которая включает как сбор разведданных, так и операции по обеспечению национальной безопасности. Деятельность АНБ охватывает широкий спектр операций, включая сигнальную разведку, кибербезопасность и глобальный

мониторинг, с целью сбора и анализа данных, имеющих отношение к национальной безопасности.

АНБ действует по всему миру и участвует в различных видах разведывательной деятельности, которые включают кибер-операции, но не ограничиваются ими. Она структурирована для поддержки более широких разведывательных и оборонных операций США, в то время как Equation специально ориентирована на сложный кибершпионаж.

3) Миссия Equation и миссия АНБ

Миссия Equation заключается в проведении кибершпионажа с целью сбора разведданных, часто путём развёртывания вредоносных программ, которые могут проникать в целевые системы и сохраняться в них незамеченными. Их операции характеризуются использованием эксплойтов нулевого дня, сложных вредоносных программ и методов, предназначенных для взлома важных объектов и сохранения их скрытности.

Напротив, миссия АНБ является более всеобъемлющей и включает в себя сбор и обработку глобальных разведывательных сигналов для принятия решений в области национальной обороны и внешней политики США. Деятельность АНБ не ограничивается кибер-операциями; она также включает широкий спектр продуктов и услуг для радиотехнической разведки и обеспечения инфобезопасности, предназначенных для защиты информационных систем США и получения иностранной радиотехнической разведывательной информации

4) Центр информационных операций Центрального разведывательного управления (ЦРУ)

Центр информационных операций Центрального разведывательного управления (IOC) играет решающую роль в расширенной миссии агентства, которая теперь включает тайные военизированные операции наряду с традиционной деятельностью по сбору разведданных. IOC, одно из крупнейших подразделений ЦРУ, переключило своё внимание с борьбы с терроризмом на наступательные кибер-операции, отражая меняющийся характер глобальных угроз и растущее значение кибервойн для национальной безопасности.

Фундамент IOC как центра цифровых и кибер-операций агентства был ещё более укреплён с созданием Директората цифровых инноваций (DDI) в 2015 году. Это новое управление, первое новое управление за пятьдесят лет, было создано для модернизации ИТ-систем ЦРУ. Он объединил ИТ-отдел шпионского агентства, кибер-возможности и разведывательные усилия с открытым исходным кодом под одной крышей, стремясь предоставить аналитикам ЦРУ более совершенные ИТ-инструменты для традиционной шпионской работы.

Создание DDI и акцент на роли IOC в кибер-операциях подчёркивают признание ЦРУ цифровой сферы в качестве важнейшего поля боя. Усилия агентства по интеграции цифровых и кибернетических возможностей в свои операции отражают более широкую тенденцию разведывательного сообщества США адаптироваться к вызовам, создаваемым цифровой эпохой, включая киберугрозы, электронное наблюдение и информационную войну

5) Группа инженерных разработок ЦРУ (EDG)

Группе инженерных разработок ЦРУ (EDG) поручено разрабатывать, тестировать и обеспечивать оперативную поддержку всех бэкдоров, эксплойтов и вредоносных полезных нагрузок, используемых ЦРУ в кибер-операциях. Эта группа играет решающую роль в создании инструментов и техник, необходимых для ведения кибершпионажа и кибервойны.

В обязанности EDG входит обеспечение того, чтобы ЦРУ поддерживало передовые возможности по проникновению в системы и сети противника, используя уязвимости в программном и аппаратном обеспечении для сбора разведданных или достижения других оперативных целей.

6) Технические аспекты кибер-операций ЦРУ (TAC)

Кибер-операции ЦРУ включают в себя сложные инструменты и методы сбора разведданных из систем и сетей противника. Это включает в себя использование передовых технологий в кибершпионаже, которые поддерживаются техническим опытом агентства.

Сотрудники ЦРУ по кибербезопасности отвечают за защиту данных и систем агентства от угроз. Они используют сложные инструменты и знания в области информационных технологий (ИТ) ЦРУ для мониторинга, оценки и управления ИТ-рисками. Это включает в себя выявление текущих угроз, снижение уровня уязвимости и прогнозирование будущих вызовов.

Отдел оперативной поддержки (OSB) ЦРУ, входящий в состав подразделения кибер-разведки, специализируется на операциях с физическим доступом, что указывает на техническую возможность разрабатывать инструменты для кибератак миссий в кратчайшие сроки, что подчёркивает техническую гибкость в кибер-операциях ЦРУ

7) TAC и EQGRP

Wikileaks даёт взгляд на оперативные проблемы, с которыми сталкиваются национальные разведывательные агентства после раскрытия их киберпотенциалов, подчёркивая постоянную необходимость повышения уровня безопасности и стратегических корректировок в кибер-операциях.

- **Совместные усилия и общие возможности**: EQGRP — это не единая организация, а собирательный термин организации под управлением TAO АНБ и IOC ЦРУ, что подчёркивает совместный характер кибер-операций между этими двумя ключевыми разведывательными структурами США.
- **Совместная разработка и авторство**: Обсуждение указывает на то, что некоторые части кибер-имплантатов, связанных с EQGRP, были созданы в соавторстве как ЦРУ, так и АНБ. Это совместное

авторство подчёркивает комплексный подход к разработке кибер-инструментов и стратегий.

- **Различия в операционных процессах**: между IOC ЦРУ и АНБ ТАО были заметные различия в процессах или их отсутствии для повторного использования кибернетических возможностей. Эти различия потенциально могут повлиять на эффективность и безопасность кибер-операций.
- **Результаты**: Утечка информации и последующее публичное разоблачение этой деятельности привели к серьёзному самоанализу в этих агентствах. Обсуждение отражает большой интерес к извлечению информации из инцидента для повышения безопасности кибер-операций.
- **Важность высококачественной информации об угрозах**: Обсуждение также подчёркивает ценность высококачественной информации об угрозах, о чем свидетельствует отчёт Касперского, который сыграл решающую роль в раскрытии этих действий. Ведомства признают необходимость понимания и смягчения последствий таких разведывательных данных для национальной безопасности.

8) Размышления

- **Схожий характер кибер-операций США**: это подчёркивает, что кибер-операции США не являются прерогативой какого-либо одного агентства. Вместо этого они предполагают сотрудничество между различными разведывательными агентствами, включая АНБ и ЦРУ. Такой совместный подход типичен для сложных кибер-операций, требующих широкого спектра навыков и ресурсов, которыми ни одно ведомство не может эффективно управлять в одиночку.
- **Роль IOC ЦРУ**: Центр информационных операций ЦРУ (IOC) выделяется как важный участник деятельности, приписываемой the Equation. Участие ЦРУ предполагает, что операции Equation имеют более широкую основу в разведывательном сообществе США, чем считалось ранее.
- **Неверная атрибуция**: проблемы и потенциальные неточности, связанные с приписыванием кибератаки конкретным группам или агентствам из-за секретного характера разведывательной деятельности и сложных технических особенностей кибервойны в т.ч. точное определение ответственности чрезвычайно сложно. Следовательно, существует тенденция чрезмерно упрощать ситуацию, приписывая все передовые кибер-операции АНБ как одному из ведомств, что безусловно не отменяет роли последнего.
- **Общественное восприятие и упрощение СМИ**: Критика СМИ и общественного дискурса часто сосредоточена на их тенденции чрезмерно упрощать повествование о кибер-операциях, приписывая их исключительно АНБ. Это чрезмерное упрощение не учитывает сложную реальность межведомственного сотрудничества и распределённый характер кибератак и возможностей ведения боевых действий.
- **Важность более широкого взгляда**: это требует более глубокого понимания того, как правительство США проводит кибер-операции. Признание участия различных агентств, помимо АНБ, важно для полного понимания возможностей и стратегий США в киберпространстве.

D. «Вместо заключения»

- **Идентификация группы Equation**: Группа Equation идентифицирована как очень сложная и продвинутая постоянная угроза, в первую очередь связанная с подразделением специализированных операций доступа (ТАО) АНБ. Эта группа активно занималась кибершпионажем и кибервойной, используя сложные инструменты и методы для проникновения в широкий круг целей по миру.
- **Последствия утечек**: Утечки Shadow Brokers в 2016 году, раскрыли важные детали об операциях Equation, включая использование сложных инструментов, таких как Bvp47. Эти утечки подтвердили связь группы с АНБ и выявили широкий охват их кибер-операций, затронувших более 287 целей в 45 странах.
- **Техническая сложность**: Инструменты Equation, такие как Bvp47, продемонстрировали расширенные возможности при сетевых атаках, оснащённых уязвимостями 0day. Их операции характеризовались высокой степенью скрытности и технической изощрённости, что делало их доминирующей силой в противостояниях в киберпространстве на национальном уровне.
- **Глобальное воздействие и жертвы**: Глобальное воздействие деятельности Equation было огромным, жертвы были в разных странах, что указывает на стратегический и широкомасштабный характер их кибер-операций. Это включало использование систем жертв в качестве переходных серверов для дальнейших атак, что подчёркивало стратегическую глубину их операций.

Руководство по выбору безопасных и доверенных технологий

Аннотация – документ "Choosing Secure and Verifiable Technologies" содержит анализ основных аспектов выбора защищённых цифровых продуктов и услуг и охватывает различные области, включая принципы безопасности при проектировании, прозрачность производителя, управление рисками, риски цепочки поставок и рекомендации после покупки, такие как политика технического обслуживания и окончания срока службы. Каждый раздел предлагает подробное изучение стратегий и практик, повышающих безопасность и достоверность технологических закупок.

Этот документ особенно полезен специалистам по кибербезопасности, ИТ-менеджерам и специалистам по закупкам в различных отраслях. Он служит ценным ресурсом, поскольку в нем описываются необходимые шаги для обеспечения того, чтобы приобретённые технологии не только соответствовали текущим стандартам безопасности, но и соответствовали текущим методам обеспечения безопасности для уменьшения будущих уязвимостей. Этот анализ направлен на принятие обоснованных решений, защищающих данные организации и инфраструктуру от потенциальных киберугроз, тем самым повышая общую устойчивость бизнеса. Интегрируя эти методы, специалисты из различных секторов могут значительно снизить риски, связанные с цифровыми технологиями, и повысить безопасность их эксплуатации.

A. Введение

Документ “Choosing Secure and Verifiable Technologies” содержит всеобъемлющее руководство для организаций по приобретению цифровых продуктов и услуг с акцентом на безопасность, начиная с этапа проектирования и заканчивая жизненным циклом технологии.

В документе подчёркивается критическая важность выбора технологий, которые по своей сути являются безопасными, для защиты конфиденциальности пользователей и данных от растущего числа киберугроз. В нем излагается ответственность клиентов за оценку безопасности, пригодности и связанных с ними рисков цифровых продуктов и услуг. ИТ-отдел выступает за переход к продуктам и услугам, которые безопасны как с точки зрения проектирования, так и по умолчанию, подчёркивая преимущества такого подхода, включая повышение устойчивости, снижение рисков и снижение затрат, связанных с исправлениями и реагированием на инциденты.

- **Безопасность по умолчанию**: необходимость проектирования и разработки технологий, обеспечивающих безопасность, является основополагающим элементом безопасности продуктов при минимальной потребности в дополнительных конфигурациях.
- **Процесс закупок**: двухэтапный подход к закупкам – оценка перед включает оценку функций безопасности продукта, прозрачности производителя и постоянной поддержки и обновлений, предоставляемых производителем.
- **Прозрачность производителя**: Организациям рекомендуется оценить приверженность производителя обеспечению безопасности, включая его способность предоставлять информацию о функциях безопасности и уязвимостях продукта. Производители должны придерживаться такой практики, как публикация полных и своевременных материалов.
- **Управление рисками**: важность непрерывного управления рисками как в процессе закупок, так и на протяжении всего жизненного цикла продукта или услуги включает регулярные обновления и исправления от производителя для устранения новых уязвимостей.
- **Риски цепочки поставок:** здесь основное внимание уделяется управлению рисками, связанными с цепочкой поставок, при этом подчёркивается необходимость того, чтобы организации обеспечивали соблюдение их поставщиками проектных принципов безопасности.
- **Управление инцидентами безопасности**: охватывает необходимость эффективного управления инцидентами безопасности и событиями (SIEM) и интеграции управления безопасностью, автоматизации и реагирования (SOAR) для управления потенциальными инцидентами безопасности и смягчения их последствий.
- **Политика жизненного цикла**: необходимость чёткой политики в отношении срока службы продуктов и услуг, включая безопасное удаление данных и переход на новые технологии.
- **Вопросы регулирования и соответствия**: организациям рекомендуется обеспечивать соответствие продуктов и услуг требованиям и стандартам, которые могут варьироваться в зависимости от отрасли и типа обрабатываемых данных.

B. Аудитория

Документ ориентирован на широкую аудиторию в сфере закупок и производства цифровых технологий.:

- **Организации, которые закупают и используют цифровые продукты и услуги**: широкий круг организаций, известных как закупающие организации, закупщики, потребители и заказчики. Эти организации находятся в центре внимания руководства документа, направленного на совершенствование процесса принятия ими решений при закупке цифровых технологий.
- **Производители цифровых продуктов и услуг**: Документ также адресован производителям цифровых технологий, предоставляя им информацию о принципах обеспечения безопасности при разработке. Это предназначено для руководства производителями при разработке технологий, отвечающих ожиданиям их клиентов в области безопасности.

Ключевым сотрудникам, которым рекомендуется ознакомиться с данным руководством и использовать его:

- **Руководители организаций и менеджеры высшего звена**: играют решающую роль в принятии решений и формулировании стратегии для своих организаций.
- **Персонал по кибербезопасности и политике безопасности**: ответственные за обеспечение безопасности цифровых технологий в своих организациях.
- **Команды разработчиков продуктов**: участвуют в создании и разработке цифровых продуктов и услуг, обеспечивая безопасность этих предложений по своей конструкции.
- **Консультанты по рискам и специалисты по закупкам**: консультируют по вопросам управления рисками и специализируются на процессе закупок, гарантируя, что приобретаемые цифровые технологии не представляют неоправданных рисков для организации.

Документ преследует несколько целей:

- Информировать организации о проектных принципах безопасности при приобретении цифровых продуктов и услуг, что приводит к более обоснованным оценкам и решениям.
- Информировать производителей о конструктивных принципах безопасности их продуктов и услуг с целью ускорения разработки безопасных технологий. Это даёт производителям ответы на ключевые вопросы безопасности и ожидания, которые они могут ожидать от своих клиентов.

В документе подчёркивается, что это не контрольный список для получения идеальных результатов цифровых закупок, а скорее руководство, помогающее закупающим организациям принимать обоснованные решения с учётом рисков в их уникальных операционных контекстах. Признается уникальность структуры и подхода каждой организации к закупкам и предполагается, что не каждый пункт документа может иметь отношение к каждой организации. Кроме того, организациям может потребоваться учитывать другие факторы, не описанные в документе, которые могут быть уникальными для их конкретной ситуации или отрасли или региона, в котором они работают.

C. Концепция “Security by design”

Концепция "Security by design" (SbD) — это упреждающий подход, ориентированный на безопасность, применяемый производителями программного обеспечения при разработке цифровых продуктов и услуг. Такой подход требует целенаправленного согласования целей кибербезопасности на всех организационных уровнях, задействованных в производственном процессе.

- **Проактивная интеграция безопасности**: подход требует, чтобы принципы были интегрированы с самого начала процесса разработки продукта, а не добавлялись как запоздалая мысль. Такая интеграция происходит на всех этапах проектирования, разработки и развёртывания.
- **Целенаправленное согласование целей в области кибербезопасности**: подход требует, чтобы цели кибербезопасности согласовывались с самого начала с бизнес-целями и дизайном продукта. Такое согласование гарантирует, что меры безопасности встроены в архитектуру продукта или услуги.
- **Учёт киберугроз**: Производители должны учитывать потенциальные киберугрозы на начальных этапах разработки продукта. Такое прогнозирование позволяет реализовать меры по смягчению последствий на ранних стадиях процесса разработки, снижая вероятность появления уязвимостей в конечном продукте.
- **Конфиденциальность пользователей и защиты данных**: Основной целью подхода является конфиденциальности пользователей и защита данных. Разрабатывая продукты с меньшим количеством уязвимостей, производители повышают безопасность пользовательских данных от несанкционированного доступа и потенциальных утечек.
- **Руководство для закупающих организаций**: Понимание принципов подхода имеет решающее значение для организаций, закупающих цифровые продукты и услуги. Эти знания помогают им принимать обоснованные решения, гарантируя, что приобретаемые ими продукты построены с учётом безопасности в качестве основополагающего элемента

D. Изменение баланса рисков кибербезопасности

Рассматриваемый документ ссылается на другой “Choosing Secure and Verifiable Technologies” от Агентства по кибербезопасности и инфраструктурной безопасности (CISA), и представляет собой совместную работу, направленную на руководство производителями

технологий в повышении безопасности их продуктов. Эта публикация представляет собой международную попытку уменьшить уязвимости, которые могут быть использованы в технологиях, используемых как государственными, так и частными организациями. Документ поддерживается коалицией агентств глобальной безопасности, включая CISA, Федеральное бюро расследований (ФБР), Агентство национальной безопасности (АНБ) и международных партнёров из Австралии, Канады, Новой Зеландии, Соединённого Королевства, Германии и Нидерландов.

1) Основополагающие принципы

- **Ответственность за результаты обеспечения безопасности клиентов**: производителям рекомендуется уделять приоритетное внимание безопасности своих клиентов, интегрируя принципы безопасности с начальных этапов разработки продукта. Этот принцип подчёркивает важность разработки продуктов, которые по своей сути являются безопасными, тем самым снижая риск киберугроз для конечных пользователей.
- **Радикальная прозрачность и подотчётность**: принцип призывает производителей быть открытыми и прозрачными в отношении функций безопасности своей продукции. Он призывает раскрывать потенциальные уязвимости и шаги, предпринятые для их устранения, способствуя формированию культуры подотчётности.
- **Безопасность — это бизнес-цель**: В техническом документе подчёркивается важнейшая роль руководителей высшего звена во внедрении безопасности в корпоративную культуру. Это предполагает, что руководство должно отстаивать безопасность как основную бизнес-цель, гарантируя, что она будет считаться приоритетной на протяжении всего жизненного цикла разработки продукта.

2) Воздействие и реализация

Документ предоставляет производителям план разработки продуктов, безопасных с точки зрения проектирования и по умолчанию, обеспечивающих защиту от распространённых киберугроз без необходимости дополнительных настроек или затрат для конечных пользователей. Это предполагает, что принятие этих принципов может переложить бремя обеспечения безопасности с потребителей на производителей, снижая вероятность инцидентов безопасности, возникающих в результате распространённых проблем, таких как неправильная конфигурация или задержка с исправлением.

Кроме того, в документе подчёркивается необходимость стратегического внимания к безопасности программного обеспечения, призывая производителей идти на сложные компромиссы и инвестиции, включая внедрение языков программирования, которые смягчают распространённые уязвимости, и отдавать приоритет безопасности, а не привлекательным, но потенциально рискованным функциональным возможностям их продуктов.

E. Категории цифровых продуктов и услуг

Различные категории цифровых продуктов и услуг подчёркивают важность понимания этих категорий для обеспечения безопасной закупки и использования.

1) Программное обеспечение

- **Определение**: Программное обеспечение охватывает все типы программ и прикладных программ, включая операционные системы и встроенные системы.
- **Проприетарное программное обеспечение**: это программное обеспечение, разработанное производителями и распространяемое по специальным соглашениям о лицензировании или покупке. Он часто имеет ограничения, такие как ограничения пользователей и запреты на перепродажу или модификацию.
- **Программное обеспечение с открытым исходным кодом (OSS)**: OSS включает программное обеспечение с исходным кодом, которое находится в свободном доступе по открытой лицензии, позволяющей любому просматривать, использовать, изучать или изменять его. Управляемая сообществом волонтёров, OSS способствует быстрой разработке продукта благодаря своему характеру сотрудничества.

2) Встроенное программное обеспечение и микропрограммное обеспечение

- **Встроенное программное обеспечение**: это программное обеспечение управляет встроенными системами, предназначенными для выполнения определённых функций в рамках более крупных систем, обычно ограниченных доступными вычислительными ресурсами и предназначенных для операций в режиме реального времени.
- **Прошивка**: Тип встроенного программного обеспечения, прошивка постоянно хранится в энергонезависимой памяти устройства и обеспечивает низкоуровневый контроль над аппаратными компонентами устройства.

3) Спецификация программного обеспечения (SBOM)

- **Функциональность**: SBOM содержит список программных компонентов или библиотек, составляющих программный пакет. Это применимо ко всем типам программного обеспечения, включая проприетарное, операционное, встроенное и прошивное.
- **Полезность**: Спецификации SBOM помогают производителям и потребителям идентифицировать компоненты и их версии в продукте, облегчая мониторинг обновлений и уязвимостей. Спецификации SBOM обычно являются машиночитаемыми для поддержки автоматического мониторинга и отчётности.

4) Аппаратное обеспечение

- **Область применения**: Аппаратное обеспечение включает любое физическое устройство, предназначенное для обработки, хранения или

передачи данных. К этой категории относятся сетевые устройства (например, брандмауэры, маршрутизаторы), устройства хранения данных и серверы.

- **Спецификация оборудования (HBOM)**: HBOM описывает физические компоненты, из которых состоит аппаратное устройство. Это крайне важно для понимания материалов, используемых в оборудовании, и оценки потенциальных рисков цепочки поставок.

5) Интернет вещей (IoT)

IoT обычно относится к аппаратному обеспечению и включает устройства и датчики, которые подключаются к Интернету для обмена данными и обеспечения функциональности. В эту категорию входят потребительские товары, медицинские устройства и операционные технологии.

6) Облачные сервисы

Поставщики облачных услуг предлагают вычислительные ресурсы по запросу, включая инфраструктуру, платформу, хранилище, сетевые услуги и обработку данных. Здесь применяются принципы безопасности, аналогичные при закупке программного обеспечения и оборудования.

7) Программное обеспечение как услуга (SaaS)

SaaS позволяет потребителям использовать программное обеспечение без необходимости устанавливать его самостоятельно или управлять им. Это снижает накладные расходы на управление и инфраструктуру и может предлагаться по различным соглашениям, включая бесплатный доступ.

8) Поставщики управляемых услуг (MSP)

MSP предоставляют специализированные услуги, помогающие организациям управлять облачной инфраструктурой, обеспечивать её безопасность и оптимизировать. Услуги включают управление облачной инфраструктурой, безопасность, резервное копирование и восстановление данных, что позволяет клиентам сосредоточиться на основных видах деятельности

F. Внешние закупки

Внешние закупки подразделяются на этапы перед покупкой и после покупки для обеспечения безопасных и обоснованных решений при приобретении цифровых продуктов и услуг.

1) Этап пред-покупки

Этап фокусируется на нескольких ключевых областях для обеспечения того, чтобы организации делали осознанный и безопасный выбор при приобретении цифровых продуктов и услуг.

a) Прозрачность и отчётность

- Организациям следует проверять прозрачность информации, предоставляемой производителями, которая может включать отраслевые отчёты, независимое тестирование и обновления функций безопасности.
- Ожидается, что производители будут уведомлять клиентов о любых обнаруженных уязвимостях и предоставлять рекомендации по их устранению, в идеале без каких-либо дополнительных затрат.
- Публикация полных и своевременных отчётов об общих уязвимостях и разоблачениях (CVE) имеет решающее значение для поддержания прозрачности.

b) Защищенный по умолчанию

- Продукты должны быть безопасными "из коробки", требуя от потребителя минимальной настройки системы безопасности для безопасной эксплуатации.
- Функции защиты по умолчанию могут включать многофакторную аутентификацию и ведение журнала безопасности с настройками по умолчанию, настроенными на самый высокий уровень безопасности.

c) Требования безопасности

- Организации должны определять и понимать свои конкретные потребности в области безопасности, чтобы гарантировать соответствие закупаемых продуктов этим требованиям.
- Использование стандартов шифрования и управление идентификационными данными.

d) Управление рисками в цепочке поставок

- Оценка безопасности цепочки поставок производителя имеет жизненно важное значение, поскольку уязвимости могут быть унаследованы закупающей организацией.
- У производителей должен быть план управления рисками в цепочке поставок для устранения потенциальных рисков.

e) Использование программного обеспечения с открытым исходным кодом

- Следует тщательно контролировать использование программного обеспечения с открытым исходным кодом (OSS), чтобы избежать рисков для безопасности.
- Производителям следует обеспечивать регулярное обновление компонентов OSS и их безопасность.

f) Обмен данными и суверенитет

- Понимание того, какие данные будут переданы, как они будут использоваться производителем, и обеспечение соблюдения законов о защите данных имеют решающее значение.
- Учитывается географическое расположение, в котором хранятся и обрабатываются данные.

g) Процесс разработки

- Организациям следует убедиться в том, что производители придерживаются безопасных методов разработки.

- Учитывается, разрабатываются ли продукты в безопасной среде и соответствуют ли они соответствующим стандартам.

h) Геополитические риски

- Производители должны осознавать геополитические риски, которые могут повлиять на их продукцию и услуги, и управлять ими.
- Учитывается понимание политической стабильности регионов, где они работают, и их цепочек поставок.

i) Регулируемые Отрасли

Продукты должны оцениваться на соответствие конкретным нормативным требованиям, относящимся к отрасли, в которой они используются.

j) Доступ к производителю

- Оценка необходимости и безопасности доступа любого производителя к системам организации.
- Учитывается как удалённый, так и физический контроль доступа.

k) Внутренняя угроза

- Учёт потенциальных рисков, исходящие от инсайдеров в организации производителя, которые могут нанести вред закупающей организации.
- Должны быть внедрены такие средства контроля, как надёжная практика найма и мониторинг.

l) Открытые стандарты

- Использование открытых стандартов способствует интероперабельности и снижает риск привязки к поставщику.
- Организациям следует проверять соответствие продукции этим стандартам.

m) Подключенные системы

Понимание всех систем, к которым будет подключаться продукт, важно для оценки потенциальных рисков и эффективного управления ими.

n) Ценность продукта

Оценка ценности продукта, включая его стоимость, ожидаемый срок службы и уровень безопасности, который он обеспечивает организации, имеет решающее значение для принятия обоснованных решений о закупках

2) Этап после покупки

На этапе рассматриваются несколько важнейших аспектов управления цифровыми продуктами и услугами после приобретения. Эти аспекты имеют решающее значение для обеспечения постоянной безопасности, соответствия требованиям и операционной эффективности.

a) Управление рисками

- Организации должны обеспечивать непрерывное управление рисками для устранения новых и эволюционирующих угроз.
- Регулярные оценки и обновления необходимы для адаптации к изменениям в ландшафте угроз и поддержания целостности безопасности технологии на протяжении всего её жизненного цикла.
- Управление инцидентами безопасности, организация безопасности, автоматизация и реагирование на них (SIEM и SOAR)
- Интеграция решений SIEM и SOAR жизненно важна для эффективного обнаружения и устранения вредоносных действий.
- Для оптимальной работы этим инструментам требуются подробные журналы из приложений, и производителям следует сотрудничать с поставщиками SIEM и SOAR, чтобы убедиться, что их продукты регистрируют достаточный объём информации.

b) Техническое обслуживание

- Организации должны проверять соблюдение производителями обязательств по техническому обслуживанию, заявленных на этапе закупок.
- Это включает предоставление своевременных обновлений и исправлений, а также поддержку для устранения любых уязвимостей, обнаруженных после покупки.

c) Контракты, лицензирование и Соглашения об уровне обслуживания

- Важно обеспечить соблюдение производителем всех договорных обязательств и соглашений об уровне обслуживания.
- Организациям следует регулярно проверять эти соглашения, чтобы подтвердить текущее соответствие и учесть любые изменения, которые влияют на качество обслуживания и безопасность.

d) Направляющие для ослабления

- Производители должны предоставлять руководства с подробным описанием параметров конфигурации, которые пользователи могут изменять в продукте.
- В этих руководствах должны быть объяснены последствия для безопасности изменения конфигураций по сравнению с настройками по умолчанию и предложены возможные компенсирующие меры безопасности.

e) Конец жизненного цикла

- Процессом окончания срока службы продукта следует управлять осторожно, чтобы избежать рисков безопасности, связанных с неподдерживаемыми или устаревшими технологиями.
- Организациям следует планировать безопасную утилизацию или передачу продукта в конце срока его службы, гарантируя, что все данные будут надлежащим образом обрабатываться и что продукт будет выведен из эксплуатации способом, обеспечивающим безопасность

G. Внутренние закупки

Внутренние закупки подразделяются на три этапа: перед закупкой, закупка и после закупки. На каждом этапе рассматриваются конкретные аспекты, которые организациям необходимо учитывать внутри компании при закупке цифровых продуктов и услуг.

1) Этап пред-покупки

Этап направлен на обеспечение соответствия внутренних аспектов организации закупкам цифровых продуктов и услуг. Этот этап включает консультации и оценки в различных отделах организации, чтобы убедиться в том, что рассматриваемый продукт или услуга соответствует организационным потребностям и стандартам безопасности.

a) Высшее руководство

- **Оценка и утверждение рисков**: Высшее руководство несёт ответственность за установление порогового значения организационного риска и утверждение закупок на основе комплексной оценки рисков. Это включает в себя понимание потенциальных рисков, связанных с продуктом или услугой, и обеспечение того, чтобы они находились в приемлемых пределах.

- **Включение плана реагирования на инциденты**: для высшего руководства крайне важно обеспечить включение продукта или услуги в план реагирования на инциденты организации, что указывает на готовность к потенциальным инцидентам безопасности.

b) Политика

- **Соответствие политике**: Закупки должны оцениваться в соответствии с существующими политиками, чтобы убедиться в отсутствии конфликтов. Это включает проверку того, что уровень риска, связанный с продуктом или услугой, не превышает принятые организацией пороговые значения риска.

- **Соответствие нормативным и законодательным требованиям**: Продукт или услуга должны соответствовать всем соответствующим требованиям к регистрации и аудиту, которые могут быть продиктованы законодательными или регулирующими стандартами. Это обеспечивает соответствие требованиям и способствует плавной интеграции продукта или услуги в деятельность организации.

c) Инфраструктура и безопасность

- **Совместимость средств контроля безопасности**: Существующие средства контроля безопасности, структуры или стандарты, которых придерживается организация, должны быть совместимы с новым продуктом или услугой. Для оценки этой совместимости следует завершить оценку воздействия на безопасность.

- **Моделирование угроз**: следует разработать тщательную модель угроз для выявления соответствующих угроз и рисков, гарантируя, что управление ими осуществляется на приемлемом уровне. Это помогает понять, как продукт или услуга впишутся в существующую инфраструктуру и какие корректировки могут потребоваться.

d) Владелец продукта

- **Потребности бизнеса и толерантность к риску**: Владелец продукта должен оценить, соответствует ли продукт потребностям бизнеса, не превышая толерантность организации к риску. Это включает в себя оценку уровня секретности, которому должна соответствовать покупка.

- **Контракт и снижение рисков**: контракт должен охватывать приемлемый уровень риска и включать соответствующие меры по снижению рисков. Владелец продукта играет решающую роль в обеспечении соответствия условий контракта и разработке плана снижения рисков

2) Этап покупки

Этап включает критические оценки и решения, которые обеспечивают соответствие процесса закупок целям организации и требованиям безопасности.

a) Высшее руководство

- **Принятие решений и принятие рисков**: Высшее руководство несёт ответственность за окончательную доработку решений о закупках. Это включает принятие любых остаточных рисков, выявленных в процессе закупок, и обеспечение того, чтобы эти риски находились в пределах допустимого риска организации.

- **Утверждение контрактов**: Высшее руководство играет решающую роль в рассмотрении и утверждении окончательных контрактов, гарантируя, что все условия соответствуют требованиям организации и что контракты обеспечивают надлежащую защиту и ценность.

b) Системное администрирование

- **Проверка технических спецификаций**: Системным администраторам поручено проверять, соответствуют ли технические спецификации закупаемых продуктов или услуг требованиям организации. Это включает в себя подтверждение правильности реализации всех системных конфигураций, интеграций и пользовательских настроек.

- **Проверки безопасности и соответствия требованиям**: они гарантируют соответствие новых систем существующим политикам и стандартам безопасности. Системные администраторы также играют определённую роль в настройке новых систем для поддержания безопасности и операционной эффективности.

c) Инфраструктура и безопасность

- **Интеграция и совместимость**: основное внимание уделяется обеспечению того, чтобы новые системы закупок беспрепятственно интегрировались с существующей инфраструктурой без ущерба для безопасности или производительности. Это

включает в себя проведение детальных проверок совместимости и планирование любых необходимых обновлений инфраструктуры.

- **Текущие оценки безопасности**: после интеграции крайне важно постоянно оценивать состояние безопасности интегрированных систем для оперативного выявления любых возникающих рисков и смягчения их последствий.

d) Владелец продукта

- **Соответствие потребностям бизнеса**: Владелец продукта гарантирует, что закупаемые продукты или услуги соответствуют потребностям бизнеса и стратегическим целям. Это включает в себя проверку соответствия функций и возможностей продукта указанным требованиям.

- **Управление жизненным циклом продукта**: владелец отвечает за надзор за жизненным циклом продукта от закупки до развёртывания и далее, гарантируя, что продукт продолжает удовлетворять потребности организации по мере их развития

3) Этап после покупки

Этап включает в себя обеспечение того, чтобы приобретённые цифровые продукты и услуги по-прежнему соответствовали целям организации в области безопасности, оперативным и стратегическим целям. Этот этап требует постоянных оценок и управленческих практик для устранения любых возникающих рисков или изменений в среде организации или продукта.

a) Высшее руководство

- **Постоянное принятие и анализ рисков**: Высшее руководство должно установить процесс для постоянного или периодического принятия и анализа рисков продукта. Это включает в себя обеспечение того, чтобы управление рисками продукта осуществлялось в реестре рисков организации, а планы обеспечения безопасности системы и непрерывности бизнеса обновлялись и принимались.

- **Управление устаревшими технологиями**: Высшее руководство также должно учитывать риски, связанные с устаревшими технологиями, обеспечивая их документирование и надлежащее управление в рамках системы управления рисками организации.

b) Системное администрирование

- **Мониторинг обновлений системы безопасности**: Системные администраторы отвечают за настройку систем мониторинга и уведомлений об исправлениях, CVE и обновлениях продуктов, включая те, которые связаны со всей цепочкой поставок. Это гарантирует, что организация по-прежнему осведомлена о новых уязвимостях или обновлениях и может реагировать на них.

- **Интеграция с SIEM и SOAR**: Продукт должен быть интегрирован в систему организации SIEM (информация о безопасности и управление событиями), и, если применимо, должны быть предоставлены возможности SOAR (управление безопасностью, автоматизация и реагирование). Эта интеграция помогает обнаруживать инциденты безопасности и реагировать на них.

- **Процедуры управления данными**: Процедуры управления данными, включая удаление, редактирование и резервное копирование, должны быть установлены и соблюдаться для защиты целостности и конфиденциальности данных.

- **Включение плана реагирования на инциденты**: Новый продукт или услуга должны быть включены в план реагирования на инциденты организации, гарантируя наличие конкретных стратегий реагирования.

c) Инфраструктура и безопасность

- **Периодический пересмотр разрешений**: Организации следует периодически проверять разрешения и учётные записи с привилегиями, чтобы гарантировать, что средства контроля доступа остаются надлежащими и безопасными.

- **Проверка сертификатов безопасности производителя**: Сертификаты безопасности производителя следует периодически проверять на наличие обновлений, чтобы убедиться, что продукт продолжает соответствовать требуемым стандартам безопасности.

- **Управление устаревшими и новыми технологиями**: Организация план поддержки для управления как устаревшими, так и новыми технологиями, гарантирующий учёт рисков безопасности и эксплуатации.

d) Владелец продукта

- **Соблюдение производителем требований**: Владелец продукта должен убедиться, что производитель продолжает соблюдать требования по безопасности и эксплуатации, сделанные на этапе покупки.

- **Периодические проверки контрактов**: Контракты и соглашения об уровне обслуживания с производителем следует периодически пересматривать, чтобы обеспечить постоянное соответствие требованиям и учитывать любые изменения в потребностях организации или характеристиках продукта.

- **Оценка рисков изменений**: Любые изменения в продукте, включая обновления или изменения конфигурации, должны подвергаться оценке рисков, чтобы убедиться, что они не привносят новых уязвимостей или не ставят под угрозу безопасность.

- **Разработка планов обеспечения непрерывности и безопасности**: Владелец продукта должен обеспечить разработку и поддержание планов обеспечения непрерывности бизнеса и системной безопасности с учётом как нормативных, так и законодательных требований

Система компетенций Европола по борьбе с киберпреступностью 2024

Аннотация – в документе представлен анализ "Europol Cybercrime Training Competency Framework 2024", направленного на расширение возможностей академических, правоохранительных, криминалистических х и учреждений в борьбе с киберпреступностью. Рассматриваются различные критические аспекты системы, включая определение основных наборов навыков для ключевых участников, участвующих в противодействии киберпреступности, процесс разработки системы и её стратегический контекст в рамках более широкой стратегии ЕС по борьбе с организованной преступностью на 2021–2025 годы.

Документ служит ценным ресурсом для понимания подходов к подготовке сотрудников правоохранительных и судебных органов к киберпреступности и реагирования на них и наращивания потенциала в борьбе с киберпреступностью, способствуя тем самым безопасности и устойчивости цифровых пространств по всему ЕС и за его пределами.

A. Введение

Документ "Europol Cybercrime Training Competency Framework 2024" охватывает широкий спектр материалов и, связанных с обучением по борьбе с киберпреступностью, рамками компетенций, стратегиями и законодательством. Эти материалы (как подборка от Европола) в совокупности направлены на расширение возможностей, судебных и правоохранительных органов и других заинтересованных сторон в эффективной борьбе с киберпреступностью.

Ключевые аспекты включают подход и сферу охвата программы детализации функциональных компетенций, необходимых правоохранительным органам и судебной системе, а также гибкость и адаптируемость программы к различным организационным структурам, а также конкретные роли, обозначенные в рамках концепции, такие как, среди прочего, руководители подразделений по борьбе с киберпреступностью, руководители групп, криминалисты и специализированные эксперты по борьбе с киберпреступностью.

- **Система компетенций Европола по обучению борьбе с киберпреступностью:** описывает наборы навыков, необходимых для различных должностей в правоохранительных и судебных органах для эффективной борьбы с киберпреступностью. Подчёркивается важность цифровой криминалистики, расследований сетевых инцидентов, программирования и специальных знаний о киберпреступности среди других навыков.
- **Инициативы Европейского союза**: Документы подчёркивают усилия ЕС по укреплению возможностей борьбы с киберпреступностью с помощью EC3 (Европейского центра по борьбе с киберпреступностью) и сотрудничества с такими организациями, как CEPOL и ECTEG в части обучения, оперативной поддержки и разработки согласованной правовой базы для борьбы с киберпреступностью.
- **Глобальные и национальные стратегии**: В различных источниках обсуждаются глобальные и национальные стратегии в области законодательства о киберпреступности и наращивания потенциала. ITU Toolkit по законодательству о киберпреступности и руководство Интерпола по национальной стратегии борьбы с киберпреступностью содержат руководящие принципы для разработки эффективных законов и стратегий в области киберпреступности. В этих стратегиях подчёркивается необходимость гармонизации законов, наращивания потенциала органов уголовного правосудия и международного сотрудничества.
- **Обучение**: Важность подготовки при расследовании киберпреступлений подчёркивается в нескольких источниках. Национальный учебный центр по борьбе с киберпреступностью (CyTrain) и орган по расследованию киберпреступлений (CIBOK) предлагают специализированное обучение для сотрудников правоохранительных органов и других заинтересованных сторон. Эти учебные программы охватывают различные аспекты расследования киберпреступлений, включая цифровую криминалистику, анализ разведданных и управление.
- **Сотрудничество и обмен информацией**: Необходимость сотрудничества между правоохранительными органами, частным сектором, научными кругами и международными организациями является постоянной темой. Эффективная борьба с киберпреступностью требует междисциплинарного подхода, обмена передовым опытом и использования экспертных знаний из различных секторов.
- **Законодательство и правовые рамки**: отмечаются проблемы и рекомендации по обновлению правовых рамок для эффективной криминализации

киберпреступлений и судебного преследования за них. Подчёркивается необходимость принятия законов, идущих в ногу с технологическими достижениями и способствующих международному сотрудничеству.

- **Наращивание потенциала и распределение ресурсов**: подчёркивается необходимость наращивания потенциала правоохранительных и судебных органов посредством обучения, предоставления технических ресурсов и создания специализированных подразделений для рассмотрения дел о киберпреступлениях. Это включает в себя устранение пробелов в навыках, знаниях и технологиях

B. Фреймворк

- **Цель**: направленность на определение необходимых наборов навыков для ключевых участников, участвующих в борьбе с киберпреступностью. Является руководством для правоохранительных органов, судебных органов и академических учреждений по пониманию компетенций, необходимых для эффективного противодействия растущей угрозе киберпреступности.
- **Процесс разработки**: Структура была разработана после процесса консультаций с участием многих заинтересованных сторон. Сюда вошли материалы различных европейских органов, таких как Агентство Европейского союза по подготовке сотрудников правоохранительных органов (CEPOL), Европейская группа по обучению и просвещению в области киберпреступности (ECTEG), Евроюст, Европейская судебная сеть по борьбе с киберпреступностью (EJCN) и представители, назначенные Целевой группой Европейского союза по борьбе с киберпреступностью (EUCTF).
- **Стратегический контекст**: обновлённая структура является частью плана действий Европейской комиссии, направленного на укрепление потенциала правоохранительных органов в цифровых расследованиях. Это согласуется со Стратегией ЕС по борьбе с организованной преступностью на период 2021–2025 годов.
- **Сфера применения и ограничения**: Система фокусируется на уникальных навыках, имеющих отношение к расследованиям киберпреступлений и работе с цифровыми доказательствами. Она не охватывает все навыки, необходимые для выполнения описанных ролей, но подчёркивает те, которые характерны для киберпреступности. Структура не является исчерпывающим перечнем навыков или одобрением структуры конкретного подразделения или профилей сотрудников. Он предназначен для наращивания стратегического потенциала в организационных структурах правоохранительных органов и судебной системы.
- **Гибкость и адаптация**: В зависимости от организационной структуры и штатного расписания роли и соответствующие наборы навыков, изложенные в структуре, могут быть объединены или переданы на аутсорсинг специализированным подразделениям, таким как уголовный анализ и криминалистика.
- **Функциональные компетенции**: Структура определяет основные функциональные компетенции, необходимые правоохранительным органам для эффективной борьбы с киберпреступностью. Особое внимание уделяется конкретным навыкам, необходимым для расследования киберпреступлений и обращения с цифровыми доказательствами, а не общим навыкам правоохранительных органов.
- **Неполный список навыков**: не предоставляется исчерпывающего списка навыков, но фокусируется на тех, которые имеют уникальное отношение к расследованиям киберпреступлений. Такой подход позволяет целенаправленно развивать компетенции, наиболее важные в контексте киберпреступности.
- **Наращивание стратегического потенциала**: предназначение в качестве инструмента для наращивания стратегического потенциала в правоохранительных и судебных учреждениях направленность на повышение компетентности, имеющей решающее значение для эффективного рассмотрения дел о киберпреступлениях.
- **Исключение общих навыков**: Общая подготовка сотрудников правоохранительных органов, управленческие навыки и "софт склиз" не включены в рамки, что гарантирует, что фреймворк ориентирован на специализированные навыки, необходимые для противодействия преступности
- **Процесс разработки**: фреймворк разработан с помощью комплексного процесса, который включал онлайн-анкеты, очный семинар и анализ ответов заинтересованных сторон. Такой совместный подход обеспечил отражение текущих потребностей и будущих требований правоохранительных органов и академических учреждений.
- **Матрица компетенций**: Матрица компетенций является центральным элементом структуры, описывающей необходимые роли, наборы навыков и желаемые уровни квалификации для практикующих специалистов. Эта матрица служит наглядным руководством для понимания конкретных компетенций, необходимых для выполнения различных функций в рамках расследований киберпреступлений.
- **Описания ролей**: Подробные описания основных функций и наборов навыков для различных ролей представлены по всему документу. Эти роли включают, среди прочего, руководителей подразделений по борьбе с киберпреступностью,

руководителей групп, криминалистов, аналитиков по киберпреступности и специализированных экспертов. Каждая роль адаптирована для решения конкретных аспектов киберпреступности и обработки цифровых доказательств.

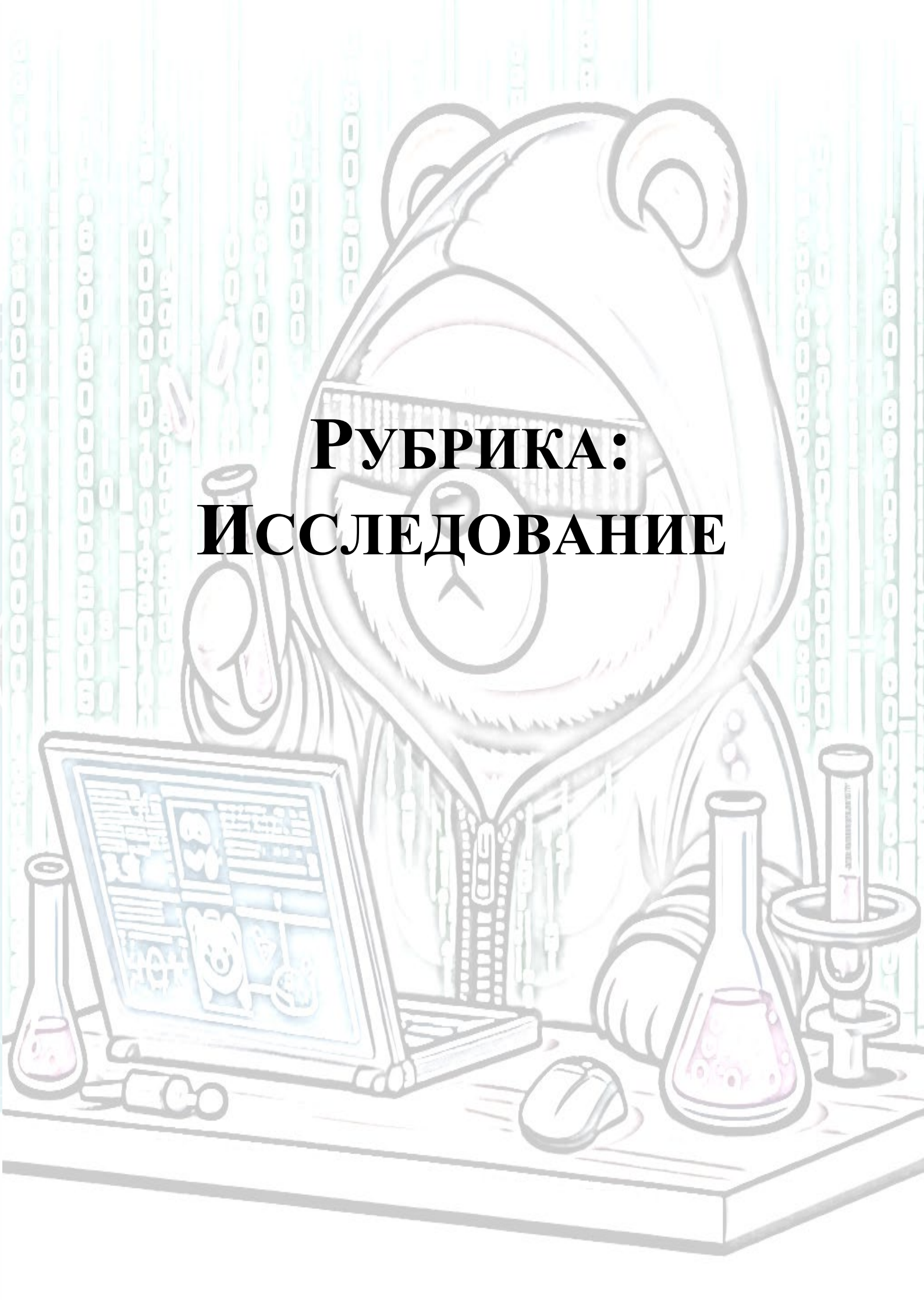
- **Наборы навыков и уровни**: Структура описывает конкретные наборы навыков, необходимые для каждой роли, и желаемые уровни мастерства. Эти наборы навыков включают, среди прочего, цифровую криминалистику, сетевые расследования, программирование и законодательство о киберпреступности. Подчёркивается важность наличия спецнавыков, которые непосредственно применимы к проблемам киберпреступности.

C. Роли

- **Руководители подразделений по борьбе с киберпреступностью**: отвечают за надзор за подразделениями по борьбе с киберпреступностью, принятие обоснованных решений по случаям киберпреступности, координацию ресурсов и расстановку приоритетов в деятельности полиции. Они должны иметь всестороннее представление о возможностях подразделения и обеспечивать необходимое обучение и инструменты для персонала. Навыки эффективного общения и управления взаимоотношениями, особенно на английском языке, необходимы для взаимодействия с международными заинтересованными сторонами.
- **Руководители групп**: руководят расследованиями киберпреступлений в своих конкретных областях. Они контролируют текущие расследования, координируют работу со старшим руководством и обеспечивают, чтобы их команда была оснащена необходимой подготовкой и инструментами. Как и руководителям подразделений, им требуется практический опыт оценки оперативной деятельности и сильные коммуникативные навыки.
- **Криминалисты**: чаще сталкиваются с кибер-элементами в различных преступлениях. Им необходимо фундаментальное понимание цифрового мира, в том числе того, как обращаться с электронными доказательствами на местах преступлений и эффективно использовать разведданные из открытых источников (OSINT).
- **Аналитики по киберпреступности**: Аналитики участвуют в сборе и анализе данных для получения оперативной информации и стратегических выводов. Им необходимо обрабатывать большие объёмы данных из различных источников и преобразовывать их в краткие отчёты. Обмен информацией с более широкой аудиторией и участие в стратегических совещаниях также являются частью их роли.
- **Криминалисты по киберпреступности**: глубоко разбирающиеся в извлечении данных и онлайн-сборе информации, и руководят расследованиями киберпреступлений и часто участвуют в обучении других инструкторов из числа сотрудников правоохранительных органов.
- **Эксперты по киберпреступности**: обладают специализированными знаниями в конкретных областях киберпреступности, таких как OSINT, даркнет, криптовалюты и устройства Интернета вещей. Оказывают оперативную поддержку в расследованиях и должны постоянно совершенствовать свои навыки посредством обмена опытом между коллегами на национальном и международном уровнях.
- **Цифровые криминалисты**: сосредоточены на выявлении, восстановлении и анализе цифровых доказательств. Они знакомы с различными операционными системами, инструментами судебной экспертизы и обладают навыками написания сценариев и программирования. Они также готовят доказательства для сложных задач дешифрования и сообщают о своих выводах.
- **Эксперты по реагированию на кибератаки**: Эти эксперты отвечают за техническое реагирование на кибератаки, сотрудничая с различными заинтересованными сторонами, такими как группы реагирования на компьютерные аварийные ситуации (CERT) и ИТ-отделы. Они несут ответственность за сохранение цифровых доказательств и обеспечение их целостности для судебных процессов.
- **Специалисты первой инстанции**: являются сотрудниками правоохранительных органов, первыми прибывающими на место кибер-инцидента. Им необходимы базовые знания в области цифровой криминалистики и киберпреступности, а в их обязанности входит идентификация и обеспечение сохранности электронных доказательств в соответствии с национальными правилами и передовой практикой.
- **Судьи первой и апелляционной инстанций**: судьям, рассматривающим дела о киберпреступлениях, необходимо эффективно интегрировать кибер-доказательства в судебный процесс. Они должны поддерживать знания о киберпреступности и цифровых доказательствах.
- **Прокуроры и судьи-следователи**: Эти юристы руководят уголовными расследованиями, связанными с кибернетическими элементами, оценивают сбор электронных доказательств и представляют дела в суде. Им требуется базовое понимание цифрового мира и способность использовать разведданные из различных источников, включая OSINT, в дополнение к своим расследованиям

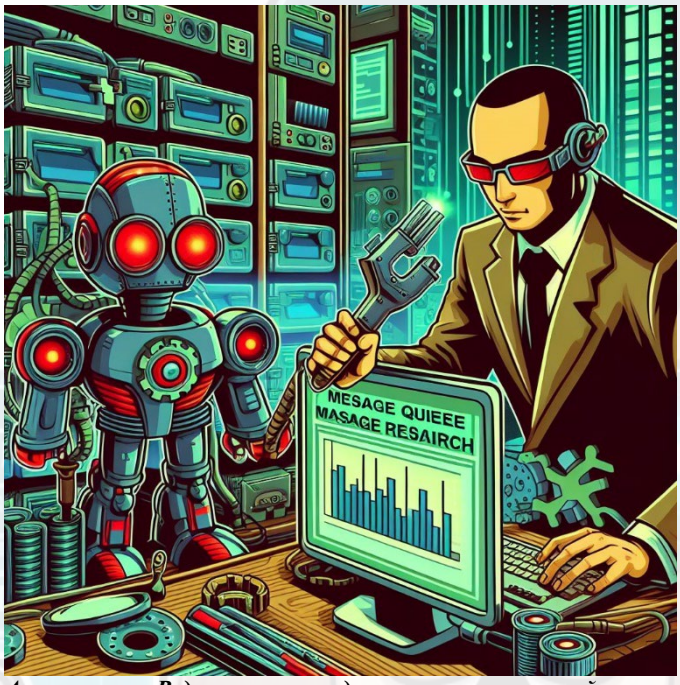
D. Навыки

- **Цифровая криминалистика**: включает идентификацию, сохранение, приобретение, валидацию, анализ, интерпретацию, документирование и представление электронных доказательств из цифровых источников. Ключевые области включают криминалистику данных в реальном времени, облачную, мобильную, сетевую криминалистику, криминалистику ОС, файловой системы, Интернета вещей, и криптографию.
- **Исследование и администрирование сети**: относится к пониманию сетевых функций, проведению расследований внутри сетей и анализу данных о трафике для выявления признаков компрометации. Навыки включают сетевое администрирование, оперативный сбор сетевых данных, сетевую криминалистику и анализ данных о трафике, а также опыт в расследованиях киберпреступлений и хранении доказательств.
- **Программирование и написание сценариев**: используется для построения информационных систем и автоматизации задач для поддержки исследований и анализа данных. Языки программирования включают, среди прочих, Python, JavaScript, Java и C ++. Навыки охватывают разработку бэкенда, фронтэнда и full-стек.
- **Составление отчётов и представление данных расследований киберпреступлений**: включает документацию, составление заметок и составление окончательного отчёта по различным типам отчётов. В нем подчёркивается важность структурированной отчётности, которая является фактической, заслуживающей доверия и приемлемой в суде. Навыки презентации включают синтез информации и адаптацию сложных технических тем для нетехнической аудитории.
- **Анализ и визуализация**: включает применение методов анализа данных для описания, иллюстрации и обобщения данных о киберпреступлениях с целью выявления закономерностей, тенденций и практических знаний. Навыки требуют опыта в области сбора данных, разработки исследований, статистических методов, визуализации передового опыта и этических соображений при обработке данных о преступлениях.
- **Законодательство о киберпреступности**: относится к пониманию законодательства, регулирующего киберпреступную деятельность, включая национальное законодательство о киберпреступности и электронных доказательствах, законы о конфиденциальности, Общие положения о защите данных (GDPR), правила ЕС о хранении данных и решения международных судов.
- **Общие знания о киберпреступности**: охватывает информацию, касающуюся киберпреступлений с поддержкой киберпространства и кибер-зависимости, тенденций киберпреступности, угроз и методов работы, а также понимание кибербезопасности.
- **Специальные знания о киберпреступности**: относятся к уникальным навыкам, полученным в результате специальной подготовки в конкретных областях киберпреступности. Области включают OSINT, даркнет, блокчейны и криптовалюты, анализ вторжений и реагирование на инциденты, этичный взлом, анализ угроз, а также анализ вредоносных программ и обратный инжиниринг.
- **Управление на месте преступления и обработка электронных доказательств**: относится к стандартам и передовой практике выявления и изъятия электронных доказательств на местах преступлений. Навыки включают сбор, упаковку, передачу и хранение устройств, которые могут содержать электронные доказательства, а также проведение опросов на месте происшествия и оказание поддержки жертвам.
- **Методы расследования киберпреступлений**: включает навыки, необходимые для расследования киберпреступлений, такие как методы сбора разведданных, обработка и интерпретация данных, отслеживание подозреваемых онлайн и офлайн, работа под прикрытием онлайн, допрос киберпреступников и управление рисками расследования



Рубрика: Исследование

Анализ рынка MQ: когда простые решения слишком дешёвые, ведь тратить больше - лучше!



Аннотация – В 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.

A. 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.

B. 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
Rabbit MQ	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%

C. Уязвимости брокеров

1) 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): у**язвимость 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.

2) 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): н**екоторые 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): у**язвимость 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: н**ебезопасная 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.

3) ApacheMQ

- **CVE-2023-46604: удалённое выполнение кода (RCE): у**далённое 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: у**язвимость позволяет прошедшим проверку подлинности пользователям выполнять RCE, используя десериализацию данных.
- **CVE-2020-13947: XSS: у**язвимости XSS в WebConsole позволяют удалённо внедрять произвольные веб-скрипты или HTML.
- **CVE-2020-13920: уязвимость JMX MITM: у**язвимость 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: у**язвимость 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.

4) IBM MQ

- **CVE-2022-27780 и CVE-2022-30115: у**язвимости 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: у**язвимости XSS в WebConsole позволяют удалённо внедрять произвольные веб-скрипты или HTML.
- **CVE-2020-13920: уязвимость JMX MITM: у**язвимость 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: у**язвимость 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.

5) *Microsoft Azure Sevice 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.

6) *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-потоки.
- **Уязвимость "Use-After-Free":** уязвимость в NanoMQ версии 0.21.2 вызывает отказ в обслуживании с помощью спец сообщений MQTT.
- **Разыменование нулевого указателя:** уязвимость разыменования 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).

7) *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 очередей 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.

8) *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.

9) Thingsboard

- **CVE-2022-45608: Вертикальное повышение привилегий: у**язвимость 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: у**язвимость 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: у**язвимость 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 серверап:** 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: ис**пользование статического ключа по умолчанию для подписи JWT в ThingsBoard позволяет подделывать действительные запросы и повышать привилегии до версии 3.4.2.

10) 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.

11) 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

12) 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

13) 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

14) 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.

15) 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

16) 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.

D. Рынок MQ-брокеров

1) 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.

a) 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.

b) 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.

c) Количество клиентов

- **Всего компаний: бол**ее 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.

d) Известные Корпоративные Клиенты

- **Alcatel-Lucent: исп**ользует RabbitMQ для различных целей обмена сообщениями.
- **Калифорнийский университет в Сан-Диего:** внедряет RabbitMQ в свои системы.
- **Beckman Coulter: исп**ользует 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.

e) 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).

f) 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.

g) 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.

h) 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.

2) 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.

a) 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.

b) 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 реальном времени 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

c) Количество клиентов

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

d) 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.

e) Распределение компаний по размерам:

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

f) 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.

g) 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.

h) 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.

i) 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.

3) 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.

a) 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.

b) 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.

c) 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.

d) Известные Корпоративные Клиенты

- **Red Hat: исп**ользует 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: исп**ользует Apache ActiveMQ для передачи сообщений.
- **Infosys Ltd:** Крупный клиент, базирующийся в Индии.
- **Fujitsu Ltd: исп**ользует Apache ActiveMQ в Японии.
- **Panasonic Corp**: ещё один клиент в Японии.
- **eBay Inc.: исп**ользует Apache ActiveMQ в США.

e) 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.

f) 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.

g) 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.

h) 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.

i) 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.

j) 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%.

4) 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.

a) 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.

b) 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.

c) 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.

d) Известные Корпоративные Клиенты

- **Capital One: исп**ользует 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: исп**ользует IBM MQ в Японии.
- **Panasonic Corp**.: ещё один крупный клиент Японии.
- **eBay Inc.: исп**ользует IBM MQ в США.

e) Распределение клиентов по размеру компании

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

f) 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.

g) 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.

h) 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.

i) 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.

j) 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.

5) 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.

a) 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.

b) 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

c) 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.

d) 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: исп**ользует Azure Service Bus для обмена сообщениями.
- **Blue Cross Blue Shield**: использует Azure Service Bus для безопасного обмена данными.
- **ASOS.com: исп**ользует Azure Service Bus в Великобритании.
- **Avanade**: использует Azure Service Bus в США.
- **Verra Mobility**: использует Azure Service Bus для транспортировки и логистики.

e) Распределение клиентов по размеру компании

- 1**000-4999 Сотрудников**: 392 компании.

- **100 - 249 Сотрудников**: 335 компаний.
- **20-49 Сотрудников**: 318 компаний.
- **Более 10 000 сотрудников**: 275 компаний.
- **50-99 Сотрудников**: 194 компании.

f) 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.

g) 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.

h) 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.

i) 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.

j) 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.

6) 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 HPE, 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.

a) 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.

b) 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.

c) 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.

d) 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.

e) 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 развертываний 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.

f) 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.

g) 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.

h) 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 развертываний Интернета вещей.

7) 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.

a) 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.

b) 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.

c) 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 развёртываниями.

d) 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.

e) 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.

f) 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.

g) 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.

h) 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.

8) 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.

a) 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 находятся 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.

b) Факторы роста

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

c) 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.

d) 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.

e) Распределение клиентов по размеру компании

- **Корпоративные клиенты:** PubNub доверяют более 500 корпоративных клиентов в критически важных ситуациях, включая известные бренды.
- **Развёртывания кластеров: н**а 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.

f) 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 глобально распределённой сетью с 15 центрами обработки данных, обеспечивая низкую задержку и высокую доступность для клиентов по всему миру.

g) 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.

h) 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.

9) 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.

a) 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.

b) 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

c) 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.

d) 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.: исп**ользует 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.

e) 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 развертываний 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.

f) 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.

g) Отраслевое применение

- **Интеллектуальная энергия**: ThingsBoard используется такими компаниями, как CIRCUTOR, для измерения энергоэффективности и качества электроэнергии.
- **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" развертываний, 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.

h) 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.

10) 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.

a) 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.

b) 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 развертываний IoT

c) 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.

d) 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): исп**ользует 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 Корее**: 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.

e) 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 развертываний 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.

f) 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.

g) 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.

h) 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.

11) 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.

a) 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.

b) 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

c) 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.

d) 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.: исп**ользует 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.

e) Распределение клиентов по размеру компании

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

f) 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).

g) 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.

h) 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.

12) 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.

a) 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.

b) Факторы роста

- **Интеграция со службами Azure**: Бесшовная 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.

c) 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.

d) 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 "Электролюкс"**: использует Azure IoT для управления качеством производственных процессов.

e) Распределение клиентов по размеру компании

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

f) 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).

g) 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.

h) 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.

13) 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.

a) 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.
- **Индия**: 16,58% клиентов Google Cloud IoT находятся в Индии.
- **Германия:** 6,39% клиентов Google Cloud IoT находятся в Германии.

b) 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

c) 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.

d) 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.
- **Apexon**: 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.

e) Распределение клиентов по размеру компании

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

f) 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.

g) 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.

h) 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.

14) 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.

a) 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.

b) 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**: Бесшовная 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.

c) 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.

d) 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.

e) Распределение клиентов по размеру компании

- Более 10 000 сотрудников: 60 компаний.
- 100-249 сотрудников: 30 компаний.
- 20-49 сотрудников: 26 компаний.

f) 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.

g) 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.

h) 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.

i) 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.

15) Cicso 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.

a) 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.

b) 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.

c) 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.

d) 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.

e) 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.

f) 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.

g) 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.

h) 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.

i) 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

Кибербезопасность и Антарктика

Аннотация – быстро и незаметно для мирового сообщества, особенно для той части, которая движет фундаментальную науку вперёд, США приостановили свои научные исследования в невероятно значимом регионе Антарктике. Да, как на колоссальном и почти неисследованном континенте, так и в окружающих морских водах. Причина? Об этом можно догадаться с одной попытки, поскольку это стало обычным явлением для всего мира: нехватка средств. С другой стороны, существует острая необходимость в управлении конкретными кибер-угрозами в Антарктике…

A. Введение

В апреле Национальный научный фонд США (NSF) объявил, что не будет поддерживать какие-либо новые полевые исследования в этом сезоне из-за задержек с модернизацией станции Макмердо. Национальный фонд и береговая охрана США также объявили о сокращениях, которые поставят под угрозу научные и геополитические интересы США в регионе на десятилетия вперёд. В частности, в апреле NSF объявил, что не будет продлевать аренду одного из двух своих антарктических исследовательских судов "Laurence M. Gould". До этого, в октябре 2023 года, NSF объявил, что в ближайшие десятилетия будет эксплуатировать только одно исследовательское судно.

Кроме того, в марте Береговая охрана США объявила, что ей необходимо "пересмотреть базовые показатели" для своей давно отложенной программы Polar Security Cutter, жизненно важной для национальных интересов США на обоих полюсах. Принятые решения, будут иметь серьёзные последствия для деятельности США в Антарктике даже за 2050 годом.

Государственный департамент воздержался от объявления внешнеполитических интересов США в Антарктическом регионе, и Белый дом, похоже, удовлетворён устаревшей и непоследовательной национальной стратегией в отношении Антарктики прошлого века. Конгресс США также не ответил на призывы учёных.

В результате 1 апреля Управление полярных программ NSF объявило, что оно приостанавливает новые предложения по полевым работам на следующие два сезона и не будет запрашивать их в Антарктиде.

Суда, способные работать в полярных морях, становятся все более востребованными, но строить их все труднее. Столкнувшись со значительными проблемами в проекте строительства кораблей и катеров ледового класса, Береговая охрана США объявила в марте, что она "сдвинет базовые сроки" разработки новых проектов ледоколов.

Результатом этих, казалось бы, независимых решений станет сокращение физического присутствия США в Антарктиде. Это будет иметь негативные последствия не только для американских учёных, но и для геополитики США в регионе, особенно учитывая тотальное превосходство России в ледоколах и догоняющее влияние Китая.

США упустили из виду наиболее важные аспекты: адекватное и регулярное финансирование научных исследований в Антарктике, новую национальную стратегию (текущая стратегия была опубликована в июне 1994 года) и понимание законодателями важности интересов и решений США в Антарктике. Неспособность финансировать оперативную и материально-техническую поддержку, необходимую для научных исследований и геополитического влияния США, эффективно означает доминирование России и Китая в антарктическом регионе, поскольку никакая другая страна, включая традиционных участников, таких как Чили, Австралия и Швеция, не может превзойти существующий и растущий научный потенциал России и Китая.

1) Ключевые аспекты

- **США сокращает исследовательские операции в Антарктике**: США объявили о значительном сокращении своих исследовательских операций в Антарктике из-за проблем с финансированием и задержек с модернизацией критически важной инфраструктуры, такой как станция Мак-Мердо. Это включает в себя отказ от продления аренды исследовательского судна Laurence M. Gould и эксплуатацию только одного исследовательского судна в ближайшие десятилетия.
- **Проблемы в программе ледоколов США**: береговая охрана США объявила о задержках в своей программе катеров Polar Security, которая имеет решающее значение для поддержания присутствия и операций США в полярных регионах. Переоценка этой программы указывает на значительные проблемы и потенциальные долгосрочные последствия для возможностей США в Антарктике.
- **Геополитические последствия вывода войск США**: сокращение присутствия США в Антарктике имеет более широкие геополитические последствия,

особенно по мере того, как Россия и Китай продолжают расширять свои возможности и влияние в регионе. Отсутствие современной национальной стратегии и адекватного финансирования антарктических операций ставит США в невыгодное положение.

- **Влияние на научные исследования**: приостановление новых предложений NSF о проведении полевых работ повлияет на научные исследования в Антарктиде, задерживая важные исследования и потенциально приводя к потере ценных данных. Это решение выдвигает на первый план более широкую проблему финансирования и поддержки научных начинаний в отдалённых регионах.

B. Влияние

Решение США приостановить научные исследования в Антарктиде вызвало различные реакции со стороны других стран, особенно тех, у которых есть значительные интересы и операции в регионе. Это решение, обусловленное бюджетными ограничениями и задержками в модернизации критически важной инфраструктуры, имеет не только геополитические последствия.

1) Геополитические последствия

a) Снижение влияния США:

- Сокращение присутствия США придаст смелости другим странам преследовать свои индивидуальные интересы в Антарктике.

b) Активизация действий соперничающих держав

- **Китай**: Китай расширяет своё присутствие в Антарктиде, и отступление США ускорит эту тенденцию. Китай недавно открыл свою пятую исследовательскую станцию в Антарктиде и наращивает научный и логистический потенциал в регионе. Расширение деятельности Китая вызывает обеспокоенность по поводу потенциальных технологий двойного назначения, которые могут служить как научным, так и военным целям. Растущее влияние Китая в Антарктиде может изменить баланс сил и усилить геополитическую напряжённость.

- **Россия**: Россия также наращивает свою деятельность в Антарктике, включая создание новых исследовательских станций. Прогресс России в области ледокольных технологий и её стратегическое позиционирование в регионе будут подкреплены сокращением присутствия США. Это приведёт к усилению доминирующей роли России в управлении Антарктидой и научных исследованиях, что ещё больше бросит вызов интересам США.

c) Реакция партнёров

- **Австралия**: Австралия, ключевой игрок в делах Антарктики, выразила обеспокоенность по поводу решения США. Австралия активно участвует в исследованиях и управлении Антарктикой и полагается на международное сотрудничество для достижения своих научных и экологических целей. Отступление США может побудить Австралию увеличить собственные инвестиции в исследования и укрепить партнёрские отношения с другими странами, чтобы «заполнить пустоту», оставленную США

- **Великобритания**: Великобритания также внесла значительный вклад в исследования в Антарктике. Страна стремится расширить своё научное присутствие и сотрудничество с другими странами для обеспечения дальнейшего прогресса в исследованиях. Правительство Великобритании подчеркнуло важность сохранения сильного международного присутствия в Антарктике для решения глобальных экологических проблем и соблюдения принципов системы Договора.

d) Стратегические уязвимости:

- Решение США сократить свои операции может выявить стратегическую уязвимость, особенно по мере того, как новые технологии снижают барьеры для стран, стремящихся увеличить своё присутствие и извлечь выгоду из ресурсов региона. Это также включает в себя потенциал для военного применения, такого как разведка и спутниковое позиционирование

- Отсутствие надёжного присутствия США может привести к стратегическому дисбалансу, когда Россия и Китай потенциально будут доминировать в регионе. Это может иметь долгосрочные последствия для глобальной безопасности и национальных интересов США.

2) Научные и экологические последствия

a) Влияние на научные исследования:

- Приостановление новых предложений NSF о проведении полевых работ приведёт к задержке важных научных исследований, к пробелам в знаниях, которые имеют решающее значение для понимания глобальных изменений окружающей среды (исследования по изменению климата, повышению уровня моря и закономерностям океанической циркуляции).

- Сокращение научной деятельности США может помешать международному научному сотрудничеству, поскольку многие страны полагаются на её инфраструктуру и материально-техническую поддержку в своих исследованиях в Антарктиде

b) Экологические риски:

Сокращение присутствия США может повлиять на мониторинг окружающей среды и усилия по её сохранению. Регион Антарктики имеет решающее значение для изучения изменения климата и его воздействия на глобальные экосистемы. Сокращение исследовательской

деятельности может замедлить прогресс в этих областях и снизить эффективность мер по охране окружающей среды.

Экологические проблемы также имеют первостепенное значение. Антарктида является критически важным регионом для изучения изменения климата и его воздействия на глобальные экосистемы. Приостановка научных исследований в США может замедлить прогресс в понимании этих последствий и смягчении их. Другим странам, возможно, потребуется активизировать свои исследовательские усилия, чтобы компенсировать сокращение вклада США, гарантируя продолжение сбора и анализа важнейших экологических данных

c) Национальная безопасность:

Решение США сократить своё присутствие в Антарктиде может иметь последствия для национальной безопасности, особенно если конкурирующие державы будут использовать регион в военных целях. Стратегическое расположение Антарктиды делает её потенциальным местом для разведки и другой военной деятельности, которая может угрожать глобальной безопасности

C. Кибер-атаки

Морская отрасль в Антарктиде сталкивается с целым рядом кибер-угроз, включая фишинг, вредоносное ПО, несанкционированный доступ, подмену GPS, атаки на цепочки поставок и атаки на операционные технологии. Угрозы усугубляются суровыми экологическими условиями региона и растущей зависимостью от цифровых систем.

1) Фишинговые атаки

- **Описание**: атаки связаны с ложными электронными письмами и сообщениями, предназначенными для обмана морского персонала с целью раскрытия конфиденциальной информации или загрузки вредоносного ПО. Фишинговые атаки могут привести к несанкционированному доступу к системам судна и конфиденциальным данным.
- **Влияние**: фишинг ставит под угрозу навигационные системы, сети связи и операционные технологии, потенциально приводя к значительным сбоям в работе.

2) Вредоносное ПО и программы-вымогатели

- **Описание**: вредоносное программное обеспечение может использоваться для нарушения работы встроенных систем, кражи конфиденциальных данных или блокировки законных пользователей, часто требуя выкуп за восстановление доступа.
- **Воздействие**: атаки вредоносных программ и программ-вымогателей могут вывести из строя критически важные системы, что приведёт к задержкам в работе и финансовым потерям. Эти атаки вызывают особую озабоченность, учитывая зависимость Антарктиды от цифровых систем навигации и связи.

3) Несанкционированный доступ и внутренние угрозы

- **Описание**: несанкционированный доступ предполагает получение доступа к системам без разрешения, часто путём использования уязвимостей или украденных учётных данных. Внутренние угрозы связаны с сотрудниками или подрядчиками, которые намеренно или непреднамеренно ставят под угрозу безопасность.
- **Влияние**: несанкционированный доступ и угрозы со стороны инсайдеров могут привести к утечке данных, сбоям в работе системы и потере конфиденциальной информации. Эти угрозы сложно обнаружить и смягчить, особенно в изолированных средах, таких как Антарктида.

4) Подмена GPS

- **Описание**: злоумышленники манипулируют сигналами GPS, чтобы ввести морские навигационные системы в заблуждение относительно местоположения или маршрута судна.
- **Влияние**: подмена GPS приведёт к ошибкам навигации, несанкционированным объездам и потенциальным авариям. Это особенно опасно в сложных условиях вод вокруг Антарктиды, где точная навигация имеет решающее значение.

5) Атаки на цепочки поставок

- **Описание**: атаки нацелены на взаимосвязанные системы и сети морской цепочки поставок, включая порты, поставщиков логистических услуг и другие сторонние сервисы.
- **Воздействие**: атаки на цепочку поставок могут нарушить всю морскую операцию, что приведёт к задержкам, финансовым потерям и поставит под угрозу безопасность груза и персонала.

6) Кибер-атаки на операционные технологии (OT)

- **Описание**: системы OT, которые включают промышленные системы управления (ICS), используемые для навигации, управления двигателем и обработки грузов, все чаще становятся мишенями хакеров.
- **Воздействие**: атаки на системы OT нарушают критически важные операции, что приводит к угрозам безопасности, задержкам в работе и значительным финансовым потерям. Интеграция IT- и OT-систем в морской отрасли увеличила поверхность атаки, сделав эти системы более уязвимыми.

D. Проблема кибербезопасности

Морская отрасль Антарктиды сталкивается с уникальными проблемами кибербезопасности, которые обусловлены удалённостью и суровыми условиями окружающей среды, интеграцией устаревших и современных систем, неопределённостью нормативных актов и нехваткой квалифицированных специалистов.

1) Суровые условия окружающей среды

- **Экстремальные погодные условия**: суровые и непредсказуемые погодные условия в Антарктиде могут нарушить работу систем связи и электроснабжения, что затруднит поддержание последовательных мер кибербезопасности.
- **Изоляция**: удалённый и изолированный характер операций в Антарктике означает, что физический доступ к инфраструктуре для технического обслуживания и реагирования на инциденты ограничен, что усложняет усилия по обеспечению кибербезопасности.

2) Интеграция IT- и OT-систем

- **Комплексная интеграция**: морская отрасль, включая операции в Антарктике, все больше полагается на интеграцию систем информационных технологий (ИТ) и операционных технологий (ОТ). Такая интеграция создаёт сложные проблемы кибербезопасности, поскольку эти системы традиционно были отдельными, а теперь взаимосвязаны, увеличивая поверхность атаки.
- **Устаревшие системы**: во многих морских операциях по-прежнему используются устаревшие системы, которые не были разработаны с учётом кибербезопасности. Эти системы теперь подключены к современным сетям, создавая уязвимости, которыми могут воспользоваться кибер-атаки.

3) Вопросы регулирования и соблюдения требований

- **Неоднозначность регулирования**: морская отрасль сталкивается с неоднозначностью регулирования, особенно в отдалённых регионах. Существующие нормативные акты, такие как Кодекс международной безопасности судов и портовых средств (ISPS) и Закон о безопасности морского транспорта (MTSA), были разработаны в доцифровую эпоху и могут не в полной мере отражать текущие кибер-угрозы.
- **Международное сотрудничество**: учитывая глобальный характер морских операций, международное сотрудничество имеет важное значение для установления единых стандартов и протоколов кибербезопасности. Это особенно сложно в Антарктиде, где интересы и операции имеют несколько стран.

4) Технологические достижения и угрозы

- **Расширение возможностей подключения**: внедрение облачных вычислений, Интернета вещей (IoT) и автономных технологий в морских операциях привело к усилению взаимосвязи между ИТ-системами и системами ОТ. Такое подключение повышает риски кибербезопасности, о чем свидетельствует увеличение кибер-атак на морские системы ОТ на 900% за последние три года.
- **Возникающие угрозы**: морская отрасль является главной мишенью для кибер-угроз, включая злоумышленников со стороны национальных государств и киберпреступников, стремящихся сорвать операции, украсть данные или потребовать выкуп. Меняющийся ландшафт угроз требует постоянного мониторинга и обновления мер кибербезопасности.

5) Рабочая сила и опыт

- **Нехватка специалистов по кибербезопасности**: в морской отрасли наблюдается повсеместная нехватка квалифицированных специалистов по кибербезопасности. Этот дефицит усугубляется в отдалённых регионах, где привлечение и удержание талантов является особенно сложной задачей.
- **Обучение и осведомлённость**: программы непрерывного обучения и осведомлённости необходимы для поддержания высокого уровня готовности к кибербезопасности. Однако логистические проблемы, связанные с проведением таких программ в Антарктике, могут снизить их эффективность.

6) Реагирование на инциденты и восстановление

- **Ограниченные возможности реагирования на инциденты**: способность реагировать на кибер-инциденты и восстанавливаться после них ограничена в Антарктиде из-за изоляции региона и суровых условий. Это делает крайне важным наличие надёжных возможностей удалённого мониторинга и реагирования на инциденты.
- **Отчётность о кибер-инцидентах**: недавнее распоряжение администрации Байдена-Харриса подчёркивает необходимость отчётности о кибер-инцидентах. Однако реализация этих требований в Антарктике может оказаться сложной задачей из-за ограничений в области связи и различий в нормативных актах.

E. Особые меры кибербезопасности

Морская отрасль в Антарктике может эффективно противостоять угрозам кибербезопасности, внедряя целостную систему кибербезопасности, соблюдая нормативные стандарты, используя передовые технологические решения, обеспечивая всестороннее обучение, разрабатывая надёжные планы реагирования на инциденты и укрепляя международное сотрудничество.

1) Целостная система кибербезопасности

- **Интеграция информационных технологий и безопасности ОТ**: конвергенция систем информационных технологий (ИТ) и операционных технологий (ОТ) в морской отрасли требует целостного подхода к кибербезопасности. Использование таких платформ, как NIST Cybersecurity Framework и ISA/IEC IACS Cybersecurity Lifecycle Model, помогает в оценке, планировании, внедрении и мониторинге мер кибербезопасности как в ИТ, так и в ОТ-средах.

- **Комплексное управление рисками**: разработка и внедрение широкого спектра средств контроля корпоративной кибербезопасности, охватывающих как суда, так и береговые объекты, имеет важное значение. Это включает в себя обращение к системам IT, OT и интернета вещей для обеспечения безопасной критической морской инфраструктуры.

2) Соответствие нормативным требованиям и стандартам

- **Соблюдение Руководящих принципов ИМО**: международная морская организация (IMO) выпустила принципы по управлению кибер-рисками на море, которые содержат рекомендации высокого уровня и функциональные элементы для минимизации рисков и воздействия на операции, связанные с судоходством, охрану и охраняемость.

- **Соблюдение CAP и UNCLOS**: CAP и Конвенция UNCLOS обеспечивают правовую основу для морских операций в Антарктике. Обеспечение соблюдения этих правил, включая требования к регистрации судов и оборудованию для обеспечения безопасности, имеет решающее значение для поддержания безопасности на море.

3) Передовые технологические решения

- **Сегментация сети**: Разделение сети на отдельные сегменты помогает сдерживать потенциальные взломы и затрудняет боковые перемещения для злоумышленников. Это особенно важно для защиты критически важных систем на судах и в портовых сооружениях.

- **Регулярное тестирование на проникновение**: Проведение регулярных тестов на проникновение для выявления и устранения уязвимостей, прежде чем они смогут быть использованы злоумышленниками, является упреждающей мерой повышения кибербезопасности.

- **Искусственный интеллект и машинное обучение**: Внедрение передовых систем обнаружения угроз, которые используют искусственный интеллект и машинное обучение для обнаружения необычного поведения, может помочь выявлять и смягчать кибер-угрозы в режиме реального времени.

- **Передовые системы кибербезопасности**: Использование передовых систем кибербезопасности, таких как Cydome's Everlight, поддерживает управление кибербезопасностью судна посредством мониторинга и оценки рисков в режиме реального времени. Эти системы помогают эффективно обнаруживать и смягчать кибер-угрозы

4) Обучение и осведомлённость

- **Учебные программы по кибербезопасности**: важно обеспечить всестороннюю подготовку по кибербезопасности всего персонала, как моряков, так и берегового персонала. Учебные программы должны охватывать новейшие угрозы безопасности, тактику фишинга и лучшие практики предотвращения кибер-атак.

- **Обучение и осведомлённость пользователей**: Регулярное информирование сотрудников о передовых методах кибербезопасности и новейших угрозах гарантирует, что они будут лучше подготовлены к обнаружению и предотвращению кибер-атак, снижая риск человеческой ошибки.

5) Реагирование на инциденты и восстановление

- **План реагирования на инциденты**: Разработка и регулярное обновление плана реагирования на инциденты обеспечивает быстрые действия и смягчение последствий в случае возникновения нарушения. Этот план должен включать чёткие протоколы обнаружения кибер-инцидентов, реагирования на них и восстановления после них.

- **Удалённый мониторинг и управление**: Учитывая изоляцию и суровые условия Антарктиды, надёжные инструменты удалённого мониторинга и управления необходимы для поддержания мер кибербезопасности и эффективного реагирования на инциденты.

6) Международное сотрудничество

- **Глобальные стандарты и протоколы**: Международное сотрудничество имеет жизненно важное значение для установления единых стандартов и протоколов кибербезопасности, выходящих за рамки национальных границ. Сотрудничество между государственными учреждениями, заинтересованными сторонами отрасли и международными партнёрами помогает повышать стандарты кибербезопасности и обмениваться передовым опытом.

- **Отчётность о кибер-инцидентах**: Внедрение обязательной отчётности о кибер-инцидентах, как подчёркивается в недавних указах президента, помогает своевременно выявлять кибер-угрозы и реагировать на них. Это имеет решающее значение для поддержания безопасности морских операций в отдалённых регионах, таких как Антарктида.

F. Тренинг в особых условиях

Морские компании в Антарктике борются с угрозами кибербезопасности, внедряя комплексные и непрерывные программы обучения для своих сотрудников. Эти программы соответствуют международным стандартам, используют передовые средства обучения и направлены на сокращение человеческих ошибок.

1) Комплексные Учебные программы по кибербезопасности

- **Курсы повышения осведомлённости о кибербезопасности**: Компании предоставляют онлайн-курсы, специально разработанные для членов экипажей судов. Эти курсы охватывают обширные знания о морской кибербезопасности, включая типы

информации, уязвимой для кибер-атак, этапы кибер-атаки и меры по смягчению последствий.

- **Целостные подходы к обучению**: Учебные программы разработаны, чтобы охватывать широкий круг тем, включая новейшие риски безопасности, политики и процедуры. Это помогает уменьшить количество человеческих ошибок, которые являются одной из основных причин инцидентов в области кибербезопасности на судах.

2) Регулярные и обновленные Учебные занятия

- **Непрерывное образование**: регулярное обновление учебных программ с учётом новейших угроз кибербезопасности и передовых практик гарантирует, что сотрудники остаются бдительными и информированными. Это включает в себя обучение новейшим тактикам фишинга и другим распространённым кибер-угрозам.

- **Обучение реагированию на инциденты**: сотрудники обучаются тому, как надлежащим образом реагировать на инциденты в области кибербезопасности, что помогает минимизировать ущерб и обеспечить бесперебойное выполнение критически важных операций.

3) Соответствие международным стандартам

- **Руководящие принципы ИМО**: учебные программы приведены в соответствие с руководящими принципами Международной морской организации (ИМО) по управлению кибер-рисками на море. Настоящие руководящие принципы содержат рекомендации высокого уровня и функциональные элементы для минимизации рисков и воздействия на операции, связанные с судоходством, безопасность.

- **Конвенция ПДНВ**: международная конвенция о стандартах подготовки, сертификации и несения вахты для моряков (STCW) пересматривается с целью включения "осведомлённости о кибербезопасности" в качестве отдельной области развития компетенций. Это гарантирует, что моряки будут обучены цифровым навыкам, коммуникациям, управлению информацией и способности адаптироваться к меняющимся условиям работы.

4) Использование передовых средств обучения

- **«Тренажёры»**: использование «тренажёров» в учебных программах помогает сотрудникам понимать реальные кибер-угрозы и управлять ими. Такой подход имеет решающее значение для развития практических навыков выявления кибер-угроз и смягчения их последствий.

- **Искусственный интеллект и машинное обучение**: передовые системы обнаружения угроз, использующие ИИ и ML, интегрируются в учебные программы. Эти системы помогают сотрудникам научиться обнаруживать необычное поведение, которое может указывать на кибер-угрозу.

5) Сокращение человеческих ошибок

- **Информационные кампании**: регулярные информационные кампании и учебные занятия помогают снизить количество человеческих ошибок за счёт повышения осведомлённости о рисках, политиках и процедурах безопасности.

- **Симуляции фишинга**: проведение симуляции фишинга в рамках обучения помогает сотрудникам распознавать попытки фишинга и предотвращать их.

G. Изменения в морской отрасли антарктиды

Новейшие правила кибербезопасности для морской отрасли в Антарктике разработаны на основе сочетания международных: Система Договора об Антарктике (ATS) и Конвенция Организации Объединённых Наций по морскому праву (UNCLOS), а также конкретных руководящих принципов Международной морской организации (IMO). Кроме того, недавние указы Президента США ввели новые требования и стандарты кибербезопасности, подчёркивая необходимость комплексного управления кибер-рисками и отчётности об инцидентах. Международное сотрудничество по-прежнему имеет важное значение для установления и поддержания эффективных мер кибербезопасности в морской отрасли.

1) Система Договора об Антарктике (CAP)

- **Обзор**: CAP представляет собой международную систему соглашений, регулирующих деятельность в Антарктике. Он включает положения о мирном использовании континента, защите окружающей среды и содействии научным исследованиям.

- **Безопасность на море**: CAP требует, чтобы все суда, заходящие в территориальные воды Антарктики и покидающие их, были зарегистрированы в Секретариате Договора об Антарктике. Он также предусматривает обеспечение соблюдения правил безопасности и мониторинг судов для обеспечения соблюдения правил международного судоходства.

2) Конвенция Организации Объединенных Наций по морскому праву (UNCLOS)

- **Морское право**: UNCLOS содержит всеобъемлющий свод норм, регулирующих море и его ресурсы, включая право стран на морское судоходство и ответственность за защиту и сохранение морской среды.

- **Положения о кибербезопасности**: хотя UNCLOS в первую очередь затрагивает традиционные вопросы безопасности на море, её принципы являются основополагающими для разработки мер кибербезопасности в морской сфере. В нем подчёркивается необходимость сотрудничества между государствами для обеспечения безопасности на море, что включает в себя противодействие кибер-угрозам.

3) Руководящие принципы Международной морской организации (ИМО)

- **Управление кибер-рисками**: ИМО представила руководящие принципы по управлению кибер-рисками для судов и судоходства, включая требование к компаниям разрабатывать планы управления кибер-рисками. Настоящие принципы содержат рекомендации высокого уровня и функциональные элементы для минимизации рисков и воздействия на операции, связанные с судоходством.
- **MSC-FAL.1-Circ.3-Rev.2**: настоящее руководство по управлению кибер-рисками на море, выпущенное в июле 2022 года, содержит рекомендации высокого уровня и в значительной степени зависит от интерпретации физического лица или компании, его применяющей.

4) U.S. Указы и федеральные правила

- **Распоряжение администрации Байдена**: 21 февраля 2024 года президент Байден подписал Распоряжение, направленное на повышение кибербезопасности портов США и морских цепочек поставок. Этот приказ вводит новые требования и стандарты безопасности для заинтересованных сторон Морской транспортной системы США (MTS) и повышает полномочия береговой охраны США по противодействию кибер-угрозам.
- **Отчётность о кибер-инцидентах**: исполнительный указ предписывает сообщать о фактических или потенциальных кибер-инцидентах, которые могут поставить под угрозу гавани, портовые или прибрежные сооружения. Это включает в себя обмен отчётами с Агентством по кибербезопасности и инфраструктурной безопасности (CISA) и Федеральным бюро расследований (ФБР).

5) Международное сотрудничество

- **Глобальные стандарты и протоколы**: учитывая глобальный характер морских операций, международное сотрудничество имеет важное значение для установления единых стандартов и протоколов кибербезопасности. Сотрудничество между госучреждениями, заинтересованными сторонами отрасли и международными партнёрами имеет решающее значение для повышения стандартов и обмена передовым опытом.
- **Регулирующие органы**: нормативная база морской кибербезопасности всё ещё развивается, что приводит к несоответствиям и проблемам с внедрением. ИМО и другие международные организации продолжают уточнять и обновлять руководящие принципы для решения растущих кибер-угроз в морской отрасли.

H. Экономические последствия

Кибер-атаки на морскую отрасль в Антарктиде могут иметь далеко идущие экономические последствия, включая сбои в научных исследованиях и операциях, увеличение операционных расходов, сбои в цепочке поставок, потерю конфиденциальных данных и интеллектуальной собственности, а также усиление нацбезопасности и геополитической напряжённости.

1) Срыв научных исследований и операций

- **Влияние на исследовательские миссии**: атаки могут нарушить работу исследовательских судов и станций, что приведёт к задержкам или отмене научных миссий к потере ценных исследовательских данных и увеличению затрат, связанных с перепланированием и продлением миссий.
- **Эксплуатационные задержки**: сбои в работе навигационных систем, сетей связи и других критически важных эксплуатационных технологий могут привести к значительным задержкам в морских операциях. Это увеличит эксплуатационные расходы и снизит эффективность исследовательских миссий и миссий по снабжению.

2) Увеличение Эксплуатационных расходов

- **Затраты на смягчение последствий и восстановление после кибер-атак**: затраты, связанные со смягчением последствий кибер-атак и восстановлением после них, могут быть значительными. Сюда входят расходы, связанные с реагированием на инциденты, восстановлением системы и внедрением дополнительных мер безопасности для предотвращения будущих атак.
- **Страховые взносы**: кибер-атаки могут привести к повышению страховых взносов для морских компаний, работающих в Антарктиде. Страховщики могут увеличить страховые взносы для покрытия повышенного риска кибер-инцидентов, увеличивая общие операционные расходы.

3) Сбои в цепочке поставок

- **Влияние на логистику**: атаки нарушают цепочку поставок, и имеют влияние на транспортировку товаров и предметов первой необходимости в Антарктиду и обратно. Это приводит к нехватке важнейших поставок, увеличению транспортных расходов и задержкам в доставке товаров.
- **Волновые эффекты для экономики**: сбои в цепочке поставок могут оказывать волновой эффект на экономику в целом, затрагивая отрасли, которые зависят от своевременных поставок товаров и материалов. Это приведёт к увеличению затрат и снижению производительности во многих секторах.

4) Потеря конфиденциальных данных и интеллектуальной собственности

- **Утечка данных**: кибер-атаки приводят к краже конфиденциальных данных, включая результаты исследований, конфиденциальную информацию и личные данные членов экипажа и исследователей. Потеря таких данных может иметь значительные экономические последствия, включая потерю конкурентного преимущества и потенциальную юридическую ответственность.

- **Кража интеллектуальной собственности**: кража интеллектуальной собственности: запатентованные исследовательские данные и технологические инновации, подорвёт экономическую ценность научных исследований и разработок в Антарктике.

5) Влияние на нацбезопасность и геополитические интересы

- **Геополитическая напряжённость**: кибер-атаки на морские операции в Антарктиде могут усугубить геополитическую напряжённость, особенно если они приписываются субъектам национального государства. Это приведёт к увеличению расходов на оборону и безопасность, поскольку страны стремятся защитить свои интересы в регионе.

- **Стратегические уязвимости**: срыв морских операций может выявить стратегические уязвимости, потенциально влияющие на национальную безопасность и экономическую стабильность. Это может привести к увеличению инвестиций в кибербезопасность и оборонные меры, отвлекая ресурсы от других важных областей.

I. Неэкономические последствия

Неэкономические последствия кибер-атак на морскую отрасль в Антарктиде значительны и многогранны. Они включают угрозы безопасности и жизни людей, ущерб окружающей среде, геополитическую напряжённость, срыв научных исследований и операционные проблемы.

1) Безопасность и человеческая жизнь

- **Безопасность экипажа**: кибер-атаки ставят под угрозу безопасность членов экипажа, нарушая работу критически важных систем, таких как навигация, связь и управление двигателем. Это может привести к авариям, посадкам на землю или столкновениям, подвергая риску жизни.

- **Поисково-спасательные операции**: сбои в работе систем связи и навигации могут затруднить поисково-спасательные операции, затрудняя обнаружение судов, терпящих бедствие, и оказание им помощи. Это приводит к задержке реагирования и увеличению риска для жизни человека.

2) Воздействие на окружающую среду

- **Загрязнение и разливы**: атаки, нарушающие работу систем навигации или управления двигателем, приводят к авариям - разливам нефти или выбросу опасных материалов в хрупкую окружающую среду Антарктики. Такие инциденты имеют долгосрочные пагубные последствия для морских экосистем и дикой природы.

- **Ущерб экосистеме**: регион Антарктики является домом для уникальных и чувствительных экосистем. Аварии, вызванные кибер-атаками, могут нанести значительный ущерб этим экосистемам, оказывая влияние на биоразнообразие и общее состояние окружающей среды.

3) Геополитические последствия и последствия для безопасности

- **Геополитическая напряжённость**: кибер-атаки на морские операции в Антарктиде усугубляют геополитическую напряжённость, особенно если они приписываются субъектам национального государства. Это может привести к увеличению военного присутствия и усилению мер безопасности в регионе, что приведёт к эскалации конфликтов.

- **Национальная безопасность**: срыв морских операций может выявить стратегические уязвимости, влияющие на национальную безопасность. Это особенно актуально для стран, имеющих значительные интересы в Антарктике, поскольку кибер-атаки могут подорвать их способность защищать и отстаивать свои претензии и интересы в регионе.

4) Срыв научных исследований

- **Влияние на исследовательские миссии**: кибер-атаки нарушают работу исследовательских судов и станций, что приведёт к задержкам или отмене научных миссий, к потере ценных исследовательских данных и мешает научному прогрессу в понимании изменения климата, морской биологии и других важнейших областей.

- **Целостность данных**: кибер-атаки ставят под угрозу целостность научных данных, что приводит к неточным или неполным результатам исследований. Это может подорвать доверие к научным исследованиям и повлиять на политические решения, основанные на таких данных.

5) Операционные и логистические проблемы

- **Сбои в работе**: кибер-атаки могут нарушить повседневную работу морских судов, затрагивая все – от навигации до обработки грузов. Это может привести к значительным логистическим проблемам, включая задержки в доставке основных материалов и оборудования на исследовательские станции.

- **Нарушение связи**: сбои в системах связи приводят к изоляции судов и исследовательских станций, затрудняя координацию действий и реагирование на чрезвычайные ситуации. Это увеличивает риск несчастных случаев и затрудняет эффективное управление в кризисных ситуациях.

ЧЕЛОВЕКОПОДОБНЫЕ РОБОТЫ

Аннотация – документ предоставляет анализ развития глобальной автоматизации и человекоподобных роботов, уделяя особое внимание различным критическим аспектам, технологическим достижениям в области человекоподобных роботов, в частности интеграции комплексного искусственного интеллекта и мультимодальных алгоритмов искусственного интеллекта, которые значительно расширяют возможности роботов в решении сложных задач и процессах принятия решений. В документе также рассматриваются экономические последствия, подчёркивая потенциал человекоподобных роботов в замене человеческих ролей, тем самым не только повышая безопасность, но и решая проблему нехватки рабочей силы в важнейших секторах, и стратегические последствия этих технологических достижений для глобальных рынков труда и конкурентоспособности промышленности.

Материал полезен для специалистов в области безопасности, которые заинтересованы в понимании влияния роботизированной автоматизации на меры безопасности и защиту инфраструктуры. Кроме того, этот анализ служит ценным ресурсом для отраслевых специалистов из различных секторов, предоставляя представление о том, как человекоподобные роботы могут быть интегрированы в их деятельность для повышения эффективности, безопасности и инноваций.

A. Введение

Гуманоидные роботы — это усовершенствованные машины, разработанные для имитации человеческой формы и поведения, оснащённые сочленёнными конечностями, усовершенствованными датчиками и часто способностью к социальному взаимодействию. Эти роботы все чаще используются в различных секторах, включая здравоохранение, образование, промышленность и сферу услуг, благодаря их адаптируемости к среде обитания человека и способности выполнять задачи, требующие человеческой ловкости и взаимодействия.

В здравоохранении человекоподобные роботы помогают выполнять клинические задачи, оказывают эмоциональную поддержку и помогают в реабилитации пациентов. В сфере образования они служат интерактивными компаньонами и персональными наставниками, улучшая опыт обучения и способствуя социальной интеграции детей с особыми потребностями. Промышленный сектор извлекает выгоду из человекоподобных роботов за счёт автоматизации повторяющихся и опасных задач, повышения эффективности и безопасности. Кроме того, в сфере услуг эти роботы оказывают помощь клиентам, направляют посетителей и выполняют задачи технического обслуживания, демонстрируя свою универсальность и потенциал для преобразования различных аспектов повседневной жизни.

B. Прогнозы рынка человекоподобных роботов

Рынок человекоподобных роботов находится на пороге существенного роста, и прогнозы указывают на многомиллиардный объём рынка к 2035 году. Ключевые факторы включают достижения в области искусственного интеллекта, снижение затрат и растущий спрос на автоматизацию в опасных отраслях и на производстве.

- Отчёт Goldman Sachs (январь 2024 г.):
  - **Общий объём адресуемого рынка (TAM)**: ожидается, что объём рынка человекоподобных роботов достигнет 38 миллиардов долларов к 2035 году, по сравнению с первоначальным прогнозом в 6 миллиардов долларов, что обусловлено четырёхкратным увеличением прогнозов поставок до 1,4 миллиона единиц.
  - **Оценки поставок**: Базовый сценарий прогнозирует совокупный годовой темп роста (CAGR) на 53% в период с 2025 по 2035 год, при этом поставки достигнут 1,4 млн единиц к 2035 году. Согласно оптимистичному сценарию, поставки достигнут 1 миллиона единиц к 2031 году, что на четыре года опережает предыдущие ожидания.
  - **Снижение затрат**: Стоимость роботов высокой спецификации снизилась на 40% до 150 000 долларов за единицу в 2023 году по сравнению с 250 000 долларами в предыдущем году из-за более дешёвых компонентов и более широкой внутренней цепочки поставок.
- **Маркетинговые исследования Data Bridge**: ожидается, что мировой рынок человекоподобных роботов вырастет с 2,46 миллиарда долларов в 2023 году до 55,80 миллиарда долларов к 2031 году, при среднем росте на 48,5% в течение прогнозируемого периода.
- **SkyQuestt**: По прогнозам, рынок вырастет с 1,48 миллиарда долларов в 2019 году до 34,96 миллиарда долларов к 2031 году, при CAGR 42,1%.

- **GlobeNewswire**: Мировой рынок человекоподобных роботов, оцениваемый примерно в 1,3 миллиарда долларов в 2022 году, как ожидается, увеличится до 6,3 миллиарда долларов к 2030 году при среднегодовом росте в 22,3%.
- **Компания по исследованию бизнеса**: ожидается, что рынок вырастет с 2,44 миллиарда долларов в 2023 году до 3,7 миллиарда долларов в 2024 году, при CAGR 51,6%. По прогнозам, к 2028 году объём рынка достигнет 19,69 миллиарда долларов, а CAGR составит 51,9%.
- **Исследование Grand View**: Размер рынка: Мировой рынок человекоподобных роботов оценивался в 1,11 миллиарда долларов в 2022 году и, как ожидается, вырастет в среднем на 21,1% с 2023 по 2030 год.
- **Goldman Sachs (февраль 2024 г.)**: рынок может достичь 154 миллиардов долларов к 2035 году, что сопоставимо с мировым рынком электромобилей и одной третью мирового рынка смартфонов по состоянию на 2021 год.
- **Macquarie Research**: Согласно нейтральному прогнозу, ожидается, что мировой рынок роботов-гуманоидов достигнет 107,1 миллиарда долларов к 2035 году, а CAGR с 2025 по 2035 год составит 71%.

1) Ключевые движущие силы и тенденции

- **Технологические достижения**: Значительный прогресс в области комплексного искусственного интеллекта и мультимодальных алгоритмов искусственного интеллекта, ускоряет итерации продукта и улучшает возможности роботов.
- **Снижение затрат**: Доступность более дешёвых компонентов и усовершенствования в дизайне и технологиях производства снижают затраты, делая разработки более экономически выгодными.
- **Последствия для рынка труда**: Национальная политика повышает спрос на роботов для выполнения опасных работ с потенциальным применением в производстве, спасении при стихийных бедствиях и уходе за пожилыми людьми.
- **Инвестиции и динамика рынка**: Увеличение инвестиций со стороны цепочек поставок, стартапов и компаний, зарегистрированных на бирже, особенно в США и Азии, являются движущей силой роста рынка. Государственная поддержка, особенно со стороны Китая, также является важным фактором.

C. Технологический прогресс

В разработке человекоподобных роботов произошёл значительный технологический прогресс, обусловленный улучшениями в области искусственного интеллекта (ИИ), машинного обучения, интеграции датчиков и проектирования аппаратного обеспечения. Эти достижения позволяют человекоподобным роботам выполнять все более сложные задачи и более естественно взаимодействовать с окружающей средой.

1) Интеграция искусственного интеллекта и машинного обучения

- **Сквозной искусственный интеллект**: Интеграция сквозного искусственного интеллекта и мультимодальных алгоритмов искусственного интеллекта позволила ускорить итерации продукта и улучшить возможности человекоподобных роботов. Такой подход позволяет роботам выполнять задачи от исходных команд до конечных результатов в соответствии с самогенерируемыми искусственным интеллектом правилами, а не с заранее запрограммированными инженерами-программистами.
- **Обучение с подкреплением (RL)**: Рамки RL, такие как та, которая использовалась при разработке гуманоидного робота "Адам", значительно повысили эффективность процессов имитационного обучения. Эти платформы позволяют роботам достигать производительности, сравнимой с работой человека, в сложных задачах по перемещению, используя данные о передвижении человека для имитационного обучения.
- **Большие языковые модели (LLM)**: Интеграция мультимодальных LLM, таких как Google Gemini и мультимодальный ChatGPT 4, улучшает способность роботов "слышать" и "видеть", способствуя более тонкому и интерактивному взаимодействию с миром. Это сближение переопределяет взаимодействие человека и робота, позволяя роботам беспрепятственно работать в реальных условиях.

2) Интеграция и объединение датчиков

- **Усовершенствованные датчики**: роботы оснащены различными датчиками, включая инерциальные измерительные блоки (IMU) для определения пространства, лидары для определения глубины и камеры для визуального восприятия, что позволяет им ощущать и понимать окружающую обстановку, позволяя им ориентироваться, общаться и принимать решения автономно.
- **Методы объединения датчиков**: нейронные сети, байесовский вывод и фильтрация Калмана, используются для объединения данных датчиков в режиме реального времени, обеспечивая полную картину окружения робота. Это позволяет роботам предсказывать своё положение, составлять карту окружающей среды и идентифицировать объекты и препятствия на своём пути.

3) Улучшения аппаратного обеспечения и дизайна

- **Снижение затрат**: Стоимость роботов с высокими техническими характеристиками значительно снизилась, что обусловлено наличием более дешёвых компонентов и более широкой внутренней цепочкой поставок. Такое снижение затрат ускоряет

сроки применения человекоподобных роботов на заводах и у потребителей.

- **Инновационные конструктивные решения**: Новые конструктивные решения, такие как те, которые используются в роботе "Адам", повышают эффективность процесса имитационного обучения, что позволяет роботам демонстрировать человекоподобные характеристики при выполнении задач передвижения.
- **Усовершенствования батареи и привода**: Увеличение срока службы батареи и конструкции привода имеют решающее значение для повышения мобильности и манёвренности человекоподобных роботов. Например, роботы, оснащённые гидравлическими приводами, обычно могут работать короткими очередями, но ожидается, что развитие аккумуляторных технологий обеспечит более длительные периоды работы.

4) Взаимодействие человека и робота и когнитивные способности

- **Когнитивные алгоритмы**: Исследователи разрабатывают алгоритмы, имитирующие важные аспекты человеческого познания, такие как восприятие, внимание, память, обучение и рассуждение. Эти когнитивные способности позволяют роботам расшифровывать сенсорную информацию, концентрироваться на релевантных входных данных, хранить и извлекать знания, а также планировать действия на основе прогнозов.
- **Эмоциональное и социальное взаимодействие**: Гуманоидные роботы, такие как PEPPER, предназначены для оказания эмоциональной поддержки путём определения выражения лица и тембра голоса, корректируя своё взаимодействие для создания комфортной обстановки. Эта возможность особенно ценна в медицинских учреждениях.

5) Реальные приложения и варианты использования

- **Промышленные и опасные среды**: Человекоподобные роботы все чаще используются в промышленных условиях для автоматизации повторяющихся и потенциально опасных задач. Их манёвренность и точность используются при проверке и обслуживании агрессивных сред, повышая эффективность промышленных операций.
- **Здравоохранение и образование**: В здравоохранении человекоподобные роботы помогают выполнять клинические задачи и оказывают эмоциональную поддержку пациентам. В сфере образования они служат интерактивными компаньонами и персональными наставниками, способствуя социальной интеграции и персонализированному обучению

D. Влияние человекоподобных роботов на рынок труда

Ожидается, что интеграция человекоподобных роботов в различные отрасли промышленности будет иметь серьёзные последствия для рынка труда. Эти последствия охватывают смену места работы, создание новых рабочих мест, изменения должностных ролей и необходимость переподготовки кадров.

1) Перемещение и создание рабочих мест

- **Замещение рутинных работ**: Человекоподобные роботы, вероятно, заменят рабочие места, связанные с повторяющимися ручными и рутинными задачами. Сюда входят такие роли, как работники производственной линии, специалисты по контролю качества и операторы станков. Внедрение роботов в этих областях может привести к значительной потере рабочих мест, особенно в обрабатывающей и автомобильной промышленности.
- **Создание новых рабочих мест**: хотя роботы могут заменить определённые рабочие места, они также создают новые возможности, особенно для высококвалифицированных специалистов. Эти новые рабочие места включают специалистов по системам искусственного интеллекта, программистов роботов и техников по техническому обслуживанию. Переход к более продвинутым ролям требует от работников развития новых навыков и адаптации к работе бок о бок с роботами.

2) Влияние на заработную плату и занятость

- **Снижение заработной платы**: Внедрение роботов на рынок труда было связано со снижением заработной платы. Например, исследования показали, что на каждого добавленного робота на 1000 работников приходится снижение заработной платы примерно на 0,42%, а соотношение занятости к численности населения уменьшается на 0,2 процентных пункта.
- **Сокращение занятости**: Внедрение роботов может привести к сокращению возможностей трудоустройства. Исследования показывают, что увеличение числа роботов на тысячу работающих снижает соотношение занятости к численности населения на 0,18–0,34 процентных пункта.

3) Воздействие на конкретный сектор

- **Производство**: ожидается, что в производственном секторе произойдут значительные изменения в связи с внедрением человекоподобных роботов. Роботы могут выполнять такие задачи, как сборка электромобилей, сортировка компонентов и другие работы в структурированной среде. Это может восполнить 4% прогнозируемого дефицита рабочей силы в обрабатывающей промышленности США к 2030 году.
- **Уход за пожилыми людьми**: по прогнозам, к 2035 году гуманоидные роботы также удовлетворят 2% мирового спроса на услуги по уходу за пожилыми

людьми. Это приложение особенно актуально в странах со стареющим населением и нехваткой лиц, осуществляющих уход.

4) Переподготовка и адаптация персонала

- **Инициативы по переквалификации**: для смягчения негативных последствий смены работы необходимы комплексные программы переквалификации и повышения квалификации. Эти программы должны быть сосредоточены на обучении работников навыкам, необходимым для работы с роботами и сотрудничества с ними. Правительства и предприятия должны инвестировать в образование и профессиональную подготовку, чтобы подготовить рабочую силу к будущему.

- **Адаптация к новым ролям**: Работникам необходимо будет адаптироваться к новым ролям, которые предполагают выполнение более сложных, творческих и чутких задач. Роботы возьмут на себя монотонные и физически сложные задачи, позволив людям сосредоточиться на более ценной работе.

5) Экономические и социальные последствия

- **Производительность и рост ВВП**: ожидается, что внедрение роботов приведёт к значительному росту производительности, что, в свою очередь, может увеличить валовой внутренний продукт (ВВП). Например, было показано, что растущее использование промышленных роботов увеличивает ежегодный рост ВВП на 0,36% в 17 странах.

- **Экономическое неравенство**: Преимущества автоматизации и робототехники, вероятно, достанутся владельцам капитала и квалифицированным работникам, что потенциально усилит экономическое неравенство. Крайне важно внедрять политику, обеспечивающую равный доступ к преимуществам автоматизации и поддержку перемещённых работников.

6) Этические и социальные соображения

- **Взаимодействие человека и робота**: Появление человекоподобных роботов вызывает этические опасения по поводу замены человеческих отношений роботизированными. С точки зрения философии ubuntu, человеческие отношения необходимы для того, чтобы стать полностью человеком, а роботизированные отношения могут привести к социальной изоляции и снижению моральной свободы.

- **Политика и регулирование**: существует потребность в надёжных этических рамках и нормативных актах, которыми можно руководствоваться при развёртывании и использовании человекоподобных роботов. Это включает в себя соображения, касающиеся конфиденциальности, безопасности и этических последствий того, что роботы берут на себя роли, традиционно выполняемые людьми

E. Увеличение инвестиций и финансирования

Источники подчёркивают значительные инвестиции и финансирование, вливаемые в сектор гуманоидной робототехники, благодаря потенциалу этой новой технологии и участию крупных технологических компаний и инвесторов.

- **Масштабный раунд финансирования Figure AI**: Стартап Figure AI, занимающийся разработкой человекоподобных роботов, привлёк 675 миллионов долларов в раунде финансирования серии B, что оценивало компанию в 2,6 миллиарда долларов постфактум. Раунд финансирования привлёк известных инвесторов, в том числе Джеффа Безоса (через Bezos Expeditions), Microsoft, Nvidia, стартап-фонд OpenAI, Индустриально-инновационный фонд Amazon, Intel Capital, Align Ventures и ARK Invest.

- **Участие крупных технологических компаний**:
  - OpenAI, компания, стоящая за ChatGPT, заключила соглашение о сотрудничестве с Figure AI для разработки моделей искусственного интеллекта следующего поколения для человекоподобных роботов, объединив исследования OpenAI с опытом Figure в области робототехники.
  - Microsoft инвестирует 95 миллионов долларов в Figure AI и предоставит свои облачные сервисы Azure для инфраструктуры искусственного интеллекта, обучения и хранения данных.
  - Nvidia, ведущий производитель чипов, инвестирует 50 миллионов долларов в искусственный интеллект.
  - Инвестиционное подразделение Amazon и венчурный фонд Intel Capital также участвуют в раунде финансирования.

- **Другие значительные инвестиции**:
  - Норвежский стартап 1X Technologies привлёк 100 миллионов долларов финансирования от OpenAI.
  - Компания Agility Robotics, поддержанная Amazon в 2022 году, тестирует своих человекоподобных роботов на складах Amazon.
  - Sanctuary AI разрабатывает гуманоидного робота по имени Феникс.
  - Повышенный интерес со стороны венчурных компаний: Венчурные компании, такие как Parkway Venture Capital, Align Ventures, ARK Venture Fund, Aliya Capital Partners и Tamarack, инвестируют в стартапы в области гуманоидной робототехники. Ситуация с

финансированием остается сложной, но бум искусственного интеллекта дал надежду стартапам в области гуманоидной робототехники.

- **Государственная поддержка**: потенциальная государственная поддержка, особенно со стороны Китая, рассматривается как фактор, стимулирующий рост рынка

F. Технологические и экономические аспекты

1) Технологические достижения:

- Интеграция сквозного искусственного интеллекта и мультимодальных алгоритмов искусственного интеллекта:
- Внедрение комплексного искусственного интеллекта и мультимодальных алгоритмов искусственного интеллекта ускорило итерации продукта и улучшило возможности роботов.
- Это позволило ускорить циклы разработки и усовершенствования в таких областях, как манипулирование и взаимодействие, как показано в различных продуктах, выпущенных в 2023 году (например, Tesla Optimus Gen 2).

2) Достижения в области оборудования и цепочки поставок:

- Усовершенствованные конфигурации оборудования и более широкая производственная цепочка поставок, особенно в Китае, способствовали технологическому прогрессу.
- Доступность более дешёвых компонентов и более широкий спектр внутренних цепочек поставок привели к снижению затрат.
- Разработка роботизированных систем управления, таких как PaLM-E, PaLI-X и RT-2, позволила значительно улучшить возможности обработки естественного языка, зрения и управления человекоподобными роботами.

3) Экономическая жизнеспособность:

- Стоимость спецификации высокопроизводительных человекоподобных роботов снизится на 40% до 150 000 долларов за единицу в 2023 году по сравнению примерно с 250 000 долларов в предыдущем году.
- Такое снижение затрат обусловлено наличием более дешёвых компонентов и более широкой внутренней цепочкой поставок, что повышает экономическую целесообразность применения на заводах и у потребителей.

4) Ускоренные сроки для обеспечения коммерческой жизнеспособности:

- Основываясь на снижении затрат и технологических достижениях, предполагается, что заводские приложения могут стать экономически выгодными в период с 2024 по 2027 год, на год раньше, чем ожидалось ранее (2025–2028).
- Ожидается, что потребительские приложения станут экономически жизнеспособными в период с 2028 по 2031 год, что на 2–4 года раньше предыдущего прогноза (2030–2035).

5) Потенциальный спрос и замещение рабочей силы:

- Учитывая текущие технологические возможности, наблюдается заметный спрос на человекоподобных роботов в структурированных средах, таких как производство (например, сборка электромобилей, сортировка компонентов).
- Для выполнения опасных задач, таких как специальные операции, спасение в случае стихийных бедствий и техническое обслуживание ядерных установок, заказчики могут быть готовы платить более высокую цену за человекоподобных роботов из-за их адаптивности, обеспечиваемой алгоритмами искусственного интеллекта.
- Предполагая, что уровень замещения рабочей силы в этих областях составит 5–15%, мировой спрос на человекоподобных роботов потенциально может достичь 1,1–3,5 млн единиц.

G. Географические тенденции

1) Географические представления

Рынок человекоподобных роботов переживает значительный рост в различных регионах, чему способствуют технологические достижения, растущий спрос на автоматизацию и поддерживающая государственная политика.

a) Северная Америка

- **США:** США являются крупным игроком на рынке человекоподобных роботов, а такие компании, как Tesla и Boston Dynamics, лидируют в разработке роботов. Ожидается, что регион будет доминировать на мировом рынке человекоподобных роботов благодаря надёжным технологическим экосистемам и значительным инвестициям в исследования и разработки. Рынок США в настоящее время оценивается в 430,8 миллиона долларов.
- **Канада и Мексика**: Эти страны также являются частью североамериканского рынка, извлекая выгоду из технологических достижений и инвестиций в регионе.

b) Южная Америка

- **Бразилия и Аргентина**: Эти страны являются частью растущего южноамериканского рынка человекоподобных роботов, чему способствуют растущие инвестиции в автоматизацию и технологические достижения

c) Азиатско-Тихоокеанскийрегион

- **Китай**: Китай настойчиво добивается массового производства человекоподобных роботов с целью стать мировым лидером в этой области к 2025 году. Китайское правительство выпустило руководящие принципы по ускорению разработки человекоподобных роботов, уделяя особое внимание ключевым технологиям, таким как искусственный интеллект, высокотехнологичное производство и новые материалы. Страна стремится создать внутреннюю экосистему для человекоподобных роботов, и ожидается, что продукция будет запущена в массовое производство к 2025 году. Прогнозируется, что рынок Китая вырастет в среднем на 26,7%, что указывает на высокий рыночный потенциал.

- **Япония**: Япония имеет давнюю традицию интеграции робототехники в различные отрасли промышленности, включая производство, здравоохранение и развлечения. Японские компании, такие как Fanuc и Softbank Robotics, являются пионерами в этой области, а стареющее население страны стимулирует разработку роботов для ухода за пожилыми людьми. Прогнозируется, что темпы роста японского рынка составят 17,5%.

- **Южная Корея**: Южная Корея известна своими инновациями в области человекоподобных роботов, подкреплёнными технологическим опытом и правительственными инициативами. Страна является домом для передовых компаний в области робототехники, таких как Корейский передовой институт науки и технологий (KAIST).

- **Другие страны Азиатско-Тихоокеанского региона**: Такие страны, как Индия, Австралия, Сингапур и Тайвань, также добиваются значительных успехов на рынке человекоподобных роботов благодаря инвестициям в исследования и разработки и внедрению технологий автоматизации.

d) Европа

- **Германия**: Германия является лидером в области промышленной робототехники и автоматизации с мощной производственной базой, стимулирующей инновации. Немецкие компании, такие как KUKA и Festo, находятся на переднем крае разработки интеллектуальных роботов для различных промышленных применений. Рынок страны находится на пути к расширению в среднем примерно на 20,9%.

- **Великобритания, Франция и Италия**: Эти страны также являются ключевыми игроками на европейском рынке человекоподобных роботов, извлекая выгоду из сильных исследовательских институтов и инвестиций в робототехнику.

- **Скандинавские страны**: Дания и Швеция известны своим вкладом в совместную робототехнику и промышленную автоматизацию. Такие компании, как Universal Robots и ABB, лидируют в разработке гибких и удобных в использовании роботов.

e) Ближний Восток и Африка

- **Регион ССАГПЗ (GCC)**: Страны Совета сотрудничества Арабских государств Персидского залива (ССАГПЗ), особенно Саудовская Аравия и ОАЭ, вкладывают значительные средства в робототехнику и автоматизацию в рамках своих стратегий диверсификации экономики. В регионе наблюдается значительный рост внедрения человекоподобных роботов для различных применений, включая здравоохранение и обслуживание клиентов.

2) Компании в секторе человекоподобных роботов

Рынок человекоподобных роботов характеризуется разнообразием компаний, разбросанных по Северной Америке, Азиатско-Тихоокеанскому региону, Европе и другим регионам. Ключевые игроки, такие как Tesla, Boston Dynamics, SoftBank Robotics и UBTECH Robotics, стимулируют инновации и коммерциализацию в этом секторе. Географическое распределение этих компаний подчёркивает глобальный характер рынка человекоподобных роботов, значительный вклад в который вносят США, Китай, Япония, Южная Корея и различные европейские страны.

3) Известные мировые бренды Человекоподобных Роботов

- **Sophia (Hanson Robotics)**: Социальный робот, известный своей способностью взаимодействовать с людьми и выполнять различные задачи.

- **Pepper (SoftBank Robotics)**: Получеловеческий робот, предназначенный для считывания эмоций и взаимодействия с людьми на нескольких языках.

- **Atlas (Boston Dynamics)**: Усовершенствованный робот, разработанный для применения в реальных условиях и известный своей ловкостью и мобильностью.

- **Digit (Agility Robotics)**: Многоцелевой робот, предназначенный для навигации и выполнения задач в различных условиях.

- **Phoenix (Sanctuary AI)**: Робот общего назначения, предназначенный для выполнения широкого спектра человеческих задач.

- **Optimus (Tesla)**: робот, разработанный для промышленного применения с использованием искусственного интеллекта и производственного опыта Tesla.

- **TALOS (PAL Robotics)**: робот, разработанный для промышленного применения, известный своими высокопроизводительными датчиками и передовыми системами управления

4) Северная Америка

a) США:

- **Tesla**: Известная своим роботом Optimus, компания использует свой искусственный интеллект и производственный опыт для разработки человекоподобных роботов для промышленного применения.
- **Boston Dynamics**: Компания Boston Dynamics, лидер в области передовой робототехники, известна своим роботом Atlas, который разработан для реальных применений.
- **Agility robotics**: Специализируется на многоцелевых роботах, таких как Digit, которые предназначены для навигации и выполнения задач в различных средах.
- **Figure AI**: фокусируется на создании коммерчески жизнеспособных автономных роботов-гуманоидов, направленных на решение проблемы нехватки рабочей силы.
- **Promobot Corp**.: Разрабатывает сервисных роботов для связей с общественностью, личной помощи и ухода.
- **Kindred Inc**. Занимается разработкой роботов, управляемых искусственным интеллектом, для различных применений.
- **National Aeronautics and Space Administration (NASA)**: Участвует в разработке человекоподобных роботов для исследования космоса и других передовых применений.

b) Канада:

- **Sanctuary AI**: Известен своим человекоподобным роботом общего назначения Phoenix, который предназначен для выполнения широкого спектра человеческих задач.
- **Diligent Robotics** Разрабатывает роботов-помощников, таких как Moxi, для поддержки медицинских работников при выполнении рутинных задач.

5) Азиатско-Тихоокеанский регион

a) Китай:

- **UBTECH Robotics**: ведущая компания по производству искусственного интеллекта и гуманоидной робототехники, известная разработкой потребительских и бизнес-роботов.
- **Unitree Robotics**: Известна своим гуманоидным роботом H1, который установил стандарты скорости и манёвренности.
- **Hanson Robotics**: Известна своим социальным роботом Софией, которая может взаимодействовать с людьми и выполнять различные задачи.
- **Xiaomi**: Занимается разработкой передовой робототехники и технологий искусственного интеллекта.

b) Япония:

- **SoftBank Robotics**: Известна своими социальными роботами, такими как Pepper, которые могут считывать эмоции и взаимодействовать с людьми.
- **Honda Motor Co., Ltd**.: Разрабатывает продвинутых человекоподобных роботов для различных применений.
- **Toyota Motor Corporation**: Известна своим роботом T-HR3, которым можно управлять дистанционно и который предназначен для безопасного взаимодействия с людьми.
- **Kawada Robotics**: Занимается разработкой человекоподобных роботов для промышленного применения.
- **ROBOTIS**: Специализируется на компонентах и системах робототехники.
- **Hajime Research Institute, Ltd**.: Специализируется на передовых исследованиях и разработках в области робототехники.
- **Advanced Telecommunications Research Institute International (ATR)**: Участвует в передовых исследованиях в области робототехники.

c) Южная Корея:

- **Samsung Electronics**: Разрабатывает передовые технологии робототехники и искусственного интеллекта для различных приложений.
- **HYULIM Robot Co., Ltd**. Занимается разработкой человекоподобных роботов для промышленного и коммерческого использования.

6) Европа

a) Испания:

- **PAL robotics**: Известна настраиваемыми роботами-гуманоидами, такими как TALOS, разработанными для промышленного и коммерческого применения.
- **Macco Robotics**: Разрабатывает роботов для гостиничного сектора, уделяя особое внимание обслуживанию продуктов питания и напитков.

b) Соединенное Королевство:

- **Engineered Arts**: Известен своими роботами, Ameca и RoboThespian, которые используются в развлекательных и образовательных целях.
- **Shadow Robot Company**: Специализируется на роботизированных руках и системах с высокой артикуляцией.

c) Италия:

- **Istituto Italiano di Tecnologia (IIT)**: Занимается передовыми исследованиями и разработками в области робототехники.

7) Ближний Восток и Африка

a) Объединенные Арабские Эмираты:

- **Различные инициативы**: Регион инвестирует в робототехнику и автоматизацию в рамках своих стратегий диверсификации экономики.

8) Южная Америка

a) Бразилия и Аргентина:

- **Развивающиеся рынки**: Эти страны являются частью растущего южноамериканского рынка человекоподобных роботов, чему способствуют растущие инвестиции в автоматизацию и технологические достижения.

H. Экономический таймлайн

На экономическую целесообразность и сроки внедрения человекоподобных роботов существенное влияние оказали достижения в области технологий, снижение затрат и растущий спрос на автоматизацию.

- **Базовый сценарий**: Базовый сценарий прогнозирует совокупный годовой темп роста (CAGR) на 53% в период с 2025 по 2035 год, при этом поставки достигнут 1,4 млн единиц к 2035 году. Этот сценарий предполагает продолжение развития искусственного интеллекта и снижение затрат.

- **Вероятный сценарий**: ожидается, что к 2031 году поставки достигнут 1 миллиона единиц, что на четыре года опережает предыдущие ожидания благодаря ускоренному развитию комплексного искусственного интеллекта.

- **Сценарий "голубого неба"**: при самом оптимистичном сценарии рынок может достичь 154 миллиарда долларов к 2035 году, что сопоставимо с мировым рынком электромобилей и одной третью мирового рынка смартфонов по состоянию на 2021 год. Этот сценарий предполагает, что все технологические и рыночные препятствия будут преодолены

- **Спрос на опасные работы**: Потребность в роботах для выполнения опасных работ возрастает в соответствии с национальной политикой. Анализ чувствительности показывает, что мировой спрос может составить от 1,1 до 3,5 млн единиц, при условии 5–15% замещения в сфере специальных операций и автомобилестроения.

- **Специальные операции**: Человекоподобные роботы особенно привлекательны для специальных операций, таких как спасение при стихийных бедствиях, техническое обслуживание ядерных реакторов и выполнение опасных задач химической промышленности, где готовность человека выполнять эти работы невелика

- **Увеличение инвестиций**: усиливается приверженность со стороны цепочки поставок, стартапов в США и Азии, а также множества зарегистрированных компаний, создающих новые подразделения роботов. Государственная поддержка, особенно со стороны Китая, также является важным фактором, стимулирующим рост рынка.

- **Кривая затрат**: кривая затрат на человекоподобных роботов снижается быстрее, чем ожидалось, что означает лучшую экономичность применения и более быстрые сроки коммерциализации.

- **Общий адресуемый рынок (TAM)**: по прогнозам, к 2035 году объём рынка человекоподобных роботов достигнет 38 миллиардов долларов, по сравнению с первоначальным прогнозом в 6 миллиардов долларов. Это увеличение обусловлено четырёхкратным увеличением прогнозов поставок до 1,4 миллиона единиц.

- **Снижение затрат**: Стоимость спецификации для высокопроизводительных человекоподобных роботов снизилась на 40% до 150 000 долларов за единицу в 2023 году по сравнению с 250 000 долларами годом ранее. Это сокращение обусловлено доступностью более дешёвых компонентов и более широкой внутренней цепочкой поставок.

- **Заводские приложения**: Сроки подачи заводских заявок были ускорены на один год, и теперь ожидается, что они будут экономически жизнеспособными в период с 2024 по 2027 год по сравнению с предыдущей оценкой в 2025–2028 годах.

- **Потребительские приложения**: Сроки подачи заявок потребителями также были ускорены на 2–4 года, и теперь ожидается, что они будут экономически жизнеспособными в период с 2028 по 2031 год по сравнению с предыдущей оценкой на период с 2030 по 2035 год.

I. Технологический прогресс

Прогресс как в аппаратном, так и в программном обеспечении, включая разработку LLM и комплексного искусственного интеллекта, значительно расширил возможности человекоподобных роботов. Эти достижения прокладывают путь к тому, чтобы человекоподобные роботы стали более интегрированными в различные аспекты повседневной жизни и промышленности, открывая многообещающие перспективы для будущего робототехники.

1) Аппаратный прогресс человекоподобных роботов

При разработке человекоподобных роботов были достигнуты значительные успехи в аппаратном обеспечении, что сделало этих роботов более универсальными, эффективными и способными выполнять сложные задачи.

- **Мобильность и ловкость на двух ногах**: Гуманоидные роботы добились значительных улучшений в мобильности на двух ногах, что позволяет им быстро и точно ориентироваться в сложных условиях. Например, Digit от Agility

Robotics демонстрирует этот прогресс своей способностью передвигаться на двух ногах, демонстрируя потенциал роботов для оказания помощи в областях, которые ранее считались слишком сложными для автоматизации. Аналогичным образом, были отмечены достижения в ловкости, особенно в манипулировании предметами, хотя в этой области по-прежнему есть возможности для совершенствования.

- **Системы сенсорного восприятия и обратной связи**: Интеграция передовых датчиков и систем обратной связи позволила человекоподобным роботам лучше воспринимать окружающую среду и взаимодействовать с ней. Эти разработки проложили путь к повышению автономности и возможностей взаимодействия, позволяя роботам более эффективно наблюдать за окружающей средой и реагировать на неё.

- **Снижение стоимости компонентов**: произошло значительное снижение стоимости компонентов, необходимых для создания человекоподобных роботов, таких как высокоточные шестерни, приводы и аккумуляторы. Такое снижение затрат в первую очередь обусловлено наличием более дешёвых компонентов, большим количеством вариантов цепочки поставок, а также усовершенствованием конструкции и технологий производства. Например, стоимость производства человекоподобных роботов снизилась с 50 000–250 000 долларов за единицу до 30 000–150 000 долларов, что способствовало более быстрой коммерциализации.

2) Прогресс программного обеспечения человекоподобных роботов

Достижения в области программного обеспечения сыграли не менее важную роль в эволюции человекоподобных роботов, достигнув значительного прогресса в таких областях, как:

- **Большие языковые модели (LLM)**: Разработка роботизированных LLM, таких как Google PaLM-E и RT-2, стала ключевым фактором в продвижении человекоподобных роботов. Эти модели повышают способность роботов обрабатывать команды на естественном языке и анализировать сценарии выполнения задач с помощью зрения, позволяя им выполнять задачи с уровнем понимания и отзывчивости, близким к человеческому восприятию.

- **Комплексный ИИ**: Переход к комплексному ИИ, при котором модели могут обучаться самостоятельно без необходимости ручного программирования инженерами, ускорил разработку роботов. Такой подход позволяет роботам быстрее адаптироваться к новым ситуациям и выполнять более широкий спектр задач. Optimus Gen 2 от Tesla - пример гуманоидного робота, пользующегося преимуществами комплексного искусственного интеллекта, демонстрирующего быструю итерацию продукта и способность выполнять задачи автономно.

3) Разработка роботизированных LLMS

- **Внедрение PaLM-E и RT-2**: в 2023 году были достигнуты значительные успехи в области роботизированных систем управления с внедрением PaLM-E **и RT-2**. Эти модели представляют собой скачок вперёд в интеграции искусственного интеллекта с робототехникой, позволяя роботам понимать окружающую среду и взаимодействовать с ней более сложными способами.

- **Мультимодальные возможностиPaLM-E**: PaLM-E, разработанный Google, представляет собой воплощённую мультимодальную языковую модель, предназначенную для робототехники. Он сочетает в себе мощь больших языковых моделей с возможностью обработки визуальных и сенсорных данных, позволяя роботам выполнять задачи в различных режимах. Архитектура PaLM-E позволяет ему понимать и выполнять задачи на различных типах роботов и для различных модальностей, включая изображения, состояния роботов и представления нейронных сцен.

- **Модель Vision-Language-Action от RT-2**: RT-2, или Robotics Transformer 2, разработанная Google DeepMind, представляет собой модель vision-language-action (VLA), которая обучается как из Интернета, так и из данных робототехники. Это переводит высокоуровневые рассуждения в низкоуровневые машинно-исполняемые инструкции, значительно повышая способность роботов справляться с непредвиденными ситуациями и делая их более универсальными в качестве универсальных машин.

- **Влияние на робототехнику**: Разработка PaLM-E и RT-2 имеет глубокие последствия для области робототехники. Эти модели позволяют роботам выполнять задачи с более высокой степенью автономии и адаптируемости, сокращая разрыв между теоретическими возможностями искусственного интеллекта и практическими приложениями в робототехнике.

4) Комплексный искусственный интеллект в робототехнике

Интеграция LLMS и комплексного искусственного интеллекта в робототехнику привела к:

- **Улучшенное взаимодействие человека и робота**: LLMS и комплексный искусственный интеллект значительно улучшили взаимодействие человека и робота, сделав роботов более способными понимать команды человека и реагировать на них естественным и интуитивно понятным образом. Это открыло новые возможности для человекоподобных роботов в различных отраслях промышленности и условиях.

- **Ускоренное обучение и адаптация**: Эти технологии позволили человекоподобным роботам извлекать уроки из опыта и более эффективно адаптироваться к новым задачам. Проект RT-X, например, направлен на объединение данных и ресурсов из нескольких лабораторий робототехники для создания универсальных роботов общего назначения, которые могут эффективно работать за пределами ограниченных лабораторных условий.
- **Повышенная автономность**: Достижения в области LLM и комплексного искусственного интеллекта способствовали повышению автономности человекоподобных роботов, позволяя им выполнять сложные задачи с минимальным вмешательством человека. Эта автономность имеет решающее значение для использования человекоподобных роботов в реальных приложениях, где необходимы человекоподобное взаимодействие и адаптивность

J. Состояние отрасли

Человекоподобные роботы предлагают значительные потенциальные преимущества для военного применения, включая расширенные возможности, операционную эффективность и экономию средств. Однако их внедрение также сопряжено с этическими, юридическими и техническими проблемами, которые необходимо тщательно решать. Экономические выгоды от инвестиций в человекоподобных роботов существенны, с потенциальным повышением производительности, масштабируемости и долгосрочным технологическим прогрессом. Поскольку технологии продолжают развиваться, крайне важно учитывать связанные с этим риски и обеспечивать ответственное и этичное использование человекоподобных роботов в вооружённых силах.

1) Современное использование роботов

- **Производство**: Человекоподобные роботы используются на производстве для выполнения таких задач, как сборка, контроль качества и погрузочно-разгрузочные работы. Они могут выполнять повторяющиеся задачи с высокой точностью и могут работать в условиях, которые могут быть опасны для человека.
- **Здравоохранение**: В здравоохранении человекоподобные роботы помогают в уходе за пациентами, реабилитации и хирургии. Они могут контролировать жизненно важные показатели, помогать в физиотерапии и даже выполнять сложные хирургические процедуры.
- **Электронная коммерция и складирование**: Человекоподобные роботы используются в электронной коммерции и на складах для управления логистикой, такой как сортировка и транспортировка товаров. Они помогают повысить эффективность и снизить трудозатраты.
- **Обслуживание клиентов и гостиничный бизнес**: человекоподобные роботы используются в ролях обслуживания клиентов, таких как консьержи, администраторы и гиды. Они могут взаимодействовать с клиентами, предоставлять информацию и улучшать качество обслуживания клиентов.
- **Безопасность**: Человекоподобные роботы используются в сфере безопасности для патрулирования территорий, обнаружения вторжений и мониторинга на предмет угроз безопасности. Они могут работать непрерывно, не испытывая усталости, и предоставлять данные операторам-людям в режиме реального времени.
- **Образование и исследования**: В образовательных учреждениях человекоподобные роботы используются в качестве учебных пособий и исследовательских инструментов. Они помогают студентам узнать о робототехнике, программировании и искусственном интеллекте.
- **Развлечения**: человекоподобные роботы также используются в сфере развлечений, например, для выступлений на мероприятиях, в качестве экскурсоводов в музеях и даже для дирижирования оркестрами

○ *Потенциальное применение (в будущем)*

- **Военные**: Человекоподобные роботы могут использоваться в военных целях для таких задач, как разведка, обезвреживание бомб и материально-техническое обеспечение. Они могут действовать в опасных условиях, снижая риск для солдат-людей.
- **Кибербезопасность**: Человекоподобные роботы могли бы сыграть определённую роль в кибербезопасности путём мониторинга и защиты биологических данных и систем от киберугроз. Их продвинутые датчики и возможности искусственного интеллекта делают их подходящими для этой роли.
- **Нефтегазовая промышленность**: В нефтегазовой промышленности человекоподобные роботы могут использоваться для инспекции, технического обслуживания и ремонта морских платформ и трубопроводов. Они могут работать во взрывоопасных средах, что снижает необходимость вмешательства человека.
- **Добыча полезных ископаемых**: Человекоподобные роботы могут использоваться в горнодобывающей промышленности для выполнения таких задач, как бурение, добыча руды и проверки безопасности. Они могут работать в опасных и замкнутых пространствах, повышая безопасность и эффективность.
- **Финансовые услуги и фондовые рынки**: Человекоподобные роботы могли бы оказывать помощь в сфере финансовых услуг, обеспечивая поддержку клиентов, проводя транзакции и анализируя рыночные данные. Их способность

быстро обрабатывать большие объёмы информации делает их ценными в этом секторе.

- **девелопмент**: В сфере недвижимости человекоподобные роботы могут использоваться для осмотра имущества, технического обслуживания и взаимодействия с клиентами. Они могут проводить виртуальные туры и помогать с задачами по управлению недвижимостью.
- **Пищевая промышленность**: Человекоподобные роботы могут использоваться в пищевой промышленности для выполнения таких задач, как заполнение полок, приготовление пищи и доставка продуктов. Они могут помочь повысить эффективность и снизить трудозатраты.
- **Самолёты**: В авиационной промышленности человекоподобные роботы могли бы помогать в техническом обслуживании, инспекциях и сборке компонентов самолётов. Их точность и способность работать в ограниченном пространстве делают их подходящими для этой роли.
- **Морское дело и судоходство**: роботы могут использоваться в морском судоходстве для таких задач, как обработка грузов, техническое обслуживание судов и проверки безопасности. Они могут работать в суровых морских условиях, повышая эффективность и безопасность.
- **Умные города**: В умных городах роботы могут использоваться для различных задач, таких как управление дорожным движением, общественная безопасность и обслуживание инфраструктуры. Они могут взаимодействовать с гражданами, предоставлять информацию и помогать управлять городской средой.

2) Подробное описание последствий для отрасли

a) Военные

- **Преимущества**: Повышение безопасности военнослужащих за счёт выполнения опасных задач, таких как обезвреживание бомб и разведывательные миссии, без риска для человеческих жизней.
- **Риски**: Возможность повышения летальности и этические проблемы, связанные с автономным принятием решений в боевых ситуациях.
- **Области применения**: Боевая поддержка, поисково-спасательные операции и логистика.
- **Экономические преимущества**: Сокращение расходов на обучение и здравоохранение, связанных с солдатами-людьми.

b) Кибербезопасность

- **Преимущества**: Улучшенные протоколы безопасности при обращении с конфиденциальными биологическими данными и материалами, снижающие риск биологической опасности.
- **Риски**: Уязвимость к взлому и неправильному использованию, потенциально ведущая к угрозам биозащиты.
- **Области применения**: Безопасное обращение с биологически опасными материалами и их анализ, надзор за зонами биологической безопасности.
- **Экономические преимущества**: Повышение эффективности управления биозащитой, потенциальное снижение затрат, связанных с нарушениями биозащиты.

c) Нефтегазовая промышленность

- **Преимущества**: Повышение безопасности за счёт выполнения опасных работ, таких как бурение и осмотр трубопроводов, снижение несчастных случаев на производстве.
- **Риски**: Высокие первоначальные инвестиционные затраты и потенциальная смена работы.
- **Области применения**: Автоматизированное бурение, техническое обслуживание и инспекция морских платформ и трубопроводов.
- **Экономические преимущества**: Эффективность эксплуатации и сокращение времени простоя, что приводит к экономии средств.

d) Добыча полезных ископаемых (металлов, золота)

- **Преимущества**: Повышенная безопасность в опасных условиях добычи полезных ископаемых и повышенная эффективность эксплуатации.
- **Риски**: смена работы и зависимость от технологий, которые могут давать сбои в удалённых или суровых условиях.
- **Области применения**: Разведка, бурение и переработка руды в опасных или труднодоступных районах.
- **Экономические преимущества**: Повышение производительности и снижение эксплуатационных расходов за счёт автоматизации.

e) Финансовые услуги и фондовые рынки

- **Преимущества**: повышенная точность и скорость анализа данных и процессов принятия решений.
- **Риски**: Вероятность ошибок алгоритмов и манипулирования финансовым рынком.
- **Приложения**: Автоматическая торговля, оценка рисков и обслуживание клиентов.
- **Экономические преимущества**: Повышение эффективности рынка и снижение эксплуатационных расходов.

f) Девелопмент недвижимости

- **Преимущества**: Улучшенное планирование и выполнение проекта за счёт точных измерений и трудоёмкости.
- **Риски**: Высокие первоначальные затраты и вероятность ошибок в сложных проектах разработки.
- **Приложения**: инспекции объектов, строительные задачи и взаимодействие с клиентами в центрах продаж.
- **Экономические преимущества**: упрощение процессов разработки и снижение затрат на рабочую силу.

g) Электронная коммерция в пищевой промышленности

- **Преимущества**: повышенная эффективность выполнения заказов и управления запасами.
- **Риски**: потенциальная потеря работы и проблемы при обращении с деликатными продуктами.
- **Области применения**: автоматизированная комплектация и упаковка, обслуживание клиентов и аудит запасов.
- **Экономические выгоды**: Повышение операционной эффективности и удовлетворённости клиентов за счёт более быстрого обслуживания.

h) Воздушное судно

- **Преимущества**: Точность производственных процессов и задач технического обслуживания.
- **Риски**: Высокие затраты на разработку и вероятность ошибок в критически важных системах безопасности.
- **Области применения**: Сборка, проверка и ремонт авиационных компонентов.
- **Экономические преимущества**: Снижение производственных затрат и затрат на техническое обслуживание, улучшение показателей безопасности.

i) Производство

- **Преимущества**: Повышенная эффективность производства и гибкость при решении разнообразных задач.
- **Риски**: смена работы и первоначальные инвестиционные затраты.
- **Области применения**: Сборочные линии, контроль качества и логистика.
- **Экономические преимущества**: повышение производительности и снижение затрат на рабочую силу.

j) Здравоохранение

- **Преимущества**: Помощь в проведении операций, уходе за пациентами и реабилитации с точностью и последовательностью.
- **Риски**: этические соображения, касающиеся взаимодействия с пациентом, и возможные сбои в работе.
- **Области применения**: Хирургическая помощь, наблюдение за пациентом и физиотерапия.
- **Экономические преимущества**: улучшение результатов лечения пациентов и потенциальное снижение затрат на здравоохранение.

k) Морское дело и судоходство

- **Преимущества**: Повышенная безопасность в опасных условиях и повышенная эффективность обработки грузов.
- **Риски**: Навигационные ошибки и потенциальная возможность пиратства или угона самолёта.
- **Области применения**: погрузка и разгрузка грузов, техническое обслуживание судов и инспекции в море.
- **Экономические преимущества**: снижение эксплуатационных расходов и увеличение времени выполнения работ.

l) Умный город

- **Преимущества**: Улучшение общественных услуг и безопасности благодаря задачам наблюдения и технического обслуживания.
- **Риски**: проблемы конфиденциальности и высокие затраты на внедрение.
- **Области применения**: Обслуживание общественных пространств, утилизация отходов и патрулирование безопасности.
- **Экономические выгоды**: повышение качества жизни жителей и потенциальная привлекательность для бизнеса.