ТОЛЬКО ПРОТИВОРЕЧИВЫЕ СОВЕТЫ ПОМОГАЮТ ПОНЯТЬ, ЧТО ТАКОЕ ИБ

ИРОНИЯ БЕЗОПАСНОСТИ

ДАЙДЖЕСТ. 2024 / 05

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.TO

SPONSR.RU

TELEGRAM

Рубрика: Новичок

Для новичков в мире ИБ или для тех, кто предпочитает работать с контентом без финансовых обязательств.

Рубрика: Специалист

Для постоянных читателей, которые заинтересованы быть в курсе последних тенденций в мире кибербезопасности

Рубрика: Профессионал

Для ИТ-специалистов, экспертов, и энтузиастов, которые готовы погрузится в сложный мир ИБ.

Больше материалов: Boosty | Sponsr | TG

Новости

Больше материалов: Boosty | Sponsr | TG

Судебный иск FTC против Ring

📌 **Судебный иск FTC против Ring:** Федеральная торговая комиссия (FTC) подала в суд на Ring, компанию по производству камер домашней безопасности, принадлежащую Amazon, за неспособность защитить конфиденциальность потребителей. В жалобе FTC, поданной в мае 2023 года, Ring обвинялась в том, что она позволяла сотрудникам и подрядчикам получать доступ к личным видеозаписям клиентов без их согласия и не принимала надлежащих мер безопасности. Эта халатность привела к несанкционированному доступу хакеров и сотрудников, что поставило под угрозу конфиденциальность и безопасность видеоматериалов потребителей.

📌 **Урегулирование и возврат средств:** в результате судебного процесса Ring согласилась на урегулирование, которое включало финансовый штраф и создание более надёжной программы обеспечения конфиденциальности и безопасности. FTC выплачивает возмещение на сумму более 5,6 миллионов долларов примерно 117 044 пострадавшим клиентам Ring. Эти возмещения осуществляются через PayPal, и клиентам рекомендуется потребовать свои платежи в течение 30 дней.

📌 **Подробности урегулирования:** По условиям соглашения Ring должна была выплатить 5,8 миллиона долларов, удалить незаконно полученные видеозаписи и принять новые строгие меры по обеспечению конфиденциальности и безопасности. Эти меры включают многофакторную аутентификацию и ограничения доступа сотрудников к видео для пользователей. FTC подчеркнула, что эти шаги были необходимы для предотвращения будущих нарушений конфиденциальности и восстановления доверия потребителей к продукции Ring.

📌 **Ответ Ring:** Компания Ring заявила, что она рассмотрела многие вопросы, вызывавшие обеспокоенность FTC, до начала расследования и не согласилась с некоторыми утверждениями. Однако компания решила пойти на мировую, чтобы избежать длительных судебных разбирательств и сосредоточиться на улучшении своих продуктов и услуг для клиентов.

📌 **Информация для потребителей и поддержка:** FTC чётко дала понять, что никогда не требует от потребителей информацию о платежах или учётной записи для получения возмещения

ИИ на службе авиации

Недавние достижения в области ИИ привели к значительным достижениям в секторе военной авиации, особенно интеграции ИИ с реактивными истребителями.

📌 **Достижения ИИ в военной авиации:** DARPA и ВВС США находятся активно внедряют ИИ в реактивные истребители. Эта интеграция достигла стадии, когда самолёты, управляемые искусственным интеллектом, такие как X-62A VISTA, теперь способны вступать в воздушные бои с самолётами, пилотируемыми человеком

📌 **Первый успешный воздушный бой ИИ против человека:** В сентябре 2023 года произошло знаменательное событие: управляемый ИИ X-62A VISTA провёл тренировочный воздушный бой против F-16, пилотируемого человеком. Это испытание, проведённое на базе ВВС Эдвардс в Калифорнии, стало первым успешным воздушным боем между реактивным самолётом, управляемым ИИ, и пилотом-человеком. ИИ продемонстрировал способность выполнять сложные боевые манёвры безопасно и эффективно.

📌 **Безопасность и контроль:** несмотря на автономные возможности искусственного интеллекта, на борту X-62A находились пилоты-люди, которые при необходимости могли отключить систему искусственного интеллекта. Однако во время испытаний не было необходимости во вмешательстве человека, что свидетельствует о высоком уровне надёжности и безопасности работы ИИ

📌 **Последствия для боевых действий в будущем:** Успешная интеграция ИИ в истребители рассматривается как трансформационный момент в военной авиации. Это говорит о будущем, в котором ИИ потенциально может справляться с динамичными боевыми сценариями, позволяя пилотам-людям сосредоточиться на стратегии и контроле, а не на непосредственном участии

📌 **Продолжение разработки и тестирования:** Продолжающееся развитие ИИ в военной авиации направлено на расширение возможностей ИИ-пилотов, включая их способность принимать автономные решения в сложных и быстро меняющихся боевых условиях. В будущих тестах, вероятно, будут рассмотрены более сложные сценарии и усовершенствованы процессы принятия решений ИИ

Change Healthcare / UnitedHealth Group

Change Healthcare, крупный игрок в секторе медицинских технологий США, столкнулся со значительными проблемами в области кибербезопасности после атаки программ-вымогателей, приписываемой BlackCat/ALPHV group:

📌 **Первоначальная атака и выплата выкупа:** 21 февраля 2024 года компания Change Healthcare подверглась разрушительной кибератаке, которая привела к широкомасштабным операционным проблемам в системе здравоохранения США. Компания, дочерняя компания UnitedHealth Group, в конечном счете заплатила выкуп в размере $22M в пользу BlackCat/ALPHV в надежде восстановить свои услуги и защитить данные пациентов

📌 **Последующие попытки вымогательства:** несмотря на первоначальную выплату выкупа, Change Healthcare столкнулась с дальнейшим вымогательством со стороны новой группы программ-вымогателей под названием RansomHub. Эта группа утверждала, что обладает четырьмя терабайтами данных, украденных во время первоначальной атаки BlackCat/ALPHV, и потребовала свой собственный выкуп, угрожая продать информацию в даркнете, если их требования не будут выполнены

📌 **Влияние на медицинские услуги:** Кибератака серьёзно повлияла на деятельность Change Healthcare, повлияв на способность больниц проверять страховые выплаты, обрабатывать процедуры для пациентов и выставлять счета. Аптеки также столкнулись с трудностями в оплате отпускаемых по рецепту лекарств из-за недоступности информации о страховке, что значительно нарушило обслуживание пациентов и финансовые операции поставщиков медицинских услуг

📌 **Проблемы с утечкой данных:** В Change Healthcare сохраняются опасения по поводу безопасности данных пациентов. Компания не смогла подтвердить, действительно ли данные пациентов были украдены.

📌 **Реакция:** Учитывая серьёзность атаки и её последствия, Госдеп США предложил вознаграждение в размере $10M за информацию о личности или местонахождении членов ALPHV/BlackCat.

📌 **Последствия:** Атака на Change Healthcare выявила уязвимость сектора здравоохранения к атакам программ-вымогателей

ArcaneDoor

В кампании по кибершпионажу ArcaneDoor, которая началась в ноябре 2023 года, участвовали хакеры, спонсируемые государством, которые использовали две 0day уязвимости в продуктах Cisco Adaptive Security Appliance (ASA) и Firepower Threat Defense (FTD).

📌 **0-day:** Хакеры использовали две уязвимости нулевого дня, CVE-2024-20353 и CVE-2024-20359, которые позволяли проводить DoS-атаки типа "отказ в обслуживании" и выполнение кода.

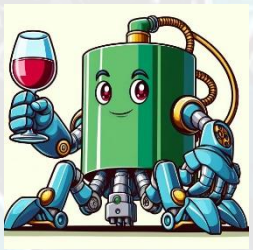
📌 **Сложное внедрение вредоносных программ:** Злоумышленники внедрили два типа вредоносных программ - Line Dancer и Line Runner. Line Dancer - это загрузчик шеллкода в памяти, который облегчает выполнение произвольных полезных нагрузок шеллкода, в то время как Line Runner - это бэкдор, который позволяет злоумышленникам запускать произвольный Lua-код на скомпрометированных системах.

📌 **Глобальное воздействие:** Кампания была нацелена на госсектор, используя уязвимости для получения доступа к конфиденциальной информации и потенциального осуществления дальнейших вредоносных действий, таких как утечка данных и горизонтальное перемещение внутри сетей.

📌 **Реакция и меры по устранению:** Cisco отреагировала на это выпуском обновлений для системы безопасности, исправляющих уязвимости, и выпустила рекомендации, призывающие клиентов обновить свои устройства. Они также рекомендовали отслеживать системные журналы на наличие признаков компрометации, таких как незапланированные перезагрузки или несанкционированные изменения конфигурации.

📌 **Внимание к атрибуции и шпионажу:** Хакерская группа, идентифицированная Cisco Talos как UAT4356, а Microsoft - как STORM-1849, продемонстрировала явную направленность на шпионаж. Считается, что кампания спонсировалась государством, и некоторые источники предполагают, что за атаками может стоять Китай.

📌 **Тенденция нацеливания на устройства периметра сети:** инцидент является частью тенденции, когда спонсируемые государством субъекты нацеливаются на устройства периметра сети, такие как брандмауэры и VPN, чтобы получить первоначальный доступ к целевым сетям в целях шпионажа



APT29

APT29, также известный как Midnight Blizzard, BlueBravo или Cozy Bear, был обнаружен с помощью нового бэкдора WINELOADER, предназначенного для политических партий Германии. Эта кампания знаменует собой значительное смещение акцента группы с её традиционных целей — дипломатических миссий — на политические структуры, что указывает на более цели по сбору политической информации.

Цель и сроки:

📌 Кампания была направлена против политических партий Германии, и фишинговые электронные письма были отправлены примерно 26 февраля 2024 года. В этих электронных письмах был логотип Христианско-демократического союза (ХДС) и вредоносные ссылки.

Технические подробности:

📌 Считается, что WINELOADER является вариантом семейств кодов BURNTBATTER и MUSKYBEAT, которые были связаны с APT29 компанией Mandiant.

📌 Вредоносная программа использует сложные методы, такие как дополнительная загрузка библиотеки DLL, шифрование RC4 для расшифровки полезной нагрузки и тактику предотвращения обнаружения, такую как проверка имён процессов/библиотек DLL и обход пользовательского режима Ntdll.

Первоначальный доступ:

📌 Первоначальный доступ был получен с помощью фишинговых вложений, ведущих к взломанному веб-сайту "waterforvoiceless[.]org", на котором размещался PYTCAB-дроппер. Затем этот дроппер облегчил загрузку и выполнение полезной нагрузки WINELOADER.

Влияние:

📌 Этот переход к преследованию политических партий отражает растущий интерес к влиянию или пониманию политической динамики на Западе, особенно в контексте сохраняющейся геополитической напряжённости.

📌 Преследование политических партий рассматривается как стратегический шаг по сбору оперативной информации, которая потенциально может повлиять на политические результаты или стратегии в Европе и за её пределами.

Последствия:

📌 Кампания против немецких политпартий рассматривается не как изолированный инцидент, а скорее как часть более широкой стратегии, которая может быть направлена против других западных политических образований.

AWS спишет деньги даже отсутствие данных в S3

В статье рассматривается важная проблема, связанная с тем, что пустое хранилище AWS S3 может привести к неожиданно высоким расходам на AWS из-за несанкционированных входящих запросов.

Это практическое исследование служит предостережением о потенциальных финансовых рисках, связанных с сервисами AWS, в частности с S3, и подчёркивает важность понимания практики выставления счетов AWS и безопасной настройки сервисов AWS во избежание непредвиденных расходов.

📌 **Неожиданно высокие затраты:** у автора неожиданно резко вырос счёт за AWS, составив более 1300 долларов, из-за того, что почти 100 000 000 запросов S3 PUT были выполнены в течение одного дня в пустой корзине S3, которую он настроил для тестирования.

📌 **Источник запросов:** изначально AWS по умолчанию не регистрирует запросы, выполняемые в корзинах S3. Автору пришлось включить журналы AWS CloudTrail, чтобы идентифицировать источник запросов. Было обнаружено, что неправильно настроенные системы пытались сохранить данные в его личном хранилище S3.

📌 **Выставление счетов за несанкционированные запросы: AWS** взимает плату за несанкционированные входящие запросы в корзины S3. Это было подтверждено во время общения автора со службой поддержки AWS, в котором подчёркивалась важная политика выставления счетов, согласно которой владелец корзины оплачивает входящие запросы независимо от их статуса авторизации.

📌 **Предотвращение и защита:** В статье отмечается, что не существует простого способа предотвратить подобные инциденты, кроме удаления корзины. AWS не позволяет защитить корзину с помощью сервисов, как CloudFront или WAF, при прямом доступе к ней через S3 API.

📌 **Расследование AWS:** после инцидента AWS начала расследование проблемы, о чем свидетельствует твит Джеффа Барра, известного евангелиста AWS. Это говорит о том, что AWS осведомлена о потенциальных проблемах и, возможно, рассматривает способы их устранения.

Сотрудники T-Mobile и Verizon сообщают о получении предложений на сумму 300 долларов за содействие в несанкционированной замене SIM-карты.

📌 **Предложения о подкупе сотрудников телекоммуникационных компаний: Сотрудники** T-Mobile и Verizon, включая бывших сотрудников, сообщили о получении нежелательных сообщений с предложением 300 долларов за каждую замену SIM-карты, которую они совершат. Этими сообщениями поделились на Reddit, продемонстрировав скриншоты текстов.

📌 **Способ связи:** Злоумышленники использовали различные способы связи, включая текстовые сообщения и зашифрованные платформы, такие как Telegram, чтобы связаться с сотрудниками. В сообщениях часто утверждалось, что они получили контактную информацию сотрудников из каталогов компаний.

📌 **Потенциальные инсайдерские угрозы: Ситуация** вызывает опасения по поводу инсайдерских угроз внутри телекоммуникационных компаний, поскольку сообщения были адресованы нынешним и бывшим сотрудникам, которые могли иметь доступ к системам, необходимым для обмена SIM-картами.

📌 **Ответы компаний:** и T-Mobile, и Verizon знают об этих инцидентах. В T-Mobile заявили, что никаких системных нарушений не было, и что они расследуют сообщения. Реакция Verizon в настоящее время не приводится подробно в отчётах.

📌 **Последствия замены SIM-карты:** Замена SIM-карты может привести к серьёзным нарушениям безопасности, позволяя злоумышленникам обойти двухфакторную аутентификацию, получить доступ к личной и финансовой информации и потенциально привести к финансовому мошенничеству и краже личных данных.

📌 **Профилактические меры и рекомендации:** Телекоммуникационным компаниям рекомендуется усилить свои внутренние меры безопасности и процессы проверки сотрудников для предотвращения подобных инцидентов. Сотрудникам рекомендуется сообщать о любых подозрительных действиях и не соглашаться на подобные предложения.

Более 100 человек арестованы в Испании по делу о мошенничестве в WhatsApp на сумму 900 000 долларов

📌 Испанская полиция арестовала 34 человека, подозреваемых в совершении различных онлайн-мошенничеств, изъяла огнестрельное оружие, катану, бейсбольную биту и 80 000 евро.

📌 Предполагаемые киберпреступники обвиняются в мошенничестве с использованием электронной почты, телефона и текстовых сообщений, включая мошенничество с "сыном в беде" и манипулирование накладными от технологических компаний.

📌 Считается, что они заработали около 3 миллионов евро и имели доступ к базе данных с украденной информацией о четырёх миллионах человек.

📌 Эта операция является частью более масштабных усилий испанских правоохранительных органов по борьбе с киберпреступностью и мошенничеством.

📌 В ходе отдельной операции испанская полиция арестовала 55 человек, причастных к широкомасштабной киберпреступной операции, которая включала фишинг, подмену SIM-карт и многое другое.

📌 Эта группировка, называвшая себя “Черные пантеры” и базировавшаяся в Барселоне, действовала четырьмя отдельными ячейками, которые похитили около 250 000 евро у почти 100 человек с помощью различных мошеннических действий, которые включали в себя захват банковских счетов.

📌 Мошенничество с выдачей себя за человека, о котором сообщалось в Федеральную торговую комиссию, обошлось жертвам примерно в 1,1 миллиарда долларов в 2023 году, что более чем в три раза превышает то, о чем потребители сообщали в 2020 году.

📌 Из числа зарегистрированных случаев в 2023 году около 40 % так или иначе были связаны с онлайн—мошенничеством, в то время как на более традиционный метод — мошеннические телефонные звонки - приходилось 32%.

📌 Киберпреступники нацеливаются на студентов колледжей с поддельными предложениями о работе в сфере биологических наук и здравоохранения в надежде получить вознаграждение от жертв.

📌 Исследователи из Proofpoint раскрыли кампанию, которая была направлена против студентов университетов в Северной Америке в мае и июне — в сезон выпускных экзаменов — с помощью мошеннических электронных писем на тему трудоустройства.

📌 Глубокие подделки добавляют коварства некоторым схемам сексуальной эксплуатации, согласно новому предупреждению Центра жалоб на интернет-преступность ФБР (IC3).

📌 Некоторые вымогатели прибегают к использованию технологий для создания изображений или видеороликов откровенного сексуального содержания из безобидного контента, размещенного в Интернете.

📌 Хакеры атакуют счета азиатских банков, используя украденные данные распознавания лиц для обхода мер безопасности.

📌 Испанская полиция арестовала 19-летнего подростка, подозреваемого в совершении ряда громких кибератак, назвав его “серьёзной угрозой национальной безопасности”.

Иранские кибершпионы

📌 **Тактика маскировки:** APT42 выдаёт себя за известные новостные агентства и аналитические центры, такие как The Washington Post, The Economist и The Jerusalem Post, чтобы воздействовать на журналистов, исследователей и активистов в западных странах и на Ближнем Востоке. Эта кампания, которая началась в 2021 году и продолжается до сих пор, включает в себя создание поддельных ссылок на веб-сайты для получения учётных данных для входа в систему от жертв.

📌 **Минимальное воздействие:** Методы, применяемые APT42, разработаны таким образом, чтобы оставлять минимальное воздействие, что усложняет сетевым защитникам задачу обнаружения и пресечения их деятельности. Такая скрытность достигается за счёт использования методов тайпосквоттинга и социальной инженерии.

📌 **Тайпсквоттинг и социнженерия:** APT42 часто использует тайпсквоттинг, приобретая веб-домены, которые выглядят как настоящие, но содержат небольшие ошибки или изменения, для создания вредоносных ссылок. Эти ссылки перенаправляют получателей на поддельные страницы входа в Google. В качестве примера приводится “washington post[.]press”, где буква "q" заменяет букву "g" в слове "Вашингтон".

📌 **Преследование конкретных лиц:** В 2023 году APT42, как сообщается, выдал себя за старшего научного сотрудника британского аналитического центра Royal United Services Institute (RUSI), пытаясь распространить вредоносное ПО среди экспертов по ядерной безопасности в базирующемся в США аналитическом центре, специализирующемся на международных делах.

📌 **Атаки в облачной среде:** В период с 2022 по 2023 год было замечено, что APT42 осуществлял утечку документов и конфиденциальной информации из общедоступной облачной инфраструктуры жертв, такой как среда Microsoft 365. Эти атаки были нацелены на юридические компании и некоммерческие организации в США и Великобритании.

📌 **Пересечение с другими операциями:** деятельность APT42 совпадает с другими операциями, связанными с Ираном: TA453, Charming Kitten и Mint Sandstorm

Предполагаемые хакеры из Китая используют вредоносную платформу "Cuttlefish" для атаки на Турцию

📌 **Идентификация вредоносного ПО и его активность:** Вредоносное ПО, идентифицированное как Cuttlefish, было активно как минимум с 27 июля 2023 года, а последняя кампания проводилась с октября 2023 по апрель 2024 года. Вирус предназначен для проникновения в маршрутизаторы и другое сетевое оборудование с целью незаметной кражи информации.

📌 **Географическая направленность и жертвы:** Кампания в основном затронула Турцию, где 99% случаев заражения происходит внутри страны. Среди остальных жертв - глобальные операторы спутниковой связи и, возможно, центр обработки данных, расположенный в США.

📌 **Связь с китайскими операциями:** Исследователи из Black Lotus Labs предполагают наличие связи между Cuttlefish и китайским правительством из-за значительного совпадения с другой вредоносной программой под названием HiatusRat, которая использовалась в операциях, отвечающих интересам Китая.

📌 **Принцип работы:** Cuttlefish собирает данные о пользователях и устройствах, находящихся за пределами целевой сети, что позволяет хакерам отслеживать весь трафик, проходящий через скомпрометированные устройства. Программа предназначена для маршрутизаторов корпоративного уровня для малого и домашнего офиса (SOHO).

📌 **Кража данных:** Вредоносная программа настроена на кражу ключей для облачных сервисов, таких как Alicloud, AWS, Digital Ocean, CloudFlare и BitBucket. Это позволяет злоумышленникам получать доступ к данным из облачных ресурсов, которые, как правило, менее защищены, чем традиционные сетевые периметры.

📌 **Проблемы обнаружения:** Характер атаки, осуществляемой через надёжную внутреннюю сеть, делает её особенно трудной для обнаружения. Многие средства обеспечения безопасности сосредоточены на внешних угрозах, тем самым потенциально упуская из виду такие действия, возникающие внутри компании.

📌 **Последствия:** освещается меняющийся ландшафт угроз, в котором методы пассивного подслушивания и перехвата данных становятся все более изощренными. Растущая проблема, связанная с использованием облачных средств аутентификации, требует усиления мер безопасности.

Больше материалов: Boosty | Sponsr | TG

Экспорт шпионских программ в Индонезию

Возможности программ-шпионов:

📌Операции со шпионскими программами можно разделить на национальные операции, проводимые собственными силами, и коммерческие программы-шпионы, продаваемые с целью получения прибыли правительству и частным клиентам.

📌Коммерческие программы-шпионы предоставляют правительствам передовые инструменты наблюдения, позволяющие им приобретать возможности, которые в противном случае были бы недоступны.

📌 Мировая индустрия шпионского ПО и цифровой криминалистики переживает бурный рост: по состоянию на 2020 год по меньшей мере 65 правительств, как авторитарных, так и демократических, заключили контракты с коммерческими поставщиками шпионского ПО.

📌Шпионское ПО может использоваться для получения конфиденциальных данных, таких как полные имена клиентов, номера телефонов, адреса, служебная документация, номера счетов, номера карт, истории транзакций, контракты и пароли

Подробности получения:

📌За большинством наблюдаемых кампаний, нацеленных на различные отрасли промышленности Индонезии, стоят спонсируемые государством террористические организации из Китая, России и Северной Кореи.

📌В мае 2023 года группа программ-вымогателей LockBit успешно взломала Bank Syariah Indonesia (BSI), дочернюю компанию государственного предприятия Bank Mandiri, в результате чего было получено 1,5 терабайта данных.

📌В мировом ассортименте коммерческого шпионского ПО наблюдается переход от старых поставщиков, таких как FinFisher и Hacking Team, к новым разработчикам, таким как NSO Group, Cytrox и Candiru.

📌Спрос на шпионские технологии остаётся высоким, а лидерами рынка являются государственные заказчики и частные компании.

Ход расследования:

📌Европейский парламент создал следственный комитет для расследования использования Pegasus и аналогичных программ-шпионов для слежки.

📌 В ходе расследования выяснилось, что по меньшей мере правительства 70 стран по всему миру стали объектами коммерческого шпионского ПО, в том числе более 180 журналистов были идентифицированы в качестве мишеней.

📌Расследование также показало, что на Кипре активно ведется деятельность в сфере слежки с участием тех же участников, которые фигурируют в скандале со шпионскими программами.

📌 Расследование по факту взлома индонезийских правительственных сетей китайской компанией Mustang Panda продолжается, и власти предпринимают шаги по выявлению и очистке зараженных систем. Однако, по состоянию на последнее обновление, хосты в индонезийских правительственных сетях все ещё взаимодействовали с серверами вредоносного ПО Mustang Panda

Архитектура NES консолей

Похоже, вы променяли захватывающий социальный мир на увлекательную область исследований игровых консолей? Что ж, давайте погрузимся в глубины вашей новообретённой одержимости под названием Super Nintendo Entertainment System (SNES).

Фабьен Англар, наш герой, тщательно проанализировал SNES, предложив нам трилогию статей, которые вполне могли бы заменить любое человеческое общение.

Во-первых, статья расскажет о картриджах для SNES, этих волшебных пластиковых блоках, которые, как ни странно, были не просто мечтой детей 90-х. Они были настоящим технологическим чудом со своим собственным оборудованием, включая такой необходимый чип для защиты от копирования CIC, который не мешал копировать и модифицировать игры направо и налево.

Затем автор отправит в историческое путешествие эволюции материнской платы SNES. За двенадцать лет было выпущено двенадцать версий, в каждой из которых количество чипов и компонентов сокращалось. Технологическое разнообразие

И давайте не будем забывать трогательную историю о тактовых генераторах SNES. Эти маленькие хронометристы позаботились о том, чтобы все работало как часы (каламбур вполне уместен). Ведь что такое игровая консоль без обеспечивающего точность ускоренных запусков инструментов?

Итак, вот она, трилогия статей, которая вполне может заменить общение между людьми. Кому нужны друзья, когда у вас есть сложные детали SNES, которые согреют вас ночью? Спасибо тебе, Фабьен Санглар, за то, что дал нам прекрасный повод отказаться от социальных обязательств в пользу исследований игровых консолей.

SNES картриджи:

Картриджи SNES были уникальны тем, что они могли включать в себя дополнительное оборудование, такое как чип защиты от копирования CIC, SRAM и процессоры повышения производительности, такие как «Super Accelerator 1» (SA-1). Эти процессоры значительно расширили возможности консоли, обеспечив улучшенную графику и игровой процесс. В нем рассказывается об эволюционных шагах, предпринятых Nintendo с материнской платой SNES для повышения эффективности и экономичности системы с течением времени.

Ключевые функции

📌 Материнская плата SNES претерпевала значительные изменения на протяжении всего производства, в первую очередь направленные на снижение сложности и стоимости системы.

📌 Изначально материнская плата содержала большое количество микросхем и компонентов, которые постепенно сокращались в более поздних версиях.

Уменьшение количества микросхем

📌 Одним из главных достижений в разработке материнской платы SNES стало появление 1-CHIP версии. Эта версия объединила центральный процессор и два PPU (блока обработки изображений) в единую ASIC (специализированную интегральную схему), сократив общее количество микросхем на материнской плате до девяти.

📌 Это сокращение не только упростило конструкцию, но и потенциально повысило надёжность и производительность системы.

Версии материнских плат

📌 За 12 лет существования Nintendo выпустила двенадцать различных версий материнской платы для SNES.

📌 Эти версии включают в себя различные модели, такие как SHVC-CPU-01, SNS-CPU-GPM-01 и SNS-CPU-1CHIP-01, каждая из которых соответствует различным годам выпуска и особенностям дизайна.

📌 Версии разделены на четыре основных поколения: Classic, APU, 1-CHIP и Junior, причём 1-CHIP и младшие версии представляют собой наиболее значительные изменения в дизайне.

📌 Super Nintendo Jr (также известная как Mini) является окончательной версией SNES, в ней сохранено меньшее количество микросхем и более интегрированный дизайн, в котором на материнской плате больше нет частей, предназначенных для конкретных подсистем.

Эволюция материнской платы SNES:

За 12 лет своего существования Nintendo выпустила двенадцать версий материнской платы SNES, в каждой из которых количество чипов и компонентов было сокращено. Наиболее заметным достижением стала версия 1-CHIP, которая объединила центральный процессор и два блока питания в единый ASIC, упростив конструкцию и потенциально повысив производительность. Это проливает свет на технические чудеса и проблемы системы картриджей SNES, подчёркивая, как Nintendo использовала дополнительное оборудование в картриджах, чтобы расширить границы того, что было возможно в видеоиграх в ту эпоху

Усовершенствованные процессоры

📌 Картриджи SNES отличались способностью включать в себя не только игровые инструкции и ресурсы. Они также могли содержать дополнительные аппаратные компоненты, такие как микросхема защиты от копирования CIC, SRAM и процессоры повышения производительности.

📌 Эти усовершенствованные процессоры, такие как чип «Super Accelerator 1» (SA-1), значительно расширили возможности SNES. Чипом SA-1, который был найден в 34 картриджах, был процессор 65C816, работающий на частоте 10,74 МГц, что в четыре раза быстрее, чем у основного процессора SNES. Он также включал 2 Кбайт оперативной памяти и встроенный CIC.

Механизм защиты от копирования

📌 В SNES использовался механизм защиты от копирования, включающий два чипа CIC, которые взаимодействовали синхронно — один в консоли, а другой в картридже. Если CIC консоли обнаруживал несанкционированную игру, она перезагружала все процессоры в системе.

📌 Некоторые игры, такие как «Super 3D Noah’s Ark», обходили эту защиту, требуя, чтобы к ним подключался официальный картридж, используя для аутентификации официальный CIC игры.

Улучшения в игре

📌 Использование усовершенствованных процессоров позволило значительно улучшить производительность игры и графику. Например, чип SA-1 позволил SNES анимировать и обнаруживать коллизии для всех 128 спрайтов, доступных в PPU, преобразовывать спрайты на лету (поворачивать/масштабировать) и записывать их обратно в видеопамять (PPU VRAM).

📌 Ещё один усовершенствованный чип, Super-GFX, отлично справлялся с рендерингом пикселей и растеризацией полигонов, как правило, рендерингом в кадровый буфер, расположенный на картридже. Затем это содержимое переносилось в видеопамять в процессе VSYNC.

Региональная совместимость и возможность обхода

📌 В статье также рассматриваются меры, которые Nintendo использовала для обеспечения региональной совместимости, такие как различные формы картриджей и система блокировки CIC. Однако в статье упоминается, что эти меры не были надёжными и их можно было обойти.

Информация о сообществе и разработках

📌 В дискуссиях на таких платформах, как Hacker News, обсуждается влияние и потенциал этих картриджей, сравниваются их с другими инновациями Nintendo и обсуждаются технические проблемы и решения, связанные с дизайном SNES

Сердце SNES:

В SNES использовались два основных тактовых генератора для управления синхронизацией различных компонентов. Эти тактовые импульсы имели решающее значение для работы центрального процессора, PPU и APU. Система также включала в себя улучшающие чипы в некоторых картриджах, которые использовали эти тактовые частоты для дополнительной вычислительной мощности, примером чего является чип SuperFX, используемый в таких играх, как StarFox. Этот подробный обзор тактовой системы SNES раскрывает сложный дизайн и инженерные разработки, которые поддерживали сложные графические и звуковые возможности консоли, обеспечивая продвинутые игровые возможности в ту эпоху.

Тактовые генераторы

📌 Материнская плата SNES оснащена двумя основными тактовыми генераторами, расположенными в разъёмах X2 и X1.

📌 В разъёме X2 расположен керамический резонатор синего цвета с частотой 24,576 МГц. Этот резонатор имеет решающее значение для работы блока обработки звука (APU), задающего скорость обработки звука на SNES.

📌 Слот X1 содержит генератор с частотой 21,300 МГц, обозначенный жёлтым цветом D21L3. Этот генератор удобно расположен рядом с центральным процессором и блоком обработки изображений (PPU), тем самым задавая темп их работы.

Микросхемы распределения тактовых импульсов и улучшения качества

📌 SNES использует эти основные тактовые импульсы в сочетании с разделителями для генерации дополнительных тактовых импульсов, необходимых различным компонентам. Например, процессор Ricoh 5A22 работает на частоте, составляющей 1/6 от основной тактовой частоты, в результате чего частота составляет 3,579545 МГц.

📌 Система включает в себя в общей сложности пятнадцать различных тактовых импульсов, что подчёркивает сложность управления синхронизацией в SNES.

📌 Линия SYS-CLK, работающая на частоте 21,47727 МГц, подключена к порту картриджа. Обычно такая настройка не требуется для основной работы картриджей, которые содержат ПЗУ с игровыми данными и инструкциями. Однако этот тактовый сигнал имеет решающее значение для картриджей, которые содержат собственные улучшающие процессоры, такие как чип SuperFX, используемый в таких играх, как StarFox.

📌 Эти усовершенствованные чипы могут использовать SYS-CLK для получения дополнительной вычислительной мощности, а некоторые чипы, такие как версия процессора SuperFX от MARIO, используют внутренний делитель для настройки тактовой частоты в соответствии с конкретными потребностями в обработке.

📌 Точность этих тактовых генераторов жизненно важна для детерминированного выполнения игрового кода, что особенно важно для таких приложений, как ускоренные запуски с помощью инструментов (TAS). Со временем точность керамических резонаторов может ухудшаться, что приводит к несоответствиям в производительности

Архитектура консолей

Серия книг Родриго Копетти «Архитектура консолей: практический анализ» погружает в увлекательный мир игровых консолей, раскрывая секреты их ошеломляющих технологий на тот момент технологий.

В своей серии автор отправляет нас в инженерное путешествие по эволюции консолей, показывая и доказывая, что они — это нечто большее, чем просто набор причудливых цифр. Эти книги, от Nintendo 3DS до серий Xbox и PlayStation, показывают, что каждая из консолей по-своему уникальна и особенна.

Итак, если вы готовы пожертвовать своей социальной жизнью ради глубокого погружения в завораживающий мир консольной архитектуры, книги Копетти — это то, что вам нужно. Это сокровищница технических знаний, идеальная для всех, кто когда-либо задавался вопросом, что заставляет эти волшебные коробки работать.

Эти книги входят в серию, посвящённую консольному архитектуре, и она структурирована аналогично другим работам посвящённым консолям PlayStation, Xbox и другим консолям. Это позволяет читателям, знакомым с архитектурами консолей, сравнить консоли бок о бок. Книги по архитектуре консолей предназначены для людей с базовыми знаниями в области вычислительной техники, которые интересуются эволюцией и внутренней работой игровых консолей. Его труды — это не руководства для разработчиков, а скорее подробное описание того, как каждая система работает внутри. Он пытается адаптировать свой контент для более широкой аудитории, чтобы даже те, кто не разбирается в компьютерных технологиях, могли найти ценность в его работе. Его книги ценятся как техническими, так и нетехническими читателями за глубокие, но доступные объяснения сложных архитектур консолей. Таким образом, его целевую аудиторию можно считать довольно широкой: от обычных читателей, интересующихся технологиями, до профессионалов игровой индустрии, компьютерных инженеров и энтузиастов консольных игр и аппаратного обеспечения.

Ещё несколько книг этого автора

📌 NES Architecture: More than a 6502 machine

📌 Game Boy Architecture

📌 Super Nintendo Architecture

📌 PlayStation Architecture

📌 Nintendo 64 Architecture

📌 GameCube Architecture

📌 Wii Architecture

📌 Nintendo DS Architecture

📌 Master System Architecture

Xbox Original

Если вы не знакомы с оригинальной версией Xbox Original, рекомендуется начать с чтения книги о консоли Xbox Original. Книга представляет собой углублённый взгляд на архитектуру консоли, уделяя особое внимание её уникальным функциям и технологическим инновациям, которые выделяют её от своих конкурентов. Книга начинается с обсуждения исторического контекста развития Xbox, отмечая, что Microsoft стремилась создать систему, которая была бы оценена по достоинству разработчиками и одобрена пользователями благодаря её знакомым возможностям и онлайн-сервисам.

📌 **Одна из основных тем, затронутых в книге, — процессор Xbox.** В консоли используется слегка модифицированная версия Intel Pentium III, популярного в то время серийного процессора для компьютеров, работающего на частоте 733 МГц. В книге исследуются последствия этого выбора и то, как он влияет на общую архитектуру Xbox.

📌 **В книге также рассматривается графика Xbox.** Он использует специальную реализацию Direct3D 8.0, которая была расширена за счёт включения функций, специфичных для Xbox. Это позволило разработчикам ПК портировать свои игры на Xbox с минимальными изменениями.

📌 **Экосистема разработки Xbox — ещё одна ключевая тема:** с оборудованием консоли взаимодействуют различные библиотеки и платформы. В книге представлен подробный анализ этой экосистемы, помогающий читателям разобраться в тонкостях разработки игр на Xbox.

📌 **Также обсуждается сетевая служба Xbox.** Xbox включал в себя подключение Ethernet и централизованную онлайн-инфраструктуру под названием Xbox Live, что в то время было инновационными функциями. В книге исследуется, как эти функции влияют на общую архитектуру Xbox.

📌 **Наконец, в книге также рассматриваются аспекты безопасности Xbox, включая систему борьбы с пиратством.** В нем объясняется, как работает эта система и как она вписывается в общую архитектуру консоли.

Краткая информация об оригинальной архитектуре Xbox

📌 В оригинальной Xbox использовалась привычная система для разработчиков и онлайн -сервисы для пользователей

📌 Процессор Xbox основан на Intel Pentium III с микроархитектурой P6

📌 Консоль имеет 64 Мб оперативной памяти DDR SDRAM, которая используется всеми компонентами совместно

📌 Графический процессор Xbox производится компанией Nvidia и называется NV2A

📌 Оригинальный контроллер Xbox, называемый Duke, был заменён на новую версию под названием ControllerS из-за критики

Xbox 360

Книга «Архитектура Xbox 360: Суперкомпьютер для всех нас» содержит всесторонний и серьёзный анализ архитектуры Xbox 360, в т. ч. её дизайн, возможности и технологические инновации, которые она представила, а также объясняет, как консоль работает внутри в буквальном и переносном смысле. Материал полезен для всех, кто интересуется развитием технологий игровых консолей, однако не ограничивается этой аудиторией. Книга входит в серию «Архитектура консолей: практический анализ», в которой рассматривается эволюция игровых консолей и их уникальные способы работы.

Книга начинается с краткой истории Xbox 360, которая была выпущена на год раньше её главного конкурента, PlayStation 3. В ней обсуждаются бизнес-аспекты процессора Xbox 360 и последовательность событий, которые привели к её разработке.

Затем автор углубляется в технические аспекты архитектуры Xbox 360, где обсуждается процессор консоли, который существенно отличается от одноядерного процессора, использовавшегося в оригинальной Xbox. Процессор Xbox 360, известный как Xenon, представлял собой трёхъядерный процессор, разработанный IBM. Каждое ядро могло обрабатывать два потока одновременно, что позволяло обрабатывать до шести потоков одновременно.

В книге также обсуждается графический процессор Xbox 360, известный как Xenos, который был разработан и изготовлен ATI. Графический процессор был основан на новой архитектуре и мог обеспечить производительность 240 гигафлопс. Графический процессор Xenos представил концепцию единого шейдерного конвейера, который объединил два разных выделенных конвейера для повышения производительности.

В книге далее обсуждается основная память Xbox 360, объем которой значительно увеличился по сравнению с 64 МБ оригинальной Xbox, что позволило запускать на консоли более сложные игры и приложения.

В книге также рассказывается об операционной системе Xbox 360, экосистеме разработки и сетевых службах. В нем обсуждается, как архитектура консоли была спроектирована так, чтобы быть гибкой и простой с точки зрения программирования, со сбалансированной аппаратной архитектурой, которая могла адаптироваться к различным жанрам игр и потребностям разработчиков.

К основным темам, затронутым в книге, относятся:

📌 **ЦП:** подробно рассматривается процессор Xbox, обсуждаются его уникальные особенности и его сравнение с процессорами других консолей. Им также обеспечивается исторический контекст, объясняя, как на конструкцию ЦП повлияли технологические тенденции и проблемы того времени.

📌 **Графика:** представлен подробный анализ графических возможностей Xbox, включая использование полунастраиваемой версии Direct3D 9 и то, как это повлияло на будущие версии Direct3D.

📌 **Безопасность:** обсуждается антипиратская система Xbox, объясняется, как она работает и какой вклад она вносит в общую архитектуру консоли.

📌 **Экосистема разработки:** исследуются сложности разработки игр для Xbox, обсуждает различные используемые библиотеки и платформы, а также то, как они взаимодействуют с оборудованием консоли.

📌 **Сетевая служба**: рассматриваются онлайн-возможности Xbox, обсуждается подключение Ethernet и онлайн-инфраструктура Xbox Live.

Краткие сведения об архитектуре Xbox 360

📌 Xbox 360 была выпущена на год раньше своего главного конкурента, PS3

📌 Центральный процессор Xbox 360, называемый Xenon, является многоядерным процессором, разработанным IBM

📌 В качестве графического процессора консоли используется частично адаптированная версия Direct3D 9, называемая Xenos

📌 Xbox 360 имеет унифицированную архитектуру памяти с 512 МБ оперативной памяти GDDR3

PlayStation 2

«Архитектура PlayStation 2» представляет собой углублённый анализ внутренней работы консоли PlayStation 2. Несмотря на то, что PlayStation 2 не была самой мощной консолью своего поколения, она достигла такого уровня популярности, который был немыслим для других компаний. В книге объясняется, что успех PlayStation 2 был обусловлен её Emotion Engine, мощным пакетом, разработанным Sony и работающим на частоте ~ 294,91 МГц. Этот набор микросхем содержал несколько компонентов, включая основной процессор и другие компоненты, предназначенные для ускорения определённых задач. В книге также обсуждается операционная система PlayStation 2, в которой для воспроизведения DVD и сжатия текстур высокого разрешения использовался блок обработки изображений (IPU). Также рассматривается экосистема разработки PlayStation 2: Sony предоставляет аппаратное и программное обеспечение для помощи в разработке игр.

Краткая информация об архитектуре PS2

📌 PlayStation 2 (PS2) была не самой мощной консолью своего поколения, но завоевала огромную популярность

📌 Сердцем PS2 является процессор Emotion Engine (EE), работающий на частоте ~ 294,91 МГц и содержащий множество компонентов, включая основной процессор

📌 Основным ядром является процессор, совместимый с MIPS R5900, с различными усовершенствованиями

📌 В PS2 используются модули VPU для расширения возможностей обработки данных

📌 Консоль имеет обратную совместимость с оригинальной PlayStation благодаря использованию процессора ввода-вывода (IOP).

📌 В PS2 был представлен контроллер DualShock 2, оснащённый двумя аналоговыми джойстиками и двумя вибромоторами

📌 Операционная система PS2 хранится на чипе ROM объёмом 4 МБ

PlayStation 3

«Архитектура PlayStation 3» предлагает всесторонний анализ внутренней структуры консоли PlayStation 3. В книге объясняется, что базовая аппаратная архитектура PlayStation 3 продолжает идеи Emotion Engine, фокусируясь на векторной обработке для достижения мощности, даже ценой сложности. Процессор PlayStation 3, Cell Broadband Engine, является продуктом кризиса инноваций и должен был идти в ногу с развитием тенденций в сфере мультимедийных услуг. В книге также обсуждается основная память PlayStation 3 и элемент синергетического процессора (SPE), которые представляют собой ускорители, включённые в ячейку PS3. PlayStation 3 также содержит чип графического процессора производства Nvidia под названием Reality Synthesizer или RSX, который работает на частоте 500 МГц и предназначен для разгрузки части графического конвейера.

Краткая информация об архитектуре PS3

📌 В PS3 основное внимание уделяется векторной обработке данных, что позволяет добиться высокой производительности даже ценой сложности

📌 Основным процессором PS3 является Cell Broadband Engine, разработанный совместно Sony, IBM и Toshiba

📌 Центральный процессор PS3 чрезвычайно сложен и оснащен мощным процессорным элементом (PPE) и несколькими синергетическими процессорными элементами (SPE)

📌 В PS3 используется графический процессор Reality Synthesizer (RSX) производства Nvidia

В книгах обсуждаются несколько заметных различий в архитектурах.

Xbox 360 и Xbox Original

📌 **Процессор:** оригинальный Xbox опирался на популярный стандартный процессор (Intel Pentium III) с небольшими изменениями. Это был одноядерный процессор с векторизованными инструкциями и сложной конструкцией кэша. С другой стороны, Xbox 360 представил новый тип процессора, не похожий ни на что, что можно было увидеть на полках магазинов. Это был многоядерный процессор, разработанный IBM, отражающий навязчивую потребность в инновациях, характерную для консолей 7-го поколения.

📌 **Графический процессор:** оригинальный графический процессор Xbox был основан на архитектуре NV20 с некоторыми модификациями для работы в среде унифицированной архитектуры памяти (UMA). Однако Xbox 360 использовал полунастраиваемую версию Direct3D 9 для своего графического процессора под названием Xenos.

📌 **Память:** оригинальный Xbox имел в общей сложности 64 МБ памяти DDR SDRAM, которая использовалась всеми компонентами системы. С другой стороны, Xbox 360 имел унифицированную архитектуру памяти с 512 МБ оперативной памяти GDDR3.

📌 **Экосистема разработки:** оригинальный Xbox был разработан с учётом особенностей, которые ценятся разработчиками, и онлайн-сервисов, приветствуемых пользователями. Однако Xbox 360 был разработан с упором на новый «многоядерный» процессор и нестандартный симбиоз между компонентами, что позволило инженерам решать неразрешимые проблемы с помощью экономически эффективных решений.

📌 **Сроки выпуска:** Xbox 360 была выпущена на год раньше своего главного конкурента, PlayStation 3, и уже заявляла о технологическом превосходстве над ещё не выпущенной PlayStation 3.

PS2 и PS3:

📌 **Процессор:** Emotion Engine для PS2 был разработан Toshiba с использованием технологии MIPS и ориентирован на достижение приемлемой производительности в 3D при меньших затратах. Напротив, процессор PS3, Cell Broadband Engine, был разработан в результате сотрудничества Sony, IBM и Toshiba и представляет собой очень сложный и инновационный процессор, который сочетает в себе сложные потребности и необычные решения.

📌 **Графический процессор:** Графический синтезатор PS2 представлял собой графический процессор с фиксированной функциональностью, предназначенный для работы в 3D. Графический процессор PS3, Reality Synthesizer (RSX), был произведён Nvidia и был разработан для разгрузки части графического конвейера, предлагая лучшие возможности параллельной обработки.

📌 **Память:** PS2 имела 32 МБ RDRAM, а PS3 имела более продвинутую систему памяти: 256 МБ XDR DRAM для ЦП и 256 МБ GDDR3 RAM для графического процессора.

📌 **Экосистема разработки:** Экосистема разработки PS2 была основана на технологии MIPS и ориентирована на достижение приемлемой производительности 3D при меньших затратах. Экосистема разработки PS3 была более сложной и включала сотрудничество между Sony, IBM и Toshiba и была сосредоточена на создании мощной и инновационной системы.

📌 **Обратная совместимость:** PS2 была обратно совместима с играми для PS1 благодаря включению оригинального процессора PS1 и дополнительных аппаратных компонентов. PS3 также предлагала обратную совместимость с играми для PS2, но в более поздних версиях консоли это было достигнуто за счёт программной эмуляции.

PS2 и Xbox Original:

📌 **Процессор:** Emotion Engine для PS2 был разработан Toshiba с использованием технологии MIPS и ориентирован на достижение приемлемой производительности в 3D при меньших затратах. Напротив, процессор Xbox Original был основан на процессоре Intel Pentium III, который был популярным серийным процессором с небольшими изменениями.

📌 **Графический процессор:** Графический синтезатор PS2 представлял собой графический процессор с фиксированной функциональностью, предназначенный для работы в 3D. Графический процессор Xbox Original был основан на архитектуре NV20 с некоторыми модификациями для работы в среде унифицированной архитектуры памяти (UMA).

📌 **Память:** PS2 имела 32 МБ RDRAM, а Xbox Original включала в общей сложности 64 МБ DDR SDRAM, которая использовалась всеми компонентами системы.

📌 **Экосистема разработки:** Экосистема разработки PS2 была основана на технологии MIPS и ориентирована на достижение приемлемой производительности 3D при меньших затратах. Xbox Original был разработан с учётом особенностей, которые ценят разработчики, и онлайн-сервисов, приветствуемых пользователями.

PS3 и Xbox 360:

📌 **ЦП:** ЦП PS3, Cell Broadband Engine, представляет собой очень сложный и инновационный процессор, который сочетает в себе сложные потребности и необычные решения. Он был разработан в результате сотрудничества Sony, IBM и Toshiba. С другой стороны, процессор Xenon для Xbox 360 представлял собой процессор нового типа, не похожий ни на что, что можно было увидеть на полках магазинов. Он отражает навязчивую потребность в инновациях, характерную черту той эпохи.

📌 **Графический процессор:** графический процессор PS3, синтезатор реальности или RSX, был произведён Nvidia и был разработан для разгрузки части графического конвейера. Графический процессор Xenos Xbox 360 представлял собой полунастраиваемую версию Direct3D 9, в которой есть место для дополнительных функций Xenos.

📌 **Память:** Память PS3 была распределена по разным микросхемам памяти, и, хотя она не реализовала архитектуру UMA, она все равно могла распределять графические данные по разным микросхемам памяти, если программисты решат это сделать.

📌 **Экосистема разработки**: Экосистема разработки PS3 была основана на Cell Broadband Engine, совместном проекте Sony, IBM, Toshiba и Nvidia. Экосистема разработки Xbox 360 была основана на процессоре Xenon и полунастраиваемой версии Direct3D 9.

Больше материалов: Boosty | Sponsr | TG

Содержание

Инфобез в медицине

Давайте оценим чудеса интеграции устройств Интернета вещей (IoT) в здравоохранение. Что может пойти не так с подключением всех мыслимых медицинских устройств к Интернету? Кардиостимуляторы, аппараты магнитно-резонансной томографии, умные инфузионные насосы - все устройства просят: "Взломайте нас, пожалуйста!"

Погружаясь в пучину угроз кибербезопасности, не будем забывать о том, как замечательно, что ритм вашего сердца зависит от чего-то такого стабильного и безопасного, как Интернет. И кто мог бы не порадоваться тому, что ваши медицинские данные хранятся в облаке и вот-вот станут достоянием общественности? Соблюдение индустриальных требований и практик волшебным образом предотвратят все кибер-угрозы. Потому что хакеры полностью соблюдают правила, и их определённо отпугивают «лучшие намерения» медицинской организации.

Последствия кибератаки на медицинские технологии сказываются не только на поставщиках медицинских услуг, но и на страховых компаниях, фармацевтических компаниях и даже службах неотложной помощи. В больницах царит хаос, лечение откладывается, а безопасность пациентов находится под угрозой — это идеальный вариант. Но давайте не будем забывать и о невоспетых героях: компаниях, занимающихся кибербезопасностью, которые радостно потирают руки, когда спрос на их услуги стремительно растёт.

Добро пожаловать в будущее здравоохранения, где ваше медицинское устройство может стать частью очередной крупной утечки данных. Спите спокойно!

Патент CN111913833A

Ещё одно блокчейн-решение, способное решить все проблемы в сфере здравоохранения. Потому что, знаете ли, индустрии здравоохранения отчаянно не хватает таких модных словечек, как "архитектура с двумя блокчейнами" и "шифрование на основе атрибутов". Кто бы не спал спокойнее, зная, что его конфиденциальные медицинские данные хранятся не в одной, а в двух блокчейнах? Это как удвоение безопасности или удвоение головной боли, в зависимости от того, как на это посмотреть. Не будем забывать и о главном: интеграции ИИ. Что ещё может подарить ощущение "надёжности и защищённости", как использование искусственного интеллекта.

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.

Но подождите, это ещё не все! Система обещает "децентрализацию" – волшебное слово, которое, по-видимому, решает проблему несанкционированного доступа к данным. Потому что, как мы все знаем, децентрализация сделала криптовалюты, такие как биткоин, полностью защищёнными от мошенничества и кражи. Или наоборот...

Если говорить серьёзно, патент CN111913833A действительно направлен на решение реальных проблем в секторе здравоохранения, таких как утечка данных и отсутствие стандартизированных протоколов для безопасного обмена данными. Однако нельзя не относиться к нему со здоровой долей скептицизма. В конце концов, если история и научила нас чему-то, так это тому, что технология хороша настолько, насколько хороша её реализация и люди, стоящие за ней. Итак, будем надеяться, что эта система транзакций на основе блокчейна для медицинского Интернета вещей - нечто большее, чем просто ещё один победитель лотереи модных слов.

Патент US11483343B2

Патент US11483343B2 смело заявляет, что произведёт революцию в борьбе со старейшей проблемой – фишингом, чтобы всех спасти от ссылок, скрывающихся в почтовых ящиках. Патент представляет новаторскую архитектуру, предназначенную для обнаружения попыток фишинга путём сканирования сообщений на наличие подозрительных URL-адресов.

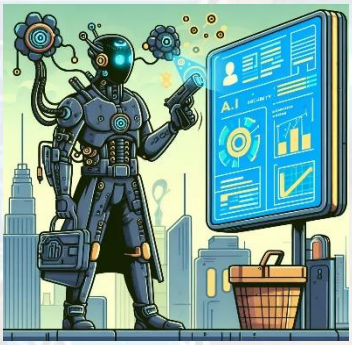
Многоступенчатая система обнаружения фишинга не только сканирует сообщения, но и разрешает URL-адреса, извлекает функции веб-страниц и использует машинное обучение, чтобы отличать легитимный объект от фишингового. Решение настолько продвинутое, что заставляет задуматься, как нам вообще удавалось выжить в Интернете без него. Несмотря на то, что компания смело выходит на поле битвы в сфере кибербезопасности, нельзя не задуматься о проблемах производительности и точности, которые ждут нас впереди в постоянно меняющейся среде фишинга

Больше материалов: Boosty | Sponsr | TG

Патент US11496512B2

Давайте погрузимся в захватывающий мир патентов, а конкретно шедевра патента компании Lookout, Inc., "Обнаружение фишинга в реальном времени с помощью фишингового клиента или сервера безопасности", потому что, кибер-мир отчаянно ждал ещё одного патента, который спас бы от тисков фишинговых атак.

В мире, изобилующем решениями для обеспечения кибербезопасности, отважные изобретатели разработали новаторский метод: вставлять на веб-страницы закодированное значение отслеживания (ETV). Этот революционный метод обещает оградить от самых незначительных неудобств, связанных с фишинговыми атаками, благодаря отслеживанию каждого нашего шага в режиме онлайн. Слежка в обмен на защиту от фишинга внушает доверие.



Databricks AI Security Framework (DASF)

Фреймворк Databricks AI Security (DASF) дарит нам грандиозную иллюзию контроля над системами искусственного интеллекта на диком западе. Это настоящий контрольный список из 53 угроз безопасности, которые вполне могут возникнуть, но только в том случае, если вам не повезёт очень сильно.

📌 **Выявление угроз безопасности:** здесь мы сделаем вид, что шокированы обнаружением уязвимостей в системах искусственного интеллекта. Мы же никогда не думали, что эти системы пуленепробиваемые, верно?

📌 **Меры контроля:** здесь мы начинаем играть в героя, реализуя те волшебные шаги, которые обещают держать ИИ-бугимена в страхе.

📌 **Модели развёртывания:** Мы рассмотрим различные способы, с помощью которых ИИ может распространиться по миру, просто чтобы не усложнить ситуацию, не зря ж авторы делали этот фреймворк.

📌 **Интеграция с существующими платформами безопасности:** поскольку изобретать велосипед стало модным только в прошлом тысячелетии, мы посмотрим, как DASF будет сочетаться с другими платформами.

📌 **Практическая реализация:** именно здесь мы засучиваем рукава и приступаем к работе, применяя платформу с таким же энтузиазмом, с каким ребёнок выполняет домашнюю работу.

Патент US11611582B2

Патент US11611582B2 предоставляет метод, который использует заранее определённую статистическую модель для обнаружения фишинговых угроз. Потому что, как вы знаете, фишинг — это настолько новая концепция, что никто раньше не задумывался о защите от него.

Этот метод, являющийся ярким примером волшебства машинного обучения, анализирует сетевые запросы в режиме реального времени. Однако это не просто анализ — это упреждающий подход! Это означает, что он на самом деле пытается остановить фишинговые атаки до того, как они произойдут, в отличие от других ленивых методов, которые просто сидят сложа руки и ждут, когда разразится катастрофа.

Когда сетевой запрос поступает в систему, он должен сначала раскрыть свои секреты — такие, как полное доменное имя, возраст домена, регистратора домена, IP-адрес и даже его географическое местоположение. Очевидно, что географическое расположение имеет решающее значение. Всем известно, что фишинговые атаки из живописных мест вызывают меньше подозрений.

Эти детали затем передаются в вечно голодную, предварительно обученную статистическую модель, которая в своей бесконечной мудрости вычисляет оценку вероятности. Этот показатель, являющийся количественной оценкой, говорит нам о вероятности того, что этот сетевой запрос на самом деле является фишинговой угрозой.

Эта статистическая модель – не какой-то статичный реликт, это живое, обучающееся создание. Она основана на наборах данных, изобилующих известными примерами фишинга и не-фишинговых атак, и периодически пополняется новыми данными, чтобы не отставать от постоянно меняющихся тенденций фишинговых атак.

Вы счастливы, что в вашем распоряжении есть такой инновационный инструмент, который неустанно защищает нашу цифровую среду от непрекращающихся атак фишинга? Что бы вы без него делали? Возможно, просто руководствовались здравым смыслом, но что в этом интересного?

Больше материалов: Boosty | Sponsr | TG

Патент US9071600B2

Патент US9071600B2 является прекрасным примером инноваций, в котором предлагается метод предотвращения фишинга и онлайн-мошенничества путём создания VPN-туннеля между компьютером пользователя и сервером. Этот патент, с его революционной идеей, гарантирует, что данные пользователя будут в безопасности. Просто удивительно, как он использует такую сложную технологию, как VPN, которая, возможно, так же стара, как и сам Интернет, для создания безопасного канала связи. Этот метод предназначен не только для защиты данных, но и для аутентификации объектов и защиты внутренних сетей от внешних угроз, чего, безусловно, мир ещё никогда не видел.

В патенте подробно описаны различные операции, такие как использование гиперссылок, веб-страниц и серверов для создания надёжной цифровой защиты. Патент заново открыл механизм онлайн-безопасности, обеспечив защиту от действий киберпреступников. Классификации, в соответствии с которыми подан этот патент, такие как протоколы сетевой безопасности для аутентификации объектов и виртуальные частные сети, являются вишенкой на торте, добавляя уровни безопасности толщиной со стены бункера.

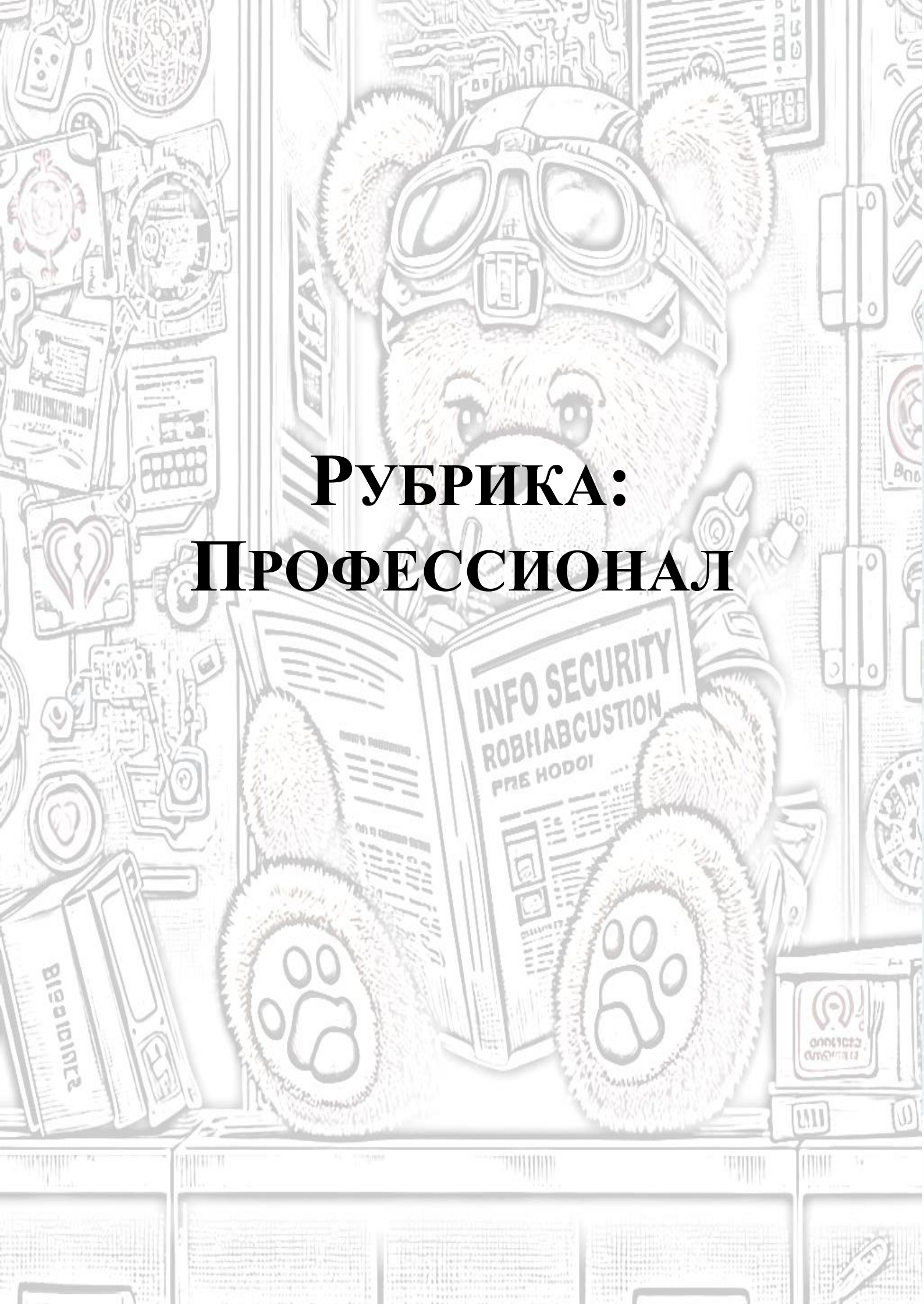
По сути, US9071600B2 — это не просто патент; это маяк надежды в мрачном мире кибер-угроз, направляющему заблудившиеся корабли в бурном море утечек данных и онлайн-мошенничества. Поистине, шедевр современных технологий, окутанный покровом VPN и протоколов сетевой безопасности!

БПЛА

Ещё одно захватывающее чтение от Министерства обороны США, появившееся в печати в августе 2023 года. "Система противодействия беспилотным летательным аппаратам (C-UAS)" - то, что нам всем нужно, – это более глубокое погружение в захватывающий мир беспилотных летательных аппаратов. Этот документ, являющийся продолжением его предшественника 2017 года, обещает стать бестселлером военной литературы, обучая солдат искусству борьбы с вражескими беспилотниками.

Он начинается с обещания просветить вооружённые силы о том, как испортить жизнь этим надоедливым беспилотным авиационным системам (БПЛА); охватывая все, от азбуки управления угрозами до способов их уничтожения в небе, это, по сути, практическое руководство по срыву миссии беспилотника - и, возможно, его KPI.

Этот документ является обязательным к прочтению для всех, кто увлечён военной стратегией, беспилотными летательными аппаратами или просто располагает большим количеством свободного времени. В нем много экшена, приключений и приложений, что делает его идеальным дополнением к книжной полке любого специалиста по безопасности или в качестве временной подпорки для дверей.



Рубрика: Профессионал

Инфобез в медицине

Аннотация – В этом документе освещаются кибер-угрозы медицинским и коммуникационным технологиям и потенциальные риски и уязвимости в связанных протоколах. Документ разработан для того, чтобы помочь организациям здравоохранения и медицинским работникам понять важность обеспечения безопасности их технологических систем для защиты данных пациентов и обеспечения непрерывности оказания медицинской помощи.

A. Введение

Интеграция устройств Интернета вещей (IoT) в секторах здравоохранения и общественного здоровья привела к значительному прогрессу в уходе за пациентами. Однако эти преимущества сопряжены с рядом проблем и угроз кибербезопасности, которые необходимо устранить для защиты конфиденциальной медицинской информации и обеспечения непрерывности предоставления медицинских услуг. Ниже представлен обзор угроз кибербезопасности в этих секторах с уделением особого внимания таким устройствам, как кардиостимуляторы, интеллектуальные инфузионные насосы, аппараты магнитно-резонансной томографии, а также более широким последствиям для медицинских технологий и протоколов связи.

Безопасность цифровых технологий в здравоохранении и секторе общественного здравоохранения имеет первостепенное значение для обеспечения защиты пациентов, конфиденциальности и целостности медицинских услуг. Организации здравоохранения должны применять комплексный подход к обеспечению безопасности данных, сети и устройств, внедряя шифрование, защищённые протоколы связи и надёжные меры безопасности. Соблюдение правил HIPAA и соблюдение передовых практик и стандартов, например CISA, HHS и DICOM, необходимы для смягчения последствий кибер-угроз и обеспечения безопасного использования цифровых технологий в здравоохранении

B. Отрасли

Кибератаки на медицинские технологии могут затронуть широкий спектр отраслей, выходящих за рамки непосредственного сектора здравоохранения:

- **Поставщики медицинских услуг**: больницы, поликлиники и частные клиники полагаются на медицинские технологии при оказании помощи пациентам. Кибератаки могут сорвать операции, задержать лечение и поставить под угрозу безопасность пациентов.
- **Технологические компании в области здравоохранения**: фирмы, разрабатывающие и поддерживающие медицинское программное обеспечение и устройства, могут пострадать от кражи интеллектуальной собственности, потери доверия клиентов и финансов.
- **Страховые компании**: страховщики могут столкнуться с исками, связанными с кибератаками на медицинские технологии, включая расходы, связанные с утечкой данных, восстановлением системы и требованиями об ответственности.
- **Фармацевтика и биотехнологии**: эти отрасли полагаются на медицинские данные для проведения исследований и разработок. Кибератаки могут привести к потере запатентованных исследовательских данных и нарушить цепочку поставок важнейших лекарств.
- **ИТ-услуги здравоохранения**: компании, предоставляющие ИТ-поддержку и услуги организациям здравоохранения, могут быть косвенно затронуты кибератаками на своих клиентов, что приводит к репутационному ущербу и финансовым потерям.
- **Правительство и регулирующие органы**: государственным учреждениям здравоохранения и регулирующим органам, потребуется реагировать на кибератаки на медицинские технологии, влияющие на общественное здравоохранение и потенциально ведущие к изменениям в законодательстве.
- **Службы неотложной помощи**: кибератаки, нарушающие работу медицинских технологий, могут привести к задержкам в реагировании на чрезвычайные ситуации и переводе пациентов, что скажется на службах скорой и неотложной медицинской помощи.
- **Юридические услуги и комплаенс-услуги**: юридические фирмы и комплаенс-консультанты могут столкнуться с ростом спроса на услуги по мере того, как организации здравоохранения будут прорабатывать правовые последствия кибератак.
- **Фирмы по обеспечению кибербезопасности**: увеличение спроса на услуги кибербезопасности от организаций здравоохранения, стремящихся к защите от будущих инцидентов.
- **Пациенты и общественность**: пациенты могут столкнуться с нарушениями в обслуживании, неприкосновенности частной жизни и потерей доверия к системе здравоохранения.

C. *Общие уязвимости и угрозы*

Сектор здравоохранения всё больше полагается на цифровые технологии для управления информацией о пациентах, медицинских процедурах и коммуникациях. Эта цифровая трансформация, несмотря на свои преимущества, создаёт значительные риски для безопасности, включая утечку данных, несанкционированный доступ и кибератаки, которые могут поставить под угрозу безопасность пациентов, конфиденциальность и целостность медицинских услуг.

Распространённые кибер-угрозы медицинским технологиям и протоколам коммуникационных технологий включают нарушение работы, деградацию и уничтожение устройств, отравление данными, кражу личных и проприетарных данных, несанкционированный доступ к медицинскому программному обеспечению. Эти угрозы усугубляются расширением ИТ-среды в здравоохранении, использованием медицинских устройств с поддержкой искусственного интеллекта (ИИ) и машинного обучения (ML), а также растущей зависимостью от беспроводной связи, включая 5G.

Медицинские устройства, такие как кардиостимуляторы, интеллектуальные инфузионные насосы и аппараты магнитно-резонансной томографии, могут быть уязвимы к кибер-инцидентам из-за отсутствия протоколов шифрования данных, плохой сегментации сети и не устранённых уязвимостей. Кроме того, медицинскому программному обеспечению, такому как DICOM и PACS, может не хватать надлежащей проверки входных данных, так как они передаются открытым текстом. Также использование некачественные крипто-алгоритмы, что делает их уязвимыми для несанкционированного доступа и модификации данных.

1) *Интеллектуальные инфузионные насосы*

Эти устройства подключаются к внутренним сетям больницы через Wi-Fi или Ethernet и передают состояние, оповещения и аварийные сигналы на центральные станции мониторинга / управления, а также данные в электронные медицинские карты (EHR).

2) *Аппараты МРТ*

Аппараты МРТ могут быть подключены к внутренней сети больницы, а снимки могут кодироваться и отправляться в программное обеспечение для архивирования изображений и системы связи (PACS) через систему цифровой визуализации и коммуникаций в медицине (DICOM). Изображения PACS могут храниться локально и быть доступными в веб-сервисе EHR, потенциально предоставляя врачам несанкционированный доступ к сетевым устройствам, включая компьютеры.

3) *Кардиостимуляторы*

Кардиостимуляторы и другие электронные устройства, имплантируемые в сердце (CIED), эволюционировали и теперь включают беспроводное подключение для мониторинга и программирования. Такое подключение, хотя и полезно для ухода за пациентами, создаёт уязвимости. Кибератаки потенциально могут привести к неисправности устройства или несанкционированному доступу к данным пациента, что представляет значительный риск для здоровья

4) *Устройства Интернета вещей*

Многие устройства Интернета вещей в здравоохранении не имеют надёжных средств контроля безопасности, что делает их уязвимыми для несанкционированного доступа и утечки данных, например ввиду проблем с шифрованием данных, их передачей в открытом виде и небезопасным хранением паролей.

5) *Сторонние поставщики*

Устройства и программное обеспечение, предоставляемые сторонними поставщиками, могут вносить уязвимости в сети здравоохранения, предоставляя бэкдор для кибератак.

6) *Медицинское программное обеспечение*

В таких программах, как DICOM и PACS, может отсутствовать надлежащая проверка входных данных и использоваться небезопасные протоколы связи, что увеличивает риск несанкционированного доступа и манипулирования данными.

7) *Радиочастотные помехи*

Радиочастотные помехи могут нарушать связь между устройствами, приводя к потере или неправильной обработке данных, что может иметь прямые последствия для ухода за пациентами.

8) *Подключение к сети 5G*

Внедрение технологии 5G в здравоохранении создаёт новые уязвимости из-за расширения возможностей для атак и потенциальных рисков в цепочке поставок.

D. *Риски*

Устранение рисков требует комплексного подхода к обеспечению безопасности данных, сети и устройств.

1) *Безопасность данных*

Безопасность данных в здравоохранении предполагает защиту конфиденциальной информации о пациентах от несанкционированного доступа, разглашения и кражи. Специальные законодательные решения, например HIPAA, устанавливает стандарт защиты данных пациентов, требующий шифрования электронной защищённой медицинской информации (ePHI), уникальной идентификации пользователя и журналов аудита для мониторинга доступа и использования PHI. Шифрование — это важнейшая технология защиты данных во время передачи, использования и хранения, гарантирующая, что данные не будут прочитаны посторонними лицами. Кроме того, принятие безопасных протоколов связи, таких как те, которые описаны DICOM, имеет важное значение для сохранения конфиденциальности и целостности информации о пациенте.

2) *Сетевая безопасность*

Сетевая безопасность в секторе здравоохранения предполагает защиту инфраструктуры, поддерживающей передачу и хранение медицинских данных. Это включает в себя обеспечение безопасности беспроводных сетей, внедрение брандмауэров и использование виртуальных

частных сетей (VPN) для шифрования передаваемых данных. Агентство по кибербезопасности и инфраструктурной безопасности (CISA) предоставляет ресурсы и передовой опыт для укрепления сетевой защиты и смягчения кибер-угроз. Организации здравоохранения также должны убедиться, что их меры сетевой безопасности соответствуют правилам HIPAA и другим соответствующим стандартам.

3) Безопасность устройства

Безопасность устройств направлена на защиту медицинских и мобильных устройств, используемых в медицинских учреждениях, от кибер-угроз. Это включает внедрение надёжных механизмов аутентификации, шифрование данных, хранящихся на устройствах, и регулярное обновление программного обеспечения для устранения уязвимостей в системе безопасности. Растущее использование устройств Интернета медицинских вещей (IoMT) создаёт дополнительные проблемы безопасности, требуя от организаций здравоохранения принятия комплексных мер для защиты этих устройств от взлома и несанкционированного доступа

E. Последствия атак

Последствия кибератаки на медицинские технологии могут быть серьёзными и широкомасштабными, затрагивая пациентов, организации здравоохранения и производителей медицинского оборудования.

- **Нарушение безопасности**: кибератаки на медицинские устройства могут привести к сбоям в работе, деградации или разрушению этих устройств, потенциально подвергая опасности здоровье и жизни пациентов.
- **Потеря конфиденциальных данных**: хакеры могут украсть или раскрыть конфиденциальные данные пациентов, включая личную информацию, записи о лечении и финансовые отчёты, что приведёт к нарушению конфиденциальности и потенциальной краже личных данных.
- **Финансовые и юридические штрафы**: организации здравоохранения могут столкнуться со значительными штрафами, юридическими последствиями и санкциями за неспособность обеспечить надлежащую защиту данных пациентов и соблюдение нормативных актов.
- **Ущерб репутации**: кибератаки могут подорвать доверие пациентов и нанести ущерб репутации организаций здравоохранения и производителей медицинского оборудования
- **Сбои в работе**: кибер-инциденты могут вызывать длительные сбои в ИТ или производстве, парализуя важнейшие службы здравоохранения и угрожая существованию пострадавших организаций.
- **Препятствие инновациям**: постоянная угроза кибератак может ограничить внедрение новых технологий и инноваций в секторе здравоохранения

1) Умные инфузионные насосы

Последствия кибератак на интеллектуальные инфузионные насосы могут быть серьёзными и потенциально опасными для жизни. Интеллектуальные инфузионные насосы — это подключённые к сети устройства, которые доставляют лекарства и жидкости пациентам. Согласно исследованию Palo Alto Networks 75% инфузионных насосов имеют недостатки в кибербезопасности, что подвергает их повышенному риску взлома хакерами

В свою очередь, это может привести к различным последствиям, в том числе:

- **Несанкционированный доступ**: хакеры могут получить несанкционированный доступ к инфузионным насосам, что потенциально позволяет им изменять способ подачи лекарств для внутривенного введения. Пациенты будут получать неправильные дозировки, которые могут быть вредными или даже смертельными.
- **Перехват незашифрованных сообщений**: некоторые инфузионные насосы передают незашифрованные сообщения, которые могут быть перехвачены хакерами, что приводит к раскрытию конфиденциальных данных пациента, таких как медицинские записи и личная информация.
- **Использование известных уязвимостей**: инфузионные насосы могут иметь известные бреши в системе безопасности, например имена пользователей и пароли остаются неизменными по сравнению с заводскими настройками устройства по умолчанию. Это может быть легко использовано хакерами, потенциально подвергая пациентов риску или раскрывая личные данные.
- **Нарушение работы служб**: нарушение работы медицинских служб приведёт к отключению программного обеспечения, потере доступа к медицинским записям и невозможности оказания надлежащей медицинской помощи. В крайних случаях медицинские учреждения могут быть вынуждены перенаправить пациентов в другие медицинские центры или отменить операции.

2) МРТ

Последствия кибератаки на аппараты МРТ многогранны и могут существенно повлиять на безопасность пациентов, целостность данных и операции здравоохранения.

- **Риски для безопасности пациентов**: кибератаки могут привести к манипуляциям с МРТ-изображениями, что потенциально может привести к неправильным диагнозам. Например, злоумышленники могут изменять изображения, чтобы удалить опухоль или ошибочно добавить её, что приведёт к ошибочному диагнозу и неправильному лечению с рисками летального исхода
- **Перебои в предоставлении медицинских услуг**: аппараты МРТ имеют решающее значение для диагностики и мониторинга различных состояний. Кибератака может вывести из строя эти машины,

что приведёт к задержкам в диагностике и лечении. В критических ситуациях даже небольшие задержки могут иметь серьёзные последствия для здоровья пациента.

- **Атаки программ-вымогателей**: аппараты МРТ, как и другие медицинские устройства, уязвимы для атак программ-вымогателей. Такие атаки могут блокировать доступ к компьютерам или шифровать изображения, требуя выкуп за восстановление доступа. Это не только нарушает работу медицинских служб, но и подвергает риску данные пациентов.
- **Раскрытие конфиденциальных данных**: Аппараты МРТ подключены к больничным сетям, что делает их потенциальными точками входа для злоумышленников, которые используют их для доступа и кражи конфиденциальных данных пациентов, включая личную и медицинскую информацию, что имеет юридические и финансовые последствия для поставщиков медицинских услуг.
- **Операционные и финансовые последствия**: восстановление после кибератаки на аппараты МРТ может быть дорогостоящим и занимать много времени. Поставщикам медицинских услуг может потребоваться замена или ремонт скомпрометированных устройств, и они могут столкнуться с потенциальными юридическими штрафами и потерей доверия со стороны пациентов.
- **Проблемы с регулированием**: строгие правила затрудняют проведение базовых обновлений на медицинских ПК, подключённых к аппаратам МРТ, усложняя усилия по защите от кибератак. Медленный процесс разработки медицинских устройств визуализации также делает их уязвимыми перед растущими кибер-угрозами

3) Кардиостимуляторы

Последствия кибератаки на кардиостимуляторы могут быть серьёзными и потенциально опасными для жизни. Уязвимости кибербезопасности в кардиостимуляторах впервые были обнаружены хакерами в 2011 году, и с тех пор они находили различные бреши в системе безопасности. В 2017 году Управление по контролю за продуктами питания и лекарствами США (FDA) отозвало имплантируемый кардиостимулятор из-за опасений, что его могут взломать

Потенциальные последствия для кардиостимуляторов включают:

- **Прямая угроза жизни пациента**: злоумышленники потенциально могут завладеть устройством, изменив функции стимуляции или нанеся неподходящий удар электрическим током, что может привести к серьёзным осложнениям для здоровья или даже смерти.
- **Разрядка аккумулятора**: определённые типы атак, например, связанные с непрерывной отправкой команд на кардиостимулятор, могут привести к быстрому разряду аккумулятора, что потребует раннего хирургического вмешательства для замены устройства, что создало бы дополнительный риск для здоровья пациента.
- **Несанкционированный доступ к личным и медицинским данным**: кардиостимуляторы могут хранить и передавать данные, касающиеся здоровья пациента и работы устройства. Кибератаки ставят под угрозу конфиденциальность этих данных, что приведёт к потенциальному неправомерному использованию личной информации.
- **Потеря доверия к медицинским устройствам**: широко распространённые сведения об уязвимостях и успешных атаках могут подорвать доверие общественности к кардиостимуляторам и другим медицинским устройствам. Эта потеря уверенности может удержать пациентов от выбора потенциально спасающих жизнь методов лечения

4) Медицинские устройства Интернета вещей

Кибератаки на медицинские устройства Интернета вещей могут иметь серьёзные последствия для ухода за пациентами, включая человеческие жертвы. Основной целью для атакующих являются устройства Интернета вещей (IoT) и Интернета медицинских вещей (IoMT), которые, в свою очередь, были основной причиной 21% всех атак программ-вымогателей в сфере здравоохранения. В топ-10 прикроватных устройств, представляющих наибольший риск для безопасности, входят инфузионные насосы, устройства VoIP, ультразвуковые аппараты, мониторы пациентов и дозаторы лекарств.

- **Риски для безопасности пациентов**: прямые угрозы жизни пациентов из-за нарушения функциональности медицинских устройств Интернета вещей, таких как кардиостимуляторы, инсулиновые помпы и аппараты искусственной вентиляции лёгких. Например, злоумышленники могут изменить настройки или функциональность устройства, что приведёт к ненадлежащему обращению или выходу из строя.
- **Утечка данных**: медицинские устройства Интернета вещей часто собирают и передают конфиденциальные данные пациентов. Кибератаки могут привести к несанкционированному доступу к этим данным, что приведёт к нарушению конфиденциальности, краже личных данных и потенциальному неправильному использованию личной медицинской информации.
- **Сбои в работе**: злоумышленники могут нарушать работу медицинских учреждений, выводя из строя устройства, что приводит к задержкам в диагностике, лечении и оказании медицинской помощи. Это будет оказывать каскадное воздействие на поток пациентов и пропускную способность больницы.
- **Финансовые затраты**: последствия могут стать значительным финансовым бременем для организаций здравоохранения, включая расходы, связанные с заменой или ремонтом устройств, реагированием на утечку данных, увеличением

страховых взносов и потенциальной юридической ответственностью.

- **Потеря доверия**: Пациенты могут не решаться использовать определённые медицинские устройства или делиться своими данными, опасаясь нарушения конфиденциальности и ставя под сомнение надёжность оказываемой им помощи.
- **Нормативно-правовые последствия**: организации здравоохранения могут столкнуться с административными штрафами за неспособность защитить данные пациентов и обеспечить безопасность медицинских устройств. Судебные иски также могут быть поданы пострадавшими пациентами или регулирующими органами.
- **Угрозы национальной безопасности**: в контексте обороны и военных операций скомпрометированные устройства Интернета вещей могут раскрывать конфиденциальную информацию, создавая риски для национальной безопасности.

5) Сторонние поставщики

Кибератаки на сторонних поставщиков в медицинском секторе могут иметь серьёзные последствия как для организаций здравоохранения, так и для пациентов, которых они обслуживают. Эти атаки представляют собой одну из самых серьёзных проблем в сфере кибер-рисков здравоохранения, поскольку больницы и системы здравоохранения подвергаются повышенному риску кибератак на третьи стороны, такие как деловые партнёры, поставщики медицинского оборудования и сторонние поставщики. Эти последствия включают:

- **Утечка данных**: сторонние поставщики часто имеют доступ к конфиденциальным данным, которые в случае взлома будут скомпрометированы, что приведёт к несанкционированному доступу к информации о пациенте.
- **Заражение вредоносными программами**: если система стороннего поставщика заражена вредоносным ПО, оно может распространиться на систему организации через этого него.
- **Атаки программ-вымогателей**: если у этих поставщиков отсутствуют надёжные меры безопасности и киберзащиты, они могут стать отправной точкой для атак программ-вымогателей.
- **Распределённые атаки типа "Отказ в обслуживании" (DDoS)**: организация может подвергаться DDoS-атакам через системы сторонних поставщиков.
- **Нарушения соответствия требованиям**: сторонние поставщики не всегда могут соблюдать те же правила, что и организации, с которыми они работают. Это может привести к нарушениям соответствия для организаций.
- **Ущерб репутации**: если сторонний поставщик будет взломан, это может нанести ущерб репутации организаций, с которыми он работает.
- **Влияние на медицинское оборудование**: кибератаки на сторонних поставщиков потенциально могут повлиять на медицинское оборудование, такое как аппараты компьютерной томографии и МРТ, которые обычно подключены к больничным сетям. Уязвимости в устаревшем программном обеспечении могут быть использованы атакующими, нарушающими работу цифровых записей пациентов и потенциально ставящими под угрозу здоровье пациентов

6) Медицинское программное обеспечение

Последствия атак на медицинское программное обеспечение выходят за рамки непосредственных финансовых потерь, создавая серьёзные риски для безопасности пациентов, целостности данных и общей эффективности оказания медицинской помощи, что подчёркивает важность приоритизации мер безопасности для защиты конфиденциальной медицинской информации и обеспечения непрерывности и качества медпомощи

- **Утечка данных**: может привести к несанкционированному доступу к конфиденциальным данным пациента, включая личную и финансовую информацию, медицинские записи и истории лечения. Это ставит под угрозу конфиденциальность пациентов и может привести к краже личных данных и финансовому мошенничеству.
- **Финансовые и юридические санкции**: организации здравоохранения могут столкнуться со значительными финансовыми потерями из-за штрафов и юридических санкций за неспособность должным образом защитить данные пациентов.
- **Проблемы с безопасностью пациентов**: могут нарушить работу медицинских служб и поставить под угрозу безопасность пациентов. Например, вмешательство в медицинские записи или диагностическое программное обеспечение может привести к неправильным диагнозам, неподходящему лечению или задержкам в оказании медицинской помощи.
- **Репутационный ущерб**: пациенты могут потерять уверенность в способности организации защитить их данные и обеспечить безопасное лечение, что нанесёт ущерб репутации организации и потенциально приведёт к потере бизнеса.
- **Снижение производительности**: может нарушить работу медицинских учреждений, что приведёт к задержкам процедур и анализов, более длительному пребыванию пациентов и общему снижению эффективности. Это приведёт к перегрузке ресурсов здравоохранения и скажется на уходе за пациентами.
- **Повышенные показатели смертности**: в некоторых случаях кибератаки были связаны с повышением показателей смертности пациентов. Задержки в процедурах, тестах и оказании медицинской помощи из-за кибератак могут иметь серьёзные последствия.

- **Ограниченные инновации**: кибератаки могут затормозить инновации в секторе ввиду расходования средств на борьбу с возникающими проблемами вследствие этих атак

7) Медицинские радиочастотные помехи

Последствия радиочастотных помех в медицинской сфере могут быть серьёзными, поскольку они способны поставить под угрозу функциональность и безопасность медицинских устройств их использующих

- **Вмешательство в функциональность устройства**: может нарушить нормальную работу медицинских устройств, потенциально приводя к неправильным показаниям или неисправностям. Это имеет серьёзные последствия для ухода за пациентами, особенно в критических ситуациях, когда необходимы точные измерения и производительность устройства.
- **Утечка данных**: радиочастотные помехи потенциально могут быть использованы для получения несанкционированного доступа к конфиденциальным данным пациента, передаваемым по каналам связи. Это может привести к утечке данных, раскрытию личной и медицинской информации и поставить под угрозу конфиденциальность пациентов.
- **Вмешательство в работу устройства**: потенциально может манипулировать радиочастотными сигналами для отправки несанкционированных команд медицинским устройствам, таким как кардиостимуляторы или инсулиновые помпы, потенциально причиняя вред пациентам. Это может включать изменение настроек устройства, введение неправильных дозировок или даже полное отключение устройств.
- **Отказ в обслуживании**: возникает ситуации, когда устройства перестают отвечать на запросы, что нарушает уход за пациентами и формирует риск, в т.ч. в ситуации оказания немедленной медпомощи.
- **Потеря доверия:** успешные атаки на радиочастотные помехи могут подорвать доверие населения к медицинским устройствам и системе здравоохранения в целом, что потенциально приведёт к нежеланию пользоваться такими устройствами или обращаться за медпомощью.

8) Подключение к сети 5G

Последствия применения 5G в медицинской сфере существенны, учитывая решающую роль 5G в улучшении связи и передачи данных в системах здравоохранения:

- **Увеличенные площади атак**: расширение сетей 5G увеличивает количество потенциальных точек входа для кибер-атакующих, усложняя защиту сети от несанкционированного доступа и утечки данных.
- **Уязвимости в устройствах Интернета вещей**: медицинские устройства (с 5G подключением) являются частью Интернета медицинских вещей (IoMT). При возникновении ИБ-инцидентов приводят к компрометации данных пациента и функциональности устройства.
- **Риски протокола туннелирования GPRS**: использование протоколов туннелирования GPRS в сетях 5G может привести к появлению уязвимостей, потенциально позволяющих перехватывать передаваемые данные и манипулировать ими.
- **Устаревшие сетевые подключения**: сети 5G, подключённые к устаревшим системам, наследуют существующие уязвимости, что используется для получения доступа к конфиденциальным медицинским данным и системам.
- **Проблемы с пропускной способностью**: более высокая пропускная способность сетей 5G может ограничить текущие возможности мониторинга безопасности, затрудняя обнаружение угроз и реагирование на них в режиме реального времени.
- **Виртуализация сетевых функций**: зависимость от программного обеспечения и виртуализации в сетях 5G создаёт новые проблемы безопасности, поскольку каждый виртуальный компонент нуждается в мониторинге и защите для предотвращения потенциальных взломов.
- **Шифрование IMSI**: слабые места в шифровании IMSI могут привести к уязвимостям в конфиденциальности идентификационных данных абонентов, потенциально позволяя осуществлять атаки по принципу "один посередине" и несанкционированное отслеживание устройств.
- **Ботнеты и DDoS-атаки**: увеличившееся количество подключённых устройств в сети 5G может быть использовано злоумышленниками для создания ботнетов или запуска распределённых атак типа "отказ в обслуживании" (DDoS)
- **Нарушение работы важнейших служб здравоохранения**: кибератаки на сети 5G нарушают связь между медицинскими устройствами и поставщиками медуслуг, что приводит к задержкам в оказании неотложной помощи и потенциально поставит под угрозу жизни пациентов.
- **Последствия для регулирования и соблюдения требований**: организации здравоохранения могут столкнуться с контролем регулирующих органов и штрафными санкциями, если они не смогут защитить данные пациентов и обеспечить безопасность своих медицинских устройств и услуг с поддержкой 5G

ПАТЕНТ CN111913833A

Аннотация – В документе представлен анализ системы транзакций медицинского Интернета вещей (IoMT), основанной на блокчейн-технологии (китайский патент CN111913833A). В ходе анализа рассматриваются различные аспекты системы, включая её архитектуру, функции безопасности, вопросы безопасности и конфиденциальности и потенциальное применение в секторе здравоохранения.

Приводится качественное изложение содержательной части патента в интересах специалистов в области безопасности и других отраслей промышленности. Этот анализ особенно полезен экспертам по кибербезопасности, инженерам DevOps, ИТ-специалистам, forensics-аналитикам и производителям медицинского оборудования для понимания последствий объединения технологии блокчейн с IoMT. Он даёт представление каким образом интеграция решает проблемы в отрасли здравоохранения, в т.ч несанкционированный доступ, утечку данных и отсутствие стандартизированного протокола для безопасного обмена данными.

A. Основная идея

Патент CN111913833A предлагает систему транзакций на основе блокчейна, специально разработанную для медицинского Интернета вещей (IoT). Эта система предназначена для решения проблем безопасности данных, конфиденциальности и функциональной совместимости в здравоохранении. Предлагаемое решение повышает безопасность и конфиденциальность данных пациентов за счёт использования двойных блокчейнов, аутентификации на основе атрибутов и интеграции искусственного интеллекта.

Основная идея патента заключается в обеспечении конфиденциальности и безопасности медицинских данных при одновременном облегчении обмена этими данными между различными заинтересованными сторонами в экосистеме здравоохранения.

Представлено несколько ключевых моментов и выводов:

- **Архитектура с двойным блокчейном**: система включает в себя две цепочки блоков: публичный блокчейн для публикации пользовательских данных и частный блокчейн для безопасного хранения медицинских данных.
- **Шифрование на основе атрибутов**: доступ к медицинским данным контролируется с помощью шифрования на основе атрибутов, которое позволяет только авторизованным пользователям с определёнными атрибутами получать доступ к данным или изменять их.
- **Конфиденциальность и безопасность**: система предназначена для повышения конфиденциальности и защищённости медицинских данных, что имеет решающее значение в отрасли здравоохранения.
- **Интероперабельность**: используя технологию блокчейн, система облегчает безопасный обмен данными между различными субъектами экосистемы здравоохранения, способствуя интероперабельности.
- **Смарт-контракты**: система использует смарт-контракты для автоматизации и обеспечения соблюдения правил доступа к данным и транзакций, уменьшая потребность в посредниках и повышая эффективность.
- **Интеграция искусственного интеллекта**: патент предполагает потенциальную интеграцию искусственного интеллекта с блокчейном для улучшения медицинских услуг в т.ч. модели прогнозирования заболеваний.
- **Мониторинг в режиме реального времени**: предлагаемая система может обеспечивать мониторинг состояния пациентов в режиме реального времени с помощью устройств Интернета вещей, предоставляя своевременные и точные данные о состоянии здоровья.
- **Децентрализация**: децентрализованный характер блокчейна обеспечивает эффективное решение для защиты от единичных сбоев и несанкционированного изменения данных.

B. Область применения

Технология обладает потенциалом улучшить способы управления медицинскими данными и их совместного использования в различных секторах индустрии здравоохранения. Ее акцент на безопасность, конфиденциальность и функциональную совместимость соответствует важнейшим потребностям этих отраслей, обещая повысить эффективность, снизить затраты и улучшить результаты лечения пациентов.

1) Здравоохранение:

Отрасль здравоохранения получит значительную выгоду от этого патента, включая больницы, диспансеры и другие медицинские учреждения, которым требуется

безопасное управление данными о пациентах и обмен ими. Предлагаемое решение может повысить безопасность и конфиденциальность медицинских данных, что имеет решающее значение для доверия пациентов и соблюдения нормативных требований. Используя блокчейн, поставщики медицинских услуг могут гарантировать неизменяемость и отслеживаемость медицинских записей

2) Медицинские устройства:

Производители и дистрибьюторы медицинских устройств Интернета вещей, таких как носимые медицинские мониторы и подключённое медицинское оборудование, непосредственно участвуют в экосистеме, о которой говорится в патенте. Система будет управлять данными, генерируемыми этими устройствами, гарантируя, что они надёжно хранятся и передаются только авторизованным сторонам. Это может улучшить мониторинг и надёжность устройств.

3) Информационные технологии в области здравоохранения:

Компании, специализирующиеся на ИТ-решениях для здравоохранения, электронных медицинских картах и системах управления медицинскими данными заинтересованы в системе повышающей потенциал безопасности данных и интероперабельности. Патент может стать новой моделью обмена медицинской информацией, сделав электронные медицинские записи более безопасными и легко доступными для обмена между различными системами здравоохранения.

4) Фармацевтические препараты:

В фармацевтической промышленности система может найти решение для безопасного обмена данными в ходе клинических испытаний и процессов разработки лекарств. Способность блокчейна обеспечивать прозрачную и неизменяемую запись транзакций может помочь в отслеживании происхождения лекарств, обеспечении их подлинности и оптимизации цепочки поставок.

5) Страхование:

Медицинские страховые компании могут использовать эту систему для безопасного доступа к данным пациентов в целях обработки претензий и предотвращения мошенничества. Неизменяемый характер записей блокчейна также может помочь страховщикам проверить точность претензий и сократить мошеннические действия.

6) Исследования и разработки:

Исследовательские учреждения, которым требуется доступ к медицинским данным для проведения исследований, могли бы воспользоваться возможностями системы безопасного и контролируемого обмена данными. Блокчейн может облегчить сотрудничество между исследователями, предоставив безопасную платформу для обмена данными при сохранении конфиденциальности пациентов.

7) Регулирующие органы:

Государственные учреждения здравоохранения и регулирующие органы могут быть заинтересованы в системе контроля за соблюдением правил конфиденциальности медицинских данных. Присущие блокчейну функции могут помочь гарантировать, что поставщики медицинских услуг и другие заинтересованные стороны придерживаются необходимых стандартов.

8) Кибербезопасность:

Компании, специализирующиеся на решениях в области кибербезопасности для отрасли здравоохранения, найдут патент актуальным в плоскости безопасности транзакций медицинских данных. Предлагаемая блокчейн-система может предложить новые способы защиты от утечек данных и кибер-угроз.

C. Предлагаемое решение

Ключевыми компонентами предлагаемого решения являются архитектура с двумя блокчейнами, шифрование на основе атрибутов для контроля доступа к данным, алгоритм консенсуса, оптимизированный для пропускной способности транзакций, контроль доступа к данным пациентов и различные функции для удалённой диагностики, обмена данными и транзакций в контексте медицинского Интернета вещей:

Архитектура с двумя блокчейнами:

- Публичный блокчейн для публикации пользовательских данных
- Частный блокчейн для безопасного хранения медицинских данных.

Шифрование на основе атрибутов (ABE):

- Доступ к медицинским данным контролируется с помощью шифрования на основе атрибутов, которое позволяет только авторизованным пользователям с определёнными атрибутами получать доступ к данным или изменять их.
- Обеспечение конфиденциальности и безопасности конфиденциальной медицинской информации.

Пропускная способность:

- Предлагается алгоритм консенсуса, основанный на доказательстве объёма транзакции для оптимизации пропускной способности.
- Решение проблемы низкой пропускной способности транзакций в существующих общедоступных решениях для обработки медицинских данных на основе блокчейна.

Контроль доступа к данным пациента:

- Пациенты имеют разрешения на управление своими медицинскими данными.
- Решение проблемы игнорирования контроля доступа к данным пациентов в текущих решениях для медицинских данных на основе блокчейна.

Функции удалённой диагностики, обмена данными и транзакций данных:

- Предоставление функций для удалённой диагностики, обмена данными и транзакции данных.
- Функции позволяют использовать различные приложения и сервисы в медицинской экосистеме Интернета вещей.

1) Архитектура с двумя блокчейнами

Предлагаемое решение использует архитектуру с двумя блокчейнами, состоящую из публичного блокчейна для публикации пользовательских данных и частного блокчейна для безопасного хранения медицинских данных. Такой подход направлен на решение проблем безопасности данных, конфиденциальности и функциональной совместимости в экосистеме медицинского ввода-вывода.

Комбинация публичных и частных блокчейнов:

- Публичный блокчейн — это блокчейн без разрешений, который позволяет любому присоединиться и участвовать в прозрачной публикации и проверке пользовательских данных.
- Частный блокчейн — это разрешённый блокчейн с ограниченным доступом для безопасного хранения конфиденциальных медицинских данных.

Дифференцированные роли и контроль доступа:

- Публичный блокчейн позволяет пользователям контролировать свои данные и обеспечивает прозрачность при публикации данных.
- Частный блокчейн обеспечивает безопасную частную среду для хранения медицинских данных и обмена ими только между авторизованными участниками.

Обеспечение баланса между прозрачностью, безопасностью и конфиденциальностью:

- Подход с двойным блокчейном направлен на использование сильных сторон блокчейнов.
- Направленность на достижение баланса между прозрачностью и децентрализацией публичных блокчейнов и повышением конфиденциальности и эффективности частных блокчейнов.

Устранение ограничений отдельных типов блокчейнов:

- Публичные блокчейны могут столкнуться с проблемами масштабируемости и конфиденциальности.
- Частные блокчейны «могут принести в жертву» некоторый уровень децентрализации и прозрачности.
- Сочетание обоих типов смягчает их индивидуальные недостатки.

Обеспечение безопасного обмена данными и совместной работы:

- Архитектура облегчает безопасный обмен медицинскими данными между уполномоченными организациями на частном блокчейне.
- Это способствует сотрудничеству между заинтересованными сторонами в сфере здравоохранения при сохранении конфиденциальности пациентов.

Повышение доверия и целостности данных:

- Неизменяемость и прозрачность публичного блокчейна помогают установить доверие ко всей системе.
- Частный блокчейн обеспечивает целостность и конфиденциальность медицинских данных.

Потенциал для повышения эффективности и эксплуатационных характеристик:

- Ограниченное участие в частном блокчейне может привести к более быстрой обработке транзакций и достижению консенсуса по сравнению с публичными блокчейнами.
- Структура с двумя блокчейнами позволяет оптимизировать систему на основе конкретных требований каждого компонента.

2) Шифрование на основе атрибутов (ABE)

ABE — это обобщение шифрования с открытым ключом, которое позволяет использовать политики контроля доступа. При традиционном шифровании с открытым ключом сообщение шифруется для конкретного получателя с использованием его открытого ключа. Напротив, ABE шифрует данные на основе атрибутов или политик, позволяя осуществлять контроль доступа на основе атрибутов, которыми обладают пользователи.

Существует два основных типа ABE:

- •**Key-Policy ABE (KP-ABE)**: в KP-ABE закрытый ключ каждого пользователя связан с политикой доступа или структурой, которая определяет, какие зашифрованные тексты может расшифровывать ключ. Зашифрованные тексты помечены наборами атрибутов.
- **Ciphertext-Policy ABE (CP-ABE)**: в CP-ABE политика доступа встроена в зашифрованный текст, и закрытый ключ каждого пользователя связан с набором атрибутов. Пользователь может расшифровать текст только в том случае, если его атрибуты удовлетворяют политике доступа.

Основные характеристики ABE:

- **Детальный контроль доступа**: ABE обеспечивает детальный контроль доступа к зашифрованным данным, позволяя определять политики доступа на основе атрибутов. Это особенно полезно в здравоохранении, где разным заинтересованным сторонам (например, врачам, медсёстрам,

исследователям) требуются разные уровни доступа к данным о пациентах.

- **Устойчивость к сговору**: схемы ABE разработаны таким образом, чтобы быть устойчивыми к атакам с целью сговора. Даже если несколько пользователей вступают в сговор и объединяют свои атрибуты, они не должны иметь возможности расшифровать текст, если хотя бы один из них по отдельности не удовлетворяет политике доступа.
- **Гибкость**: ABE позволяет создавать политики доступа и применять сложные требования к контролю доступа.
- **Отзыв атрибута**: некоторые схемы ABE поддерживают отзыв атрибута, затрагивая других пользователей, которые используют те же атрибуты. Это важно в динамичных средах, таких как здравоохранение, где роли пользователей и разрешения могут меняться с течением времени.
- **Обновление политики**: некоторые конструкции ABE допускают обновления, позволяя изменять политики доступа, связанные с зашифрованными текстами, без повторного шифрования данных. Это обеспечивает гибкость в управлении контролем доступа по мере изменения требований.
- **Отслеживаемость**: схемы ABE позволяют отследить личность пользователя, который слил свой ключ дешифрования. Это помогает поддерживать подотчётность и предотвращать несанкционированный обмен данными.

ABE в здравоохранении

ABE обладает значительным потенциалом в обеспечении безопасности медицинских данных, особенно в облачных системах электронного здравоохранения. Используя ABE, данные пациента могут быть зашифрованы с помощью детализированных политик доступа, гарантирующих, что расшифровать данные и получить к ним доступ смогут только авторизованные пользователи (например, поставщики медицинских услуг с определёнными ролями или атрибутами). Это помогает защитить конфиденциальность пациентов и соответствовать нормативным требованиям, таким как HIPAA.

Более того, такие функции, как отзыв атрибута и обновление политики, имеют решающее значение в здравоохранении, поскольку роли пользователей и требования к доступу к данным могут часто меняться. Отслеживание также важно для предотвращения утечки данных и обеспечения соответствия требованиям.

3) Алгоритм консенсуса, основанный на доказательстве объёма транзакции

В системах блокчейна консенсусные алгоритмы используются для достижения соглашения между участвующими узлами о состоянии леджеров. Они гарантируют, что все узлы имеют согласованное представление о блокчейне, и предотвращают двойные расходы или другие вредоносные действия. Однако традиционные консенсусные алгоритмы, такие как Proof-of-Work (PoW) и Proof-of-Stake (PoS), часто сталкиваются с проблемами масштабируемости, что приводит к низкой пропускной способности транзакций.

Предложенный в патенте алгоритм консенсуса, основанный на доказательстве объёма транзакций, направлен на оптимизацию их пропускной способности специально для медицинского сценария Интернета вещей.:

- **Объём транзакций как показатель**: алгоритм, использует объём или количество транзакций, обработанных узлом, в качестве показателя для определения его права создавать новые блоки. Узлам, обрабатывающим больший объём транзакций, может быть присвоен приоритет или больший вес в процессе согласования.
- **Поощрение активного участия**: основываясь на консенсусе по объёму транзакций, алгоритм стимулирует узлы к активному участию в сети и обработке транзакций. Узлы, которые вносят больший вклад в пропускную способность сети, получают более высокую вероятность создания новых блоков и получения вознаграждения.
- **Оптимизация пропускной способности**: за счёт приоритизации узлов с более высокими объёмами транзакций алгоритм направлен на оптимизацию общей пропускной способности сети. Узлам, которые могут эффективно обрабатывать транзакции, предоставляется больше возможностей для добавления новых блоков, тем самым увеличивая пропускную способность блокчейна.
- **Решение проблемы масштабируемости**: алгоритм разработан для устранения ограничений масштабируемости существующих общедоступных решений для обработки медицинских данных на основе блокчейна. Уделяя особое внимание объёму транзакций в качестве ключевого показателя, он направлен на улучшение способности сети обрабатывать большое количество транзакций, что имеет решающее значение в контексте медицинского Интернета вещей.

Ключевые особенности алгоритма консенсуса

- **Оптимизация пропускной способности**: основная цель алгоритма – оптимизировать пропускную способность транзакций, позволяя сети блокчейн эффективно обрабатывать больший объём транзакций.
- **Масштабируемость**: решая проблему низкой пропускной способности транзакций, алгоритм направлен на повышение масштабируемости блокчейн-системы, делая её пригодной для обработки крупномасштабных данных.
- **Стимулирование активного участия**: алгоритм вознаграждает узлы, которые активно участвуют в сети и обрабатывают большой объём транзакций.

Это побуждает узлы вносить свой вклад в пропускную способность сети и поддерживать здоровую экосистему.

- **Настройка для медицинского Интернета вещей**: алгоритм разработан специально для медицинской системы транзакций Интернета вещей с учётом уникальных требований и задач этой области, таких как необходимость высокоскоростной обработки больших объёмов медицинских данных.
- **Интеграция с архитектурой с двумя блокчейнами**: алгоритм консенсуса, основанный на доказательстве объёма транзакции интегрирован с архитектурой с двумя блокчейнами, предложенной в патенте, оптимизируя производительность компонентов публичного блокчейна и частного блокчейна.

4) Контроль доступа к данным пациента

Контроль доступа к данным пациентов является важнейшим компонентом предлагаемой системы транзакций медицинского Интернета вещей (IoT), основанной на блокчейне.

Система позволяет пациентам контролировать их конфиденциальную медицинскую информацию, использует шифрование на основе атрибутов и смарт-контракты для обеспечения детализированных и автоматизированных политик доступа, предоставляет проверяемые и прозрачные записи, допускает динамические изменения разрешений и интегрируется с более широкой экосистемой Интернета вещей. Такой комплексный подход к контролю доступа повышает безопасность и конфиденциальность данных пациентов.

Ключевыми функциями механизма контроля доступа к данным пациента в этой системе являются:

Контроль, ориентированный на пациента:

- Система предназначена для предоставления пациентам первичных прав контроля и управления их собственными медицинскими данными.
- Подход, ориентированный на пациента, гарантирует защиту его прав и интересов в отношении конфиденциальной медицинской информации.
- Пациенты могут решать, кто имеет доступ к их данным и при каких обстоятельствах.

Управление доступом на основе атрибутов:

- Доступ к медицинским данным контролируется с помощью шифрования на основе атрибутов (ABE).
- ABE разрешает доступ к данным или их изменение только авторизованным пользователям с определёнными атрибутами.
- Атрибуты могут относиться к роли пользователя (например, врача, медсестры, исследователя), специальности, местоположению или другим значимым факторам.
- Детализированный контроль доступа гарантирует, что конфиденциальные данные будут доступны только тем, у кого есть законная потребность и разрешение.

Автоматизация на основе интеллектуальных контрактов:

- Политики контроля доступа и разрешения закодированы в смарт-контрактах на блокчейне.
- Смарт-контракты позволяют автоматически выполнять и обеспечивать соблюдение правил доступа без ручного вмешательства.
- Автоматизация упрощает процесс контроля доступа и снижает риск несанкционированного доступа из-за человеческой ошибки или манипуляций.

Прозрачность и отслеживаемость:

- Все попытки доступа и транзакции с данными неизменно регистрируются в блокчейне.
- Это позволяет отслеживать, кто к каким данным обращался и когда.
- Прозрачность и отслеживаемость, обеспечиваемые блокчейном, помогают обеспечить соблюдение правил защиты данных и предотвращают попытки несанкционированного доступа.

Динамический и отзываемый доступ:

- Разрешения на доступ к пациенту могут предоставляться, изменяться или отзываться по мере необходимости.
- Например, пациент может предоставить временный доступ к специалисту для проведения определённого лечения, а затем отозвать этот доступ после завершения лечения.
- Гибкость позволяет системе контроля доступа адаптироваться к динамичным потребностям медицинского обслуживания при сохранении безопасности.

Интеграция с медицинской экосистемой Интернета вещей:

- Система контроля доступа интегрирована с более широкой медицинской системой транзакций Интернета вещей, предложенной в патенте.
- Это обеспечивает безопасный и контролируемый доступ к данным, генерируемым различными медицинскими устройствами Интернета вещей и носимыми устройствами.
- Авторизованные поставщики медицинских услуг могут получить доступ к этим данным Интернета вещей для удалённого мониторинга, диагностики и лечения пациентов.

D. Технологический процесс

Предлагаемое решение использует архитектуру с двумя блокчейнами: публичный блокчейн для публикации данных и частный блокчейн для безопасного хранения данных. ABE используется для детального контроля доступа, в то время как согласованный алгоритм обеспечивает эффективную проверку транзакций. Пациенты сохраняют контроль над своими данными с помощью механизмов контроля доступа. Система призвана обеспечить безопасный, эффективный и ориентированный на пациента подход к управлению медицинскими данными и обмену ими в среде Интернета вещей.

graph TD
A[Владелец данных] - Шифрует данные с помощью ABE -> B (Публичный блокчейн - блокчейн)
A - Устанавливает политики доступа -> B
B - Хранит зашифрованные данные -> C (Частный блокчейн - блокчейн)
C - Безопасное хранение медицинских данных -> D [Облачное хранилище]
E[Пользователь] -- Запрашивает доступ к данным --> F(Полномочия атрибута)
F -- Проверяет атрибуты пользователя --> F
F -- Выдаёт ключ дешифрования --> E
E - Извлекает зашифрованные данные -> D
E -- Расшифровывает данные с помощью ключа --> E
G[Согласованные узлы] - Проверка транзакций с помощью алгоритма консенсуса -> C
H[Пациент] -- Предоставляет / отменяет права доступа --> C

Настройка политики шифрования данных и доступа:

- Владелец данных (например, пациент или поставщик медицинских услуг) шифрует медицинские данные на основе атрибутов (ABE).
- Владелец данных определяет политики доступа, решающие, какие атрибуты требуются для расшифровки данных.
- Зашифрованные данные и политики доступа публикуются в общедоступной блокчейн-цепочке.

Безопасное хранение данных:

- Зашифрованные медицинские данные из блокчейна надёжно хранятся в частной блокчейне.
- Блокчейн действует как безопасный уровень хранения конфиденциальных медицинских данных с контролируемым доступом.
- Зашифрованные данные также могут храниться в облачном хранилище для обеспечения масштабируемости и доступности.

Аутентификация пользователя и выдача ключа:

- Пользователь (например, врач), который хочет получить доступ к зашифрованным данным, отправляет запрос в Центр управления атрибутами.
- Центр управления проверяет атрибуты пользователя на соответствие политикам доступа.
- Если пользователь обладает требуемыми атрибутами, Центр управления выдаёт пользователю ключ дешифрования.

Доступ к данным и их расшифровка:

- Авторизованный пользователь извлекает зашифрованные данные из блокчейна или облачного хранилища.
- Используя ключ дешифрования, полученный от Администратора атрибута, пользователь расшифровывает данные.
- Пользователь может получить доступ к открытым медицинским данным в соответствии с предоставленными правами доступа.

Проверка транзакции и достижение консенсуса:

- Узлы в сети блокчейн проверяют транзакции с использованием алгоритма консенсуса, основанного на доказательстве объёма транзакции.
- Этот механизм консенсуса оптимизирует пропускную способность транзакций и обеспечивает целостность и безопасность блокчейна.

Контроль доступа пациентов:

- Пациенты имеют контроль над своими медицинскими данными и могут предоставлять или отзывать разрешения на доступ определённым пользователям или организациям.
- Политика контроля доступа обеспечивается с помощью смарт-контрактов на блокчейне.

Дополнительные функции:

- Система поддерживает удалённую диагностику, позволяя авторизованным поставщикам медицинских услуг получать доступ к данным пациента в целях телемедицины.
- Функции обмена и транзакций обеспечивают безопасный обмен медицинскими данными между уполномоченными сторонами, такими как поставщики медицинских услуг, исследователи или страховщики.

E. Преимущества, недостатки и значимость предлагаемого решения

Предлагаемая система медицинских транзакций Интернета вещей, основанная на блокчейне, предлагает значительные преимущества с точки зрения повышения безопасности, конфиденциальности, контроля за пациентами и обмена данными. Однако она также сталкивается с ограничениями, связанными со сложностью, масштабируемостью, соблюдением нормативных требований, и зависимостью от технологии блокчейн.

Преимущества:

- **Повышенная безопасность и конфиденциальность**: архитектура с двумя блокчейнами,наряду с шифрованием на основе атрибутов (ABE) для детального контроля доступа, значительно повышает безопасность и приватность конфиденциальных медицинских данных.
- **Контроль, ориентированный на пациента**: система предоставляет пациентам разрешения на управление своими медицинскими данными, гарантируя защиту их прав и интересов.
- **Улучшенный обмен данными и совместная работа**: безопасный и эффективный обмен данными, обеспечиваемый системой, способствует сотрудничеству между заинтересованными сторонами в сфере здравоохранения при сохранении конфиденциальности пациентов.
- **Повышение доверия и целостности данных**: неизменность и прозрачность транзакций на блокчейне устанавливают доверие к системе и обеспечивают целостность данных.
- **Потенциал повышения эффективности**: алгоритм консенсуса, основанный на доказательстве объёма транзакции, направлен на оптимизацию пропускной способности транзакций, решая проблемы масштабируемости в существующих решениях.

Ограничения:

- **Сложность и проблемы с внедрением**: предлагаемая система включает в себя множество компонентов и технологий, которые могут создавать проблемы с точки зрения сложности, совместимости и внедрения организациями здравоохранения.
- **Соблюдение нормативных требований**: обеспечение соблюдения правил и стандартов конфиденциальности медицинских данных может быть сложной задачей и потребовать дополнительных мер.
- **Масштабируемость и производительность**: хотя предлагаемый согласованный алгоритм направлен на повышение пропускной способности транзакций, масштабируемость и производительность системы при обработке больших объёмов медицинских данных в реальных сценариях нуждаются в дальнейшей проверке.
- **Управление ключами и контроль доступа**: внедрение безопасного и эффективного управления ключами для ABE и управление динамическими политиками контроля доступа могут быть сложными, особенно в чрезвычайных ситуациях.
- **Зависимость от технологии блокчейн**: система в значительной степени зависит от технологии блокчейн, которая все ещё развивается и может столкнуться с проблемами, связанными с потреблением энергии, функциональной совместимостью и юридическим признанием.

Значимость:

- **Обеспечение безопасного управления медицинскими данными**: Предлагаемое решение решает важнейшие проблемы безопасности, конфиденциальности и совместного использования медицинских данных, способствуя разработке более безопасных и ориентированных на пациента систем управления медицинской информацией.
- **Стимулирование инноваций в здравоохранении**: используя передовые технологии, такие как блокчейн, ABE и IoT, патент поощряет инновации в области здравоохранения, что потенциально ведёт к улучшению ухода за пациентами, научных исследований и общей эффективности.
- **Расширение прав и возможностей пациентов**: акцент на контроле пациентами своих данных соответствует растущей тенденции развития здравоохранения, ориентированного на пациента, и может вдохновить на дальнейшие инновации в этом направлении.
- **Поощрение сотрудничества и обмена данными**: возможности системы безопасного обмена данными способствуют беспрецедентному уровню сотрудничества между поставщиками медицинских услуг, исследователями и другими заинтересованными сторонами, ускоряя прогресс в медицине.
- **Вклад в развивающийся ландшафт блокчейна в здравоохранении**: патент дополняет растущий объём исследований и инноваций, изучающих применение технологии блокчейн в секторе здравоохранения, помогая определить её будущее направление и потенциальное влияние.

1) Архитектура с двумя блокчейнами

Архитектура с двумя блокчейнами предлагает значительные преимущества в повышении безопасности, конфиденциальности, интеграции Интернета вещей, масштабируемости и контроле доступа к данным пациентов

a) Преимущества

Интеграция с устройствами Интернета вещей:

- Архитектура обеспечивает безопасный обмен медицинскими данными, собранными с различных медицинских устройств Интернета вещей и носимых устройств.
- Авторизованные поставщики медицинских услуг могут получить доступ к этим данным Интернета вещей для удалённого мониторинга, диагностики и лечения пациентов.

- Децентрализованный характер блокчейна повышает целостность и безопасность данных, генерируемых устройствами Интернета вещей.

Масштабируемость и производительность:

- Структура с двумя блокчейнами позволяет оптимизировать систему на основе конкретных требований каждого компонента блокчейна.
- Ограниченное участие в частном блокчейне может привести к более быстрой обработке транзакций и достижению консенсуса по сравнению с публичными блокчейнами.
- Методы распараллеливания могут быть использованы для увеличения пропускной способности системы и сокращения сетевого трафика.

Контроль доступа к данным пациента:

- Пациенты имеют контроль над своими медицинскими данными и могут предоставлять или отзывать разрешения на доступ определённым пользователям или организациям.
- Политика контроля доступа обеспечивается с помощью смарт-контрактов на блокчейне.
- Детальный контроль доступа осуществляется с помощью шифрования на основе атрибутов, гарантирующего доступ к данным пациента только авторизованным сторонам.

b) Ограничения:

Сложность и проблемы с внедрением:

- Архитектура с двойным блокчейном включает в себя множество компонентов и технологий, которые могут создавать проблемы с точки зрения сложности, функциональной совместимости и внедрения организациями здравоохранения.
- Интеграция системы с существующей инфраструктурой здравоохранения и обеспечение совместимости могут оказаться сложными задачами.

Соответствие нормативным требованиям:

- Обеспечение соблюдения правил и стандартов конфиденциальности медицинских данных может быть сложной задачей и потребовать дополнительных мер.
- Ориентироваться в нормативно-правовом ландшафте различных юрисдикций может быть сложно.

Ограничения на масштабируемость и производительность:

- Хотя архитектура с двумя блокчейнами направлена на повышение масштабируемости и производительности, способность системы обрабатывать большие объёмы медицинских данных в реальных сценариях нуждаётся в дальнейшей проверке.
- Механизм консенсуса и синхронизация данных по-прежнему могут сталкиваться с проблемами масштабируемости.

c) Влияние:

Повышение безопасности управления медицинскими данными:

- Архитектура с двумя блокчейнами решает важнейшие задачи в области безопасности, конфиденциальности и совместного использования медицинских данных.
- Это способствует разработке более безопасных и ориентированных на пациента систем управления медицинской информацией.

Обеспечение безопасного обмена данными и совместной работы:

- Архитектура облегчает безопасный обмен медицинскими данными между уполномоченными организациями, способствуя сотрудничеству между поставщиками медицинских услуг, исследователями и другими заинтересованными сторонами.
- Это обеспечивает беспрецедентный уровень обмена данными при сохранении конфиденциальности пациентов.

Расширение прав и возможностей пациентов:

- Предоставляя пациентам контроль над их правами доступа к медицинским данным, система расширяет возможности пациентов и соответствует тенденции развития здравоохранения, ориентированного на пациента.
- Это позволяет пациентам выборочно делиться своими данными для улучшения обслуживания и исследовательских целей.

2) Шифрование на основе атрибутов (ABE)

ABE предлагает значительные преимущества в повышении безопасности, конфиденциальности и детальном контроле доступа к медицинским данным, обеспечивая при этом их безопасный обмен и расширение прав и возможностей пациентов. Однако масштабируемость, производительность и соблюдение нормативных требований остаются ключевыми проблемами, требующими решения.

a) Преимущества:

Повышенная безопасность и конфиденциальность:

- ABE позволяет шифровать данные таким образом, что только пользователи, обладающие определёнными атрибутами, могут расшифровывать данные и получать к ним доступ, обеспечивая детальный контроль доступа

- Это позволяет пациентам хранить свои медицинские записи в зашифрованном виде и криптографически обеспечивает соблюдение политик доступа пациентов или организаций.
- ABE защищает конфиденциальную медицинскую информацию от несанкционированного доступа, повышая конфиденциальность.

Интеграция с блокчейном и Интернетом вещей:

- ABE можно эффективно комбинировать с технологией блокчейн для обеспечения безопасного и децентрализованного контроля доступа в средах Интернета вещей, включая здравоохранение.
- Это позволяет безопасно обмениваться данными, собранными с различных медицинских устройств Интернета вещей и носимых устройств, между авторизованными сторонами.
- Интеграция ABE и блокчейна обеспечивает целостность, конфиденциальность и возможность проверки данных Интернета вещей.

Детальный контроль доступа:

- ABE обеспечивает детальный контроль доступа к зашифрованным данным, позволяя определять политики доступа на основе атрибутов.
- Он поддерживает политики доступа, которые могут быть представлены в виде логических формул или древовидных структур, что позволяет применять сложные требования к контролю доступа.
- Различным заинтересованным сторонам в сфере здравоохранения, таким как врачи, медсестры и исследователи, могут быть предоставлены разные уровни доступа к данным о пациентах в зависимости от их характеристик.

b) Ограничения:

Масштабируемость и производительность:

- Схемы ABE могут сталкиваться с проблемами масштабируемости, особенно при работе с большим количеством атрибутов или сложными политиками доступа.
- Вычислительные затраты на операции шифрования и дешифрования в ABE растут со сложностью политик доступа и количеством задействованных атрибутов.
- Эффективные механизмы управления ключами и отзыва атрибутов имеют решающее значение для практического внедрения ABE в крупномасштабных системах.

Соответствие нормативным требованиям:

- Внедрение ABE в системах здравоохранения должно обеспечивать соблюдение правил и стандартов конфиденциальности данных, может быть непростой задачей.
- Обеспечение баланса между необходимостью детального контроля доступа и требованиями экстренного доступа к данным пациента в критических ситуациях является сложной проблемой.

c) Влияние:

Обеспечение безопасного обмена данными и совместной работы:

- ABE облегчает безопасный обмен конфиденциальными медицинскими данными между уполномоченными сторонами
- Это позволяет осуществлять детальный контроль доступа, гарантируя, что разные пользователи могут получать доступ только к определённым данным.

Расширение прав и возможностей пациентов:

- Интегрируя ABE в системы здравоохранения, пациенты могут иметь больший контроль над тем, кто может получить доступ к их медицинским записям и при каких условиях.
- Такой подход, ориентированный на пациента, соответствует растущей тенденции предоставления пациентам возможности самостоятельно управлять своими медицинскими данными.

Развитие здравоохранения с сохранением конфиденциальности:

- ABE вносит свой вклад в разработку решений для здравоохранения, обеспечивающих конфиденциальность, безопасное хранение медицинских данных и обмен ими в облачных средах.
- Он решает важнейшие проблемы безопасности данных и конфиденциальности в эпоху цифрового здравоохранения и Интернета вещей.

3) Алгоритм консенсуса, основанный на доказательстве объёма транзакции

Алгоритм консенсуса, основанный на доказательстве объёма транзакции, предлагает преимущества с точки зрения оптимизации пропускной способности транзакций, стимулирования активного участия и решения проблем масштабируемости. Однако у него также есть ограничения, связанные с потенциальной централизацией, уязвимостью к атакам и проблемами с внедрением.

a) Преимущества:

Оптимизированная пропускная способность транзакций:

- Основная цель алгоритма - оптимизировать пропускную способность транзакций, позволяя

сети блокчейн эффективно обрабатывать больший объём транзакций.

- За счёт приоритизации узлов с более высокими объёмами транзакций алгоритм направлен на повышение общей пропускной способности сети и способности обрабатывать большое количество транзакций.

Решение проблем масштабируемости:

- Алгоритм направлен на устранение низкой пропускной способности транзакций и ограничений масштабируемости существующих общедоступных решений для обработки медицинских данных на основе блокчейна.
- Уделяя особое внимание объёму транзакций как ключевому показателю, алгоритм стремится повысить способность сети обрабатывать крупномасштабные данные, генерируемые в медицинских сценариях Интернета вещей.

b) Ограничения:

Потенциальная централизация:

- Если небольшое количество узлов последовательно обрабатывает значительно больший объём транзакций, они могут получить непропорционально большое влияние на процесс согласования.
- Это может привести к некоторой централизации, подрывающей децентрализованный характер сети блокчейнов.

Уязвимость к атакам:

- Узлы с большими объёмами транзакций могут стать объектами атак, поскольку их компрометация позволит злоумышленнику нарушить процесс согласования.
- Алгоритму могут потребоваться дополнительные меры безопасности для снижения риска таких атак.

Сложность и проблемы с внедрением:

- Внедрение и интеграция алгоритма с существующими системами могут создавать проблемы с точки зрения сложности и внедрения.
- Эффективность алгоритма в реальных медицинских сценариях Интернета вещей требует дальнейшей проверки и тестирования.

c) Влияние:

Продвижение масштабируемых блокчейн-решений:

- Алгоритм способствует разработке более масштабируемых и эффективных блокчейн-решений для обработки больших объёмов транзакций.
- Это решает важнейшую проблему применения технологии блокчейн в областях с большим объёмом данных

Продвижение внедрения блокчейна в здравоохранении:

- Оптимизируя пропускную способность транзакций, алгоритм может сделать блокчейн более жизнеспособным для управления большими объёмами медицинских данных и обмена ими.
- Это может способствовать внедрению технологии блокчейн в отрасли здравоохранения, обеспечивая безопасное и эффективное управление данными и совместную работу.

Поощрение инноваций в алгоритмах достижения консенсуса:

- Алгоритм представляет собой инновационный подход к достижению консенсуса, ориентированный на объём транзакций как ключевой показатель.
- Это способствует текущим исследованиям и разработке новых согласованных алгоритмов, адаптированных к конкретным случаям использования и требованиям.

4) Контроль доступа к данным пациента

Механизм контроля доступа к данным пациента предлагает значительные преимущества с точки зрения повышения безопасности, конфиденциальности, детального контроля и расширения возможностей пациента.

a) Преимущества:

Повышенная безопасность и конфиденциальность:

- Система гарантирует, что пациенты имеют разрешения на управление своими медицинскими данными, защищая их права и интересы.
- Детальный контроль доступа с помощью шифрования на основе атрибутов (ABE) позволяет только авторизованным пользователям с определёнными атрибутами получать доступ к данным или изменять их.
- Политики контроля доступа применяются с помощью смарт-контрактов на блокчейне, обеспечивая автоматизированный и безопасный способ управления разрешениями.

Интеграция с блокчейном и Интернетом вещей:

- Механизм контроля доступа к данным пациента интегрирован с более широкой медицинской системой IoT-транзакций на основе блокчейна, предложенной в патенте.
- Эта интеграция обеспечивает безопасный и контролируемый доступ к данным, генерируемым

различными медицинскими устройствами Интернета вещей и носимыми устройствами.

- Неизменяемость и прозрачность блокчейна устанавливают доверие к системе и обеспечивают целостность данных.

Детальный контроль доступа:

- Система использует шифрование на основе атрибутов (ABE) для обеспечения детального контроля доступа к данным.
- Политики доступа могут определяться на основе различных атрибутов, таких как роли пользователей, местоположения или другие соответствующие факторы, что обеспечивает детальный и гибкий контроль доступа.

b) Ограничения:

Сложность и проблемы с внедрением:

- Внедрение детального контроля доступа и интеграция его с системами блокчейна и интернета вещей могут быть сложными, требующими значительных технических знаний и ресурсов.
- Проблемы с внедрением могут возникнуть из-за необходимости для организаций здравоохранения адаптировать свои существующие системы и процессы для включения новых механизмов контроля доступа.

Проблемы с масштабируемостью и производительностью:

- По мере роста объёма данных о пациентах и числа пользователей могут быть протестированы масштабируемость и производительность системы контроля доступа.
- Эффективное управление ключами, отзыв атрибутов и обновления политик становятся решающими для поддержания оперативности и эффективности системы.

c) Влияние:

Обеспечение безопасного обмена данными и совместной работы:

- Отлаженная система контроля доступа облегчает безопасный обмен данными о пациентах между уполномоченными заинтересованными сторонами в сфере здравоохранения, способствуя сотрудничеству и улучшая координацию медицинской помощи.
- Это позволяет исследователям получать доступ к анонимизированным данным пациентов для медицинских исследований, сохраняя при этом конфиденциальность пациента.

Стимулирование инноваций в сфере безопасности здравоохранения:

- Интеграция блокчейна, Интернета вещей и шифрования на основе атрибутов для контроля доступа к данным пациентов представляет собой инновационный подход к безопасности медицинских данных.
- Он демонстрирует потенциал использования новейших технологий для решения важнейших проблем конфиденциальности данных, безопасности и расширения прав и возможностей пациентов в эпоху цифрового здравоохранения.

5) Функции удалённой диагностики, обмена данными и транзакций данных

Функции удалённой диагностики, обмена данными и транзакций данных предлагают значительные преимущества с точки зрения улучшения доступа к медицинскому обслуживанию, расширения обмена данными и совместной работы. Однако существуют ограничения, связанные с техническими проблемами, соображениями безопасности данных и конфиденциальности, а также проблемами внедрения и интеграции.

a) Преимущества:

Улучшение доступа к медицинскому обслуживанию:

- Дистанционная диагностика позволяет пациентам получать медицинские консультации и диагнозы, не выходя из дома.
- Это особенно полезно для пациентов в сельской местности, пожилых пациентов или лиц с ограниченными физическими возможностями, которым может быть трудно получить доступ к традиционным медицинским учреждениям.
- Удалённый мониторинг позволяет непрерывно отслеживать данные о состоянии здоровья пациентов, обеспечивая раннее выявление потенциальных проблем со здоровьем и вмешательство в них.

Улучшенный обмен данными и совместная работа:

- Система облегчает безопасный обмен медицинскими данными между уполномоченными сторонами, такими как поставщики медицинских услуг, исследователи и страховщики.
- Технология блокчейн обеспечивает целостность, конфиденциальность и возможность проверки совместно используемых данных.
- Улучшенный обмен данными способствует сотрудничеству и позволяет принимать более обоснованные решения при уходе за пациентами.

Эффективные операции с данными:

- Система обеспечивает эффективные и безопасные транзакции данных между различными заинтересованными сторонами в экосистеме здравоохранения.

- Смарт-контракты могут автоматизировать процессы доступа к данным и совместного использования, снижая административные издержки и повышая эффективность.
- Безопасные транзакции с данными помогают сохранить конфиденциальность пациентов, обеспечивая при этом авторизованный доступ для законных целей.

b) Ограничения:

Технические проблемы:

- Для реализации удалённой диагностики и мониторинга может потребоваться специализированное оборудование и надёжное подключение к Интернету, что может быть сложной задачей в определённых областях.
- Обработка больших объёмов данных, генерируемых устройствами Интернета вещей, и обеспечение обработки и анализа в режиме реального времени могут быть технически сложными.

Вопросы безопасности и конфиденциальности данных:

- Обмен конфиденциальными медицинскими данными вызывает опасения по поводу безопасности данных и конфиденциальности пациентов.
- Для предотвращения несанкционированного доступа и утечки данных необходимо внедрить надёжные меры безопасности, такие как шифрование и механизмы контроля доступа.
- Соблюдение правил защиты данных, таких как HIPAA, усложняет проектирование и внедрение системы.

Проблемы внедрения и интеграции:

- Внедрение технологий дистанционной диагностики и мониторинга может потребовать значительных изменений в существующих рабочих процессах здравоохранения.
- Поставщикам медицинских услуг может потребоваться обучение и поддержка для эффективного использования новых технологий и интерпретации полученных данных.
- Интеграция с существующими системами электронной медицинской карты (EHR) и обеспечение бесперебойного обмена данными могут оказаться сложной задачей.

c) Влияние:

Трансформация системы оказания медицинской помощи:

Функции удалённой диагностики, обмена и транзакций данных потенциально могут преобразовать оказание медицинской помощи, сделав его более доступным, эффективным и ориентированным на пациента.

Эти технологии позволяют перейти к проактивной и профилактической помощи, снижая нагрузку на медицинские учреждения и улучшая результаты лечения пациентов.

Продвижение персонализированной медицины:

- Постоянный мониторинг и анализ данных о пациентах с помощью дистанционного мониторинга позволяет проводить персонализированные и целевые вмешательства.
- Медицинские работники могут разрабатывать планы лечения на основе индивидуальных потребностей пациента и его реакции, что приводит к более эффективному уходу.

Внедрение системы здравоохранения, основанной на данных:

- Система генерирует огромное количество медицинских данных, которые могут быть использованы для исследований, аналитики и поддержки принятия решений.
- Анализ агрегированных и анонимизированных данных о пациентах может привести к пониманию характера заболеваний, эффективности лечения и тенденций в области здоровья населения.
- Подходы, ориентированные на данные, могут служить основой для политики здравоохранения, распределения ресурсов и разработки новых методов лечения и вмешательств.

ПАТЕНТ US11483343B2

Аннотация – В документе представлен анализ патента US11483343B2, который относится к системе обнаружения фишинга и способу её использования. В ходе анализа будут рассмотрены различные аспекты патента, включая его технологическую основу, новизну изобретения, потенциальные области применения, а также выделены ключевые элементы, придающие ему значимость в области кибербезопасности.

Анализ полезен специалистам по безопасности, ИТ-экспертам и заинтересованным сторонам в различных отраслях, поскольку даёт им полное представление о сути патента и его полезности для усиления мер кибербезопасности. Он служит ценным ресурсом для понимания вклада запатентованной технологии в текущие усилия по борьбе с фишингом и другими кибер-угрозами.

A. Введение

Патент US11483343B2 "Phishing Detection System and Method of Use" посвящён усовершенствованной системе и методологии выявления фишинговых атак и смягчения их последствий. В патенте предлагается особая архитектура системы обнаружения фишинга, которая сканирует сообщения на наличие подозрительных URL-адресов и анализирует соответствующие веб-страницы для выявления попыток фишинга.

B. Область применения

Система и метод обнаружения фишинга применимы в широком спектре отраслей, которые полагаются на цифровые коммуникации и уязвимы для фишинговых атак:

1) Технологический сектор:

- Технологические компании, особенно те, которые предоставляют программное обеспечение, облачные сервисы, платформы социальных сетей и электронную коммерцию, являются основными целями фишинговых атак с целью получения пользовательских данных и учётных данных.
- Технологический сектор выигрывает от улучшения обнаружения фишинга для защиты своих платформ, клиентов и репутации.

2) Финансовый сектор:

- Финансовые учреждения, такие как банки, инвестиционные фирмы, страховые компании и финтех-стартапы, обрабатывают конфиденциальные финансовые данные и транзакции.
- Фишинговые атаки часто выдают себя за финансовые службы для кражи учётных данных учётной записи, платёжных реквизитов и совершения мошенничества.
- Финансовый сектор остро нуждается в эффективном обнаружении фишинга для обеспечения безопасности учётных записей клиентов и соблюдения нормативных требований.

3) Сектор здравоохранения:

- Организации здравоохранения, такие как больницы, поликлиники, страховые и фармацевтические компании, хранят личную медицинскую информацию и данные о страховании / платежах.
- Фишинговые атаки могут быть направлены на кражу данных пациента, мошенничество со страховкой или нарушение работы.
- Защита от фишинга имеет решающее значение для соблюдения требований HIPAA и доверия пациентов к сектору здравоохранения.

4) Образовательный сектор:

- Образовательные учреждения, от школ до университетов, перевели многие сервисы в онлайн-режим и хранят личные и финансовые данные учащихся.
- Фишинговые атаки могут быть нацелены на студентов, преподавателей и персонал с целью кражи академических записей, личных или исследовательских данных.
- Школы и университеты нуждаются в мерах по борьбе с фишингом для защиты образовательных данных и интеллектуальной собственности.

5) Государственный сектор:

- Правительственные учреждения на федеральном, местном уровне становятся мишенью атакующих, стремящихся получить конфиденциальные данные или нарушить работу сервисов.
- Улучшенное обнаружение фишинга может помочь обезопасить системы и данные госсектора.

C. Предлагаемое решение

Патент предлагает многоступенчатую систему обнаружения фишинга, которая сканирует сообщения, разрешает встроенные URL-адреса, извлекает функции веб-страниц и применяет машинное обучение для выявления попыток фишинга. Хотя он предлагает более упреждающий

и всеобъемлющий охват, чем традиционные методы, он может столкнуться с проблемами производительности и точности в меняющемся ландшафте фишинговых атак. Тем не менее, это представляет собой значительный шаг на пути к автоматизированному обнаружению и предотвращению фишинга в режиме реального времени.

Система и метод выявляют попытки фишинга в электронных сообщениях и направлены на упреждающее обнаружение и блокирование таких вредоносных сообщений.

1) Ключевые компоненты предлагаемого решения:

Детектор фишинга: основным компонентом является модуль детектора фишинга, который анализирует сообщения на предмет подозрительного содержания. Он состоит из двух основных подкомпонентов:

- **Механизм сканирования**: сканирует текст сообщения и вложения, чтобы идентифицировать любые присутствующие URL (веб-адреса) и извлекает эти URL для дальнейшего анализа.
- **Компонент Fetcher**: принимает URL-адреса, найденные механизмом сканирования, и преобразует их в реальные веб-страницы, на которые они указывают. Извлекает исходный HTML-код этих веб-страниц.

Механизмы извлечения: затем детектор фишинга извлекает два типа функций из полученных веб-страниц:

- **Извлечение на основе URL-адресов**: анализирует структуру и компоненты самого URL-адреса, такие как длина, специальные символы, использование IP-адреса и т.д. Подозрительные шаблоны могут указывать на попытку фишинга.
- **Извлечение на основе гиперссылок**: проверяет гиперссылки, присутствующие в исходном коде веб-страницы. Проверяет целевые URL-адреса, якорный текст и другие атрибуты ссылок на наличие признаков обмана.

Модели машинного обучения:

- **Гибридный принцип**: функции URL и гиперссылки объединены в гибридный набор функций, представляющий каждую веб-страницу что даёт характеристику подозрительности страницы.
- **Модели машинного обучения**: гибридные наборы функций используются для обучения классификаторов машинного обучения различать фишинговые и легитимные веб-страницы. Модели обучаются на больших наборах данных известных фишинговых и неопасных примеров.

2) Способ применения:

- **Сканирование сообщений**: при поступлении нового сообщения механизм сканирования детектора фишинга идентифицирует все URL-адреса, присутствующие в контенте.
- **Получение содержимого URL-адресов**: компонент fetcher преобразует найденные URL-адреса в целевые веб-страницы и извлекает исходный код страницы.
- **Механизм извлечения**: функции на основе URL-адресов и гиперссылок извлекаются с каждой веб-страницы.
- **Классификация**: предварительно подготовленные модели машинного обучения применяются к извлеченному набору функций. Модели классифицируют веб-страницу как фишинговую или легитимную.
- **Реализация действия**: если веб-страница считается попыткой фишинга, исходное сообщение может быть помещено в карантин или заблокировано. Для администраторов или предполагаемого получателя могут быть сформированы предупреждения.

D. Технологический процесс

Основной технологический процесс включает в себя механизм сканирования, извлекающий URL-адреса из сообщений, средство выборки преобразует эти URL-адреса в веб-страницы, анализирует характеристики URL-адресов и гиперссылок на этих страницах и применяет модели ML для обнаружения попыток фишинга, что приводит к автоматическому удалению фишинговых сообщений. Многоступенчатый анализ позволяет осуществлять упреждающую фильтрацию фишингового контента в режиме реального времени на основе характеристик целевой веб-страницы, выходя за рамки традиционных методов фильтрации по URL или контенту.

Технологический процесс охватывает полный жизненный цикл предлагаемого решения и фокусируется на требуемых аспектах:

1) Механизм сканирования и выборки:

- Модуль сканирования проверяет входящие сообщения, чтобы идентифицировать и извлекать любые URL-адреса, присутствующие в тексте сообщения или вложениях.
- Затем компонент fetcher преобразует извлечённые URL-адреса в реальные веб-страницы, на которые они указывают, и извлекает исходный HTML-код этих веб-страниц.

2) Обнаружение и получение содержимого URL-адресов:

- Механизм сканирования отвечает за обнаружение URL-адресов, встроенных в сообщения. Он сканирует содержимое сообщений и вложения для идентификации строк URL-адресов.
- Как только URL-адреса обнаружены, компонент fetcher преобразует их в целевые веб-страницы. Это включает в себя следующие перенаправления и получение конечной веб-страницы, на которую в итоге указывает URL-адрес.

- Программа выборки извлекает полный исходный HTML-код разрешённой веб-страницы для дальнейшего анализа.

3) Анализ веб-страницы:

- Полученный HTML-код веб-страницы анализируется для извлечения двух типов функций:
  - **Извлечение на основе URL**: анализ самой строки URL на наличие подозрительных шаблонов, таких как длина, специальные символы, использование IP-адреса и т.д.
  - **Извлечение на основе гиперссылок**: проверка гиперссылок в источнике веб-страницы, поиск целевых URL-адресов, текста привязки и атрибутов ссылки.
- Функции URL и гиперссылки объединены в гибридный набор функций, отражающий подозрительность веб-страницы.
- К набору функций применяются предварительно подготовленные модели машинного обучения, позволяющие классифицировать веб-страницу как фишинговую или легитимную.

4) Критерии обнаружения фишинга:

- Ключевыми критериями обнаружения фишинга являются URL-адрес и гиперссылки, извлечённые из веб-страницы.
- Подозрительные шаблоны URL-адресов могут включать чрезмерную длину, случайные символьные строки, IP-адреса, средства сокращения URL-адресов и т.д.
- Признаки гиперссылки, такие как несоответствие целевых URL-адресов, подозрительный якорный текст или ссылки на известные вредоносные сайты, могут указывать на фишинг.
- Модели машинного обучения совершенствуются на наборах данных известных фишинговых и законных веб-страниц для изучения отличительных паттернов.
- Веб-страница классифицируется как фишинговая, если модель определяет, что её URL-адрес и характеристики гиперссылок соответствуют изученным шаблонам вредоносных страниц.

5) Удаление сообщения:

- Если веб-страница, ссылка на которую содержится в сообщении, будет признана попыткой фишинга, исходное сообщение может быть помещено в карантин или удалено автоматически.
- Это предотвращает взаимодействие пользователя с вредоносным контентом и потенциальную компрометацию его информации.
- Удаление сообщения может произойти сразу после определения факта фишинга, до того, как сообщение попадёт во входящие пользователя.
- В качестве альтернативы подозрительные сообщения могут быть помечены для проверки перед удалением на случай потенциальных ложных срабатываний.

E. Преимущества, недостатки и значимость предлагаемого решения

1) Преимущества

Ключевыми преимуществами этой системы обнаружения фишинга являются её способность автоматически удалять фишинговые сообщения, избегать использования потенциально устаревших внешних чёрных списков, повышать точность обнаружения за счёт машинного обучения, предотвращать фишинг в режиме реального времени до того, как сообщения попадут в почтовые ящики, и интеграция с существующей инфраструктурой электронной почты для многоуровневой защиты. Эти возможности представляют собой значительный прогресс по сравнению с традиционными методами предотвращения фишинга.

a) Автоматическое удаление сообщений о фишинге:

- Если веб-страница, ссылка на которую содержится в сообщении, будет признана попыткой фишинга, исходное сообщение может быть автоматически помещено в карантин или удалено
- Это предотвращает взаимодействие пользователя с вредоносным контентом и потенциальную компрометацию его информации
- Удаление сообщения может произойти сразу после определения факта фишинга, до того, как сообщение попадёт во входящие пользователя

b) Снижение зависимости от внешних чёрных списков:

- Система позволяет избежать зависимости от внешних чёрных списков или баз данных, которые могут устареть
- Используются только функции на основе URL-адресов и гиперссылок, извлечённые из самого исходного кода веб-страницы, не полагаясь на сторонние сервисы
- Это позволяет ему обнаруживать новые и развивающиеся попытки фишинга, которые, возможно, ещё не внесены в чёрные списки

c) Повышена точность обнаружения фишинга:

- Объединение анализа URL-адресов и гиперссылок обеспечивает более полный охват и точность по сравнению с традиционными методами
- Модели машинного обучения совершенствуются на больших наборах данных известных примеров фишинга и вредоносных программ для изучения отличительных паттернов
- Это обеспечивает гибкую автоматизированную классификацию и снижает количество

ложноположительных результатов по сравнению с подходами, основанными на правилах

d) Предотвращение фишинга в режиме реального времени:

- Система обнаруживает фишинг, анализируя целевые веб-страницы, а не только содержимое сообщений
- URL-адреса разрешаются, а веб-страницы анализируются в режиме реального времени по мере поступления сообщений
- Это позволяет блокировать попытки фишинга до того, как они попадут в почтовый ящик пользователя, предотвращая взаимодействие с вредоносным контентом

e) Интеграция с агентами передачи почты или клиентским программным обеспечением:

- Система обнаружения фишинга может быть интегрирована в агенты передачи почты (MTAS) или программное обеспечение почтового клиента
- Интеграция с MTA позволяет сканировать и блокировать фишинговые сообщения в процессе доставки электронной почты
- Интеграция с почтовыми клиентами обеспечивает защиту последней мили на уровне устройства пользователя
- Это обеспечивает многоуровневую защиту как на сервере, так и на конечной точке

2) Ограничения

Несмотря на то, что система предлагает улучшения по сравнению с традиционными методами, она по-прежнему сталкивается с проблемами с точки зрения вычислительной эффективности, адаптируемости к новым угрозам, компромиссов в отношении точности, зависимости от внешних факторов, языкового охвата и поведения пользователя. Устранение этих ограничений будет ключом к обеспечению надёжной защиты от фишинга в режиме реального времени перед лицом постоянно развивающихся атак..

a) Вычислительные затраты и масштабируемость:

- Разрешение URL-адресов и масштабный анализ веб-страниц могут быть дорогостоящими с точки зрения вычислений
- Системе необходимо обрабатывать большой объем сообщений и URL-адресов, что может повлиять на производительность и масштабируемость
- Возможные задержки в доставке сообщений из-за процесса сканирования могут повлиять на работу пользователя

b) Постоянная гонка вооружений:

- Атакующие постоянно совершенствуют свои методы, чтобы избежать обнаружения, что приводит к продолжающейся гонке вооружений
- Системе может быть трудно справляться с новыми моделями фишинга и атаками нулевого дня
- Злоумышленники могут найти способы скрыть фишинговый контент или имитировать безопасные страницы, чтобы обойти обнаружение

c) Обработка ложноположительных и отрицательных результатов:

- Система может выдавать ложноположительные результаты, ошибочно помечая законные сообщения как фишинговые
- Ложноотрицательные сообщения, при которых попытки фишинга остаются незамеченными, также представляют опасность
- Балансировка точности и минимизация ложноположительных / отрицательных результатов является сложной задачей и влияет на доверие пользователей

d) Зависимость от внешних источников данных:

- Система использует данные сторонних производителей, такие как записи WHOIS, PageRank и т.д. для анализа веб-страниц
- Изменения или сбои в работе этих внешних источников данных могут повлиять на точность и надёжность системы

e) Язык и интернационализация:

- Попытки фишинга на разных языках или в определённых регионах может быть сложнее обнаружить
- Системе может потребоваться адаптация и обучение для обеспечения многоязычного и международного охвата

f) Поведение пользователей и социальная инженерия:

- Ни одно техническое решение не может полностью уберечь пользователей от хорошо продуманных попыток социальной инженерии
- Любопытство, рассеянность или недостаточная осторожность пользователя могут привести к переходам по фишинговым ссылкам, несмотря на предупреждения
- Непрерывное обучение и осведомлённость пользователей по-прежнему необходимы в дополнение к любой технической системе обнаружения

g) Потенциальные проблемы с конфиденциальностью:

- Анализ сообщений пользователей и активности в Интернете на предмет обнаружения фишинга может вызвать вопросы конфиденциальности

- Необходимо учитывать баланс между конфиденциальностью пользователей и эффективным обнаружением угроз

h) Опережать возникающие угрозы:

- По мере развития фишинговых тактик система обнаружения нуждается в постоянном обновлении и переподготовке
- Адаптация к новым моделям фишинга и векторам атак требует постоянных усилий и ресурсов

3) Значимость

Ключевым значением системы обнаружения фишинга является её способность повышать точность обнаружения с помощью машинного обучения, предотвращать фишинг в режиме реального времени до того, как сообщения попадут в почтовые ящики, автоматическое удаление фишинговых сообщений, избегание использования устаревших чёрных списков и интеграции с существующей инфраструктурой электронной почты для комплексной многоуровневой защиты. Эти возможности представляют собой значительный прогресс по сравнению с традиционными методами предотвращения фишинга в продолжающейся борьбе со все более изощренными фишинговыми атаками.

a) Повышение точность обнаружения фишинга:

- Объединение анализа URL-адресов и гиперссылок обеспечивает более полный охват и точность по сравнению с традиционными методами
- Модели машинного обучения совершенствуются на больших наборах данных известных примеров фишинга и вредоносных программ для изучения отличительных паттернов, что обеспечивает адаптируемую автоматическую классификацию и сокращает количество ложных срабатываний

b) Предотвращение фишинга в режиме реального времени:

- Система активно обнаруживает фишинг, анализируя веб-страницы назначения, а не только содержимое сообщений, в режиме реального времени по мере поступления сообщений
- Это позволяет блокировать попытки фишинга до того, как они попадут в почтовые ящики пользователей, предотвращая взаимодействие с вредоносным контентом

c) Автоматическое удаление сообщений:

- Если веб-страница, ссылка на которую содержится в сообщении, будет признана попыткой фишинга, исходное сообщение может быть автоматически помещено в карантин или удалено до того, как оно попадёт в почтовый ящик пользователя
- Это предотвращает взаимодействие пользователей с вредоносным контентом и потенциальную компрометацию их информации

d) Снижение зависимости от внешних чёрных списков:

- Система позволяет избежать зависимости от потенциально устаревших внешних чёрных списков, используя только функции URL и гиперссылок, извлечённые из самого исходного кода веб-страницы
- Это позволяет ему обнаруживать новые и развивающиеся попытки фишинга, которые, возможно, ещё не внесены в чёрные списки

e) Интеграция с инфраструктурой электронной почты:

- Система обнаружения фишинга может быть интегрирована в агенты передачи почты или программное обеспечение почтового клиента для сканирования на стороне сервера или защиты конечных точек последней мили
- Это обеспечивает многоуровневую защиту как на уровне доставки электронной почты, так и на уровне пользовательского устройства

ПАТЕНТ US11496512B2

Аннотация – в документе представлен подробный анализ патента US11496512B2, в котором описываются методы обнаружения фишинговых веб-сайтов. Анализ охватывает различные аспекты патента, включая его техническую основу, стратегии реализации и потенциальное влияние на практику кибербезопасности. Анализируя методику, этот документ призван дать всестороннее представление о её вкладе в повышение безопасности в Интернете.

Анализ обеспечивает качественное раскрытие содержательной части и даёт представление не только о технической стороне патента, но и исследует его практическое применение, преимущества в плане безопасности и потенциальные проблемы. Анализ важен для специалистов по кибербезопасности, ИТ-специалистов и заинтересованных сторон в различных отраслях, стремящихся понять и внедрить передовые методы обнаружения фишинга.

A. *Введение*

Патент US20220232015A1 «Detecting realtime phishing from a phished client or at a security server» выдан 8 ноября 2022 года изобретателям Джереми Бойд Ричардс и Брайан Джеймс Бак, и правопреемнику – компания Lookout, Inc. Патент описывает способ, включающий получение запроса на веб-страницу с клиентского устройства на сервере, генерацию и вставку закодированного значения отслеживания на веб-страницу.

B. *Основная идея*

Предлагаемое решение направлено на улучшение протоколов безопасности для защиты от фишинга, который является значительной угрозой в сфере кибербезопасности. Использование встраиваемого значения является технической мерой для отслеживания и проверки веб-взаимодействий с целью предотвращения несанкционированного доступа или утечки данных.

Ключевые моменты:

Назначение: метод обнаружения фишинговых атак в реальном времени, который может применяться при фишинге клиентского устройства или на уровне сервера безопасности.

Методология: метод включает в себя получение запроса веб-страницы с клиентского устройства на сервере, генерацию закодированного значения отслеживания (ETV) и вставку этого ETV на веб-страницу.

Применение: предлагаемое решение является частью более широкой системы, направленной на усиление мер кибербезопасности, конкретно нацеленной на обнаружение попыток фишинга в режиме реального времени.

Составляющие процесса функционирования предлагаемого решения:

Получение запроса: сервер получает запрос на веб-страницу от клиентского устройства.

Генерация и вставка закодированного значения отслеживания (ETV): сервер генерирует ETV и вставляет его на веб-страницу.

Дополнительные вставки: сервер может выполнять дополнительные вставки или модификации веб-страницы в рамках своей работы.

C. *Предлагаемое решение*

Решение представляет собой комплексный метод, направленный на повышение безопасности путём обнаружения попыток фишинга в режиме реального времени. Ниже приводится подробное описание предлагаемого метода с акцентом на его трех основных компонентах: получение запроса, генерация и вставка закодированного значения отслеживания (ETV) и дополнительные вставки.

1) *Получение запроса*

На начальном этапе сервер получает запрос на веб-страницу от клиентского устройства. Этот шаг имеет важное значение, поскольку устанавливает связь между клиентом и сервером, подготавливая почву для применения последующих мер безопасности. Получение запроса является для сервера отправной точкой для инициирования процесса обеспечения безопасности веб-страницы и мониторинга фишинговых действий.

В контексте безопасности получение первоначального запроса позволяет установить законность взаимодействия и применить соответствующие протоколы безопасности. Начиная процесс с получения запроса, метод гарантирует, что каждое взаимодействие с самого начала рассматривается как защищённое.

a) *Получение запроса*

Инициирование связи: процесс начинается, когда первое вычислительное устройство, которым может быть мобильное или любое другое клиентское устройство, инициирует запрос на доступ к услуге. Запрос направлен на

сервер, на котором размещён или контролируется рассматриваемый сервис или веб-страница.

Запуск мер безопасности: при получении запроса серверу предлагается предпринять действие. На этом этапе рассматриваются и потенциально применяются меры безопасности. Ответ сервера на запрос касается не только обслуживания запрошенной веб-страницы, но и обеспечения безопасности транзакции.

Идентификация клиентского устройства: сервер идентифицирует запрашивающее клиентское устройство. Эта идентификация имеет важное значение для адаптации ответа системы безопасности к контексту запроса. Например, если известно, что клиентское устройство защищено или имеет историю взаимодействий с сервером, меры безопасности могут отличаться по сравнению с неизвестным или подозрительным устройством.

Возможности обнаружения фишинга в режиме реального времени: получение запроса связано не только с доставкой контента, но и с отслеживанием признаков фишинга. Сервер может проанализировать запрос на наличие аномалий или признаков компрометации, которые указывают на попытку фишинга.

Основа для кодированного значения отслеживания (ETV): приём запроса создаёт основу для следующих шагов в методе, в частности, для генерации и вставки кодированного значения отслеживания. Закодированное значение является важным компонентом, который будет встроен в веб-страницу в ответ на запрос, предоставляя средства для её отслеживания и проверки целостности.

2) Генерация и вставка закодированного значения отслеживания (ETV)

После получения запроса веб-страницы сервер генерирует закодированное значение отслеживания (ETV) и вставляет его на веб-страницу. ETV – это уникальный идентификатор или маркер, который служит нескольким целям: **отслеживанию, безопасности и проверке**.

Этот шаг представляет собой комплексный подход к повышению кибербезопасности. Благодаря использованию уникальных безопасных идентификаторов, встроенных непосредственно в веб-страницы, метод обеспечивает надёжный механизм для обнаружения фишинга в режиме реального времени, проверки целостности и общего повышения уровня цифровой безопасности протоколов

Компонент является важным этапом в предлагаемом методе повышения кибербезопасности, особенно в контексте обнаружения фишинга в режиме реального времени. Этот шаг следует за первоначальным приёмом запроса веб-страницы с клиентского устройства и имеет решающее значение для создания механизма отслеживания, безопасности и проверки.

a) Генерация закодированного значения отслеживания (ETV)

Создание ETV: сервер генерирует кодированное значение отслеживания (ETV) при получении запроса для веб-страницы. ETV – это уникальный идентификатор или код, который специально создаётся для сеанса или взаимодействия. Генерация этого значения представляет собой процесс, который сложно воспроизвести злоумышленникам.

Безопасность и уникальность: ETV-значение включает элементы, повышающие безопасность, такие как шифрование или хэширование, что делает его надёжным средством защиты от несанкционированного доступа и подделки. Уникальность каждого ETV имеет решающее значение для отслеживания запросов и ответов на отдельные веб-страницы, гарантируя, что каждое взаимодействие может быть независимо проверено.

b) Вставка ETV на веб-страницу

Процесс встраивания: после формирования ETV это значение вставляется на веб-страницу, которая должна быть отправлена на запрашивающее клиентское устройство. Вставка может быть выполнена различными способами, например встраивание в код веб-страницы, вставка в виде скрытого поля или включение в метаданные веб-страницы.

Цель вставки: основная цель вставки ETV на веб-страницу – создать отслеживаемую связь между ответом сервера и запросом клиента. Это позволяет серверу проверять целостность и подлинность веб-страницы при доступе к ней или взаимодействии с ней клиентского устройства.

c) Роль в обнаружении фишинга

Обнаружение в режиме реального времени: ETV позволяет серверу обнаруживать попытки фишинга в режиме реального времени. Проверяя наличие и целостность ETV при последующих взаимодействиях (таких как отправка форм или запросов на дополнительные ресурсы), сервер может выявить несоответствия, которые указывают на фишинговую атаку.

Верификация и проверка целостности: ETV выступает в качестве краеугольного камня для проверки целостности веб-страницы. Любое изменение или отсутствие ETV в ожидаемых взаимодействиях может вызвать оповещения или инициировать защитные меры, тем самым предотвращая успех фишинговых атак.

d) Преимущества

Повышенная безопасность: создание и вставка ETV значительно повышают безопасность веб-взаимодействий за счёт добавления уровня проверки, который злоумышленникам трудно обойти.

Гибкость и адаптируемость: метод обеспечивает гибкость в способах создания и вставки ETV, что делает его адаптируемым к различным веб-технологиям и требованиям безопасности.

Проактивный подход: благодаря встраиванию системы безопасности непосредственно в веб-страницу, предоставляемую клиенту, метод использует проактивный подход к обеспечению безопасности, а не полагается исключительно на меры реагирования после обнаружения атаки.

3) Дополнительные вставки

Метод также включает в себя возможность внесения дополнительных вставок или модификаций на веб-страницу. Это дополнительные меры безопасности, коды отслеживания или любые другие изменения, которые будут сочтены необходимыми для повышения безопасности и целостности веб-страницы. Гибкость в добавлении дополнительных уровней мер безопасности гарантирует, что метод может адаптироваться к развивающимся кибер-угрозам и методам фишинга.

Этот компонент является важнейшим аспектом предлагаемого метода повышения кибербезопасности, особенно в контексте обнаружения фишинга в режиме реального времени и основан на основополагающих шагах получения запроса веб-страницы и генерации и вставки закодированного значения отслеживания (ETV).

a) Концепция дополнительных вставок

После того, как ETV сгенерировано и вставлено на веб-страницу, метод допускает дальнейшие модификации или вставки. Дополнительные вставки могут служить различным целям, повышая безопасность, функциональность или удобство использования веб-страницы пользователем. Характер вставок может сильно различаться в зависимости от конкретных требований безопасности, типа обслуживаемого контента и ожидаемых угроз.

b) Типы дополнительных вставок

Улучшения безопасности: могут быть введены дополнительные меры безопасности, такие как более сложные коды отслеживания, сценарии для обнаружения необычного поведения пользователя или механизмы проверки действий пользователя. Эти усовершенствования направлены на защиту веб-страницы от более широкого спектра кибер-угроз, включая фишинг, но не ограничиваясь им.

Персонализация контента: вставки также могут включать персонализированный контент или функции, адаптированные к профилю пользователя или прошлым взаимодействиям с сервисом. Персонализация, хотя и не имеет прямого отношения к безопасности, может повысить вовлеченность пользователей и, как следствие, эффективность любых подсказок или предупреждений по безопасности.

Улучшения взаимодействия с пользователем: могут быть включены дополнительные сценарии или элементы, улучшающие взаимодействие с пользователем, такие как функции специальных возможностей, интерактивные элементы или динамические обновления контента. Улучшение взаимодействия с пользователем косвенно способствует повышению безопасности, делая законные веб-страницы более отличимыми от попыток фишинга.

c) Значение для обнаружения фишинга

Включение дополнительных вставок особенно актуально в контексте обнаружения фишинга по нескольким причинам:

Многоуровневый подход к обеспечению безопасности: обеспечивая несколько уровней мер безопасности, метод создаёт более надёжную защиту от фишинга и других кибер-угроз. Такой многоуровневый подход затрудняет злоумышленникам имитацию или обход функций безопасности законной веб-страницы.

Адаптивность к возникающим угрозам: гибкость при включении дополнительных вставок означает, что метод со временем может быть адаптирован для решения новых или развивающихся кибер-угроз. Поскольку методы фишинга становятся все более изощренными, для противодействия им могут быть разработаны и внедрены новые типы вставок.

Улучшенное отслеживание и анализ: дополнительные вставки предоставляют больше точек данных для отслеживания взаимодействий с пользователем и анализа поведения. Эти данные могут оказаться бесценными для выявления подозрительной активности, которая может указывать на попытку фишинга или другие угрозы безопасности.

D. Значимость предлагаемого решения

Значение предлагаемого метода решения в области кибербезопасности, особенно в борьбе с фишинговыми атаками, многогранно и глубоко. Метод, который включает в себя получение запроса веб-страницы, генерацию и вставку закодированного значения отслеживания (ETV), а также выполнение дополнительных вставок, представляет собой комплексный подход к повышению онлайн-безопасности.

Эти свойства помогают выходит за рамки технических достоинств, представляя собой переход к более активным, адаптивным и ориентированным на пользователя подходам к кибербезопасности. Встраивая систему безопасности непосредственно в структуру веб-взаимодействий, метод обеспечивает надёжную защиту от фишинговых атак, повышая безопасность и целостность онлайн-пространств. Поскольку кибер-угрозы продолжают развиваться, такие инновационные подходы будут иметь решающее значение для защиты цифровых активов и укрепления доверия к цифровой экосистеме.

1) Упреждающая защита от фишинга

Фишинговые атаки стали чрезвычайно эффективными и часто идут в обход традиционных мер безопасности. Предлагаемый метод вводит механизм упреждающей защиты, который активно внедряет её в саму веб-страницу посредством использования ETV и дополнительных вставок. Подход направлен не только на обнаружение попыток фишинга по мере их возникновения, но и на их предотвращение, значительно затрудняя злоумышленникам копирование законных веб-страниц или их подделку.

2) Повышение целостности веб-страницы и доверия

Создавая и внедряя ETV на веб-страницу, метод гарантирует, что целостность веб-страницы может быть проверена в любой момент её взаимодействия с клиентом. Процесс создаёт уровень доверия между сервером и

клиентом, заверяя пользователей в том, что контент, с которым они взаимодействуют, безопасен и не был скомпрометирован. Это особенно важно в эпоху, когда доверие к цифровым технологиям имеет первостепенное значение для пользовательского опыта.

3) Способность адаптироваться к возникающим угрозам

Включение «Дополнительных вставок» как части метода обеспечивает гибкую и адаптивную стратегию безопасности. По мере развития кибер-угроз разрабатываются новые меры безопасности, которые могут быть легко интегрированы в веб-страницу, не требуя капитального ремонта существующей инфраструктуры безопасности. Такая адаптивность гарантирует, что метод остаётся эффективным в борьбе с будущими методами фишинга и другими кибер-угрозами.

4) Обнаружение и реагирование в режиме реального времени

Одной из отличительных особенностей предлагаемого метода является его способность обнаруживать попытки фишинга в режиме реального времени. Отслеживая целостность ETV и поведение веб-страницы в режиме реального времени, система может быстро выявлять потенциальные фишинговые действия и реагировать соответствующим образом. Возможность немедленного реагирования имеет решающее значение для минимизации воздействия фишинговых атак на пользователей и организации.

5) Вклад в исследования и практику в области кибербезопасности

Метод вносит вклад в более широкую область исследований и практики в области кибербезопасности, обеспечивая новый подход к обнаружению и предотвращению фишинга. Он предлагает практическое решение, которое может быть реализовано организациями для защиты своих онлайн-активов и пользователей. Кроме того, метод служит основой для будущих исследований и разработок в области веб-безопасности, поощряя дальнейшие инновации в борьбе с кибер-угрозами.

E. Потенциальные результаты применения .

Потенциальные результаты для будущих исследований огромны и охватывают технические достижения в области кибербезопасности, улучшения пользовательского опыта, междисциплинарные приложения и влияние на политику и регулирование. Закладывая основу для создания более безопасной и заслуживающей доверия цифровой среды, этот метод создаёт основу для широкого спектра исследовательских возможностей, направленных на дальнейшее повышение онлайн-безопасности и доверия пользователей.

Предлагая новый подход к обнаружению фишинга в режиме реального времени, он не только удовлетворяет критическую потребность в кибербезопасности, но и открывает новые возможности для совершенствования исследовательских методологий, повышения целостности данных, стимулирования междисциплинарных исследований и внесения вклада в совершенствование политики и практики в эпоху цифровых технологий.

Метод также направлен на повышение кибербезопасности за счёт обнаружения фишинга в режиме реального времени с помощью закодированных значений отслеживания и дополнительных вставок, что имеет значительные потенциальные последствия для будущих исследований в нескольких ключевых областях:

1) Совершенствование мер кибербезопасности

Метод представляет собой новый подход к обнаружению и смягчению последствий фишинговых атак в режиме реального времени, что может вдохновить на дальнейшие исследования более сложных механизмов кибербезопасности. В будущих исследованиях могут быть рассмотрены вопросы оптимизации методов генерации и внедрения закодированных значений, разработки более совершенных алгоритмов для обнаружения угроз в режиме реального времени и интеграции моделей машинного обучения для более эффективного прогнозирования и предотвращения попыток фишинга.

2) Улучшение проверки целостности веб-страницы

Использование встраиваемых значений для проверки целостности веб-страниц открывает новые возможности для исследований в области обеспечения подлинности цифрового контента. Это может привести к разработке новых стандартов и протоколов веб-безопасности с упором на динамическую проверку элементов веб-страниц для предотвращения несанкционированного доступа и модификации контента.

3) Улучшение пользовательского опыта и доверия

Акцент метода на поддержании целостности веб-взаимодействий без ущерба для пользовательского опыта стимулирует исследования решений безопасности, ориентированных на пользователя. Это исследование может привести к разработке более интуитивно понятных и менее навязчивых механизмов безопасности, которые повышают вовлеченность пользователей, обеспечивая при этом надёжную защиту от кибер-угроз.

4) Междисциплинарные приложения

Принципы, лежащие в основе предлагаемого метода, могут иметь последствия не только для кибербезопасности, вдохновляя на исследования в таких областях, как цифровая криминалистика, электронная коммерция и онлайн-образование. Например, подход метода к отслеживанию и проверке взаимодействий на веб-страницах может быть адаптирован для использования в цифровых судебных расследованиях, что повысит способность отслеживать вредоносные действия и проверять подлинность цифровых доказательств.

5) Политические и нормативные последствия

Поскольку метод обеспечивает упреждающий подход к борьбе с фишингом, он может повлиять на будущие политики и нормативные акты, касающиеся онлайн-безопасности и защиты данных. В ходе исследования можно было бы изучить последствия широкого внедрения таких методов для законов о конфиденциальности,

стандартов защиты данных и нормативных требований к онлайн-сервисам. Это приведёт к выработке рекомендаций для директивных органов о том, как включить передовые меры кибербезопасности в нормативно-правовую базу.

F. Потенциальные возможности

Метод фокусируется на обнаружении фишинга в режиме реального времени посредством генерации и вставки закодированных значений отслеживания и дополнительных вставок и предлагает ряд потенциальных преимуществ для будущих исследований в различных областях. Эти преимущества не только подчёркивают непосредственное применение метода для повышения кибербезопасности, но и подчёркивают его более широкое значение для совершенствования исследовательских методологий, улучшения целостности данных и стимулирования междисциплинарных исследований.

Это предлагает основу для будущих исследований в самых разных областях. Новый подход к обнаружению фишинга в режиме реального времени не только удовлетворяет критическую потребность в кибербезопасности, но и открывает новые возможности для совершенствования исследовательских методологий, повышения целостности данных, стимулирования междисциплинарных исследований и внесения вклада в совершенствование политики и практики в эпоху цифровых технологий.

1) Продвижение исследований в области кибербезопасности

Метод обеспечивает новый подход к обнаружению и смягчению последствий фишинговых атак, который может послужить основой для дальнейших исследований в области кибербезопасности. Это открывает новые возможности для изучения того, как можно разработать динамические механизмы обнаружения в реальном времени и интегрировать их в существующие системы безопасности. Исследователи могут использовать этот метод для создания более сложных алгоритмов и технологий, которые учитывают меняющийся ландшафт кибер-угроз.

2) Повышение целостности и доверия к данным

Обеспечивая целостность веб-взаимодействий с помощью ETV, предлагаемый метод может внести вклад в исследования целостности данных и доверия в цифровых средах. Это особенно актуально в таких областях, как электронная коммерция, онлайн-банкинг и цифровые коммуникации, где аутентичность данных и доверие пользователей имеют первостепенное значение. В будущих исследованиях можно изучить, как аналогичные механизмы применяются к другим типам цифровых транзакций и взаимодействий для предотвращения мошенничества и обеспечения целостности данных.

3) Содействие Междисциплинарным исследованиям

Акцент метода на обнаружение в режиме реального времени и использование закодированных значений отслеживания имеет последствия не только для кибербезопасности, но и потенциально приносит пользу междисциплинарным исследованиям, сочетающим технологии с психологией, социологией и юриспруденцией. Например, исследователи могут исследовать психологические аспекты фишинговых атак и реакцию пользователей на меры безопасности или изучить правовые рамки для защиты пользователей и судебного преследования злоумышленников.

4) Совершенствование исследовательских методологий

Метод также может влиять на методологии исследований, особенно на то, как данные собираются, проверяются и анализируются в исследованиях в режиме реального времени. Это может привести к разработке новых исследовательских инструментов и методов, которые используют кодированное отслеживание или аналогичные механизмы для обеспечения подлинности и достоверности данных, собранных из онлайн-источников или с помощью цифровых платформ.

5) Вклад в мировую практику

Наконец, предлагаемый метод потенциально может служить основой для разработки политики и внедрения передовых практик в области кибербезопасности. Продемонстрировав эффективность обнаружения фишинга в режиме реального времени, будущие исследования могли бы дать основанные на фактических данных рекомендации по разработке более строгих политик, нормативных актов и отраслевых стандартов кибербезопасности. Это поможет организациям, правительствам и частным лицам лучше защитить себя от фишинга и других кибер-угроз.

G. Потенциальные ограничения

В будущих исследованиях необходимо будет устранить потенциальные ограничения путём изучения масштабируемости метода, его адаптируемости к развивающимся угрозам, моделей взаимодействия с пользователем, точности анализа, последствий для конфиденциальности и универсальности для различных платформ и технологий. Признание и устранение этих ограничений имеет решающее значение для продвижения применения метода и для внесения вклада в более широкую область исследований в области кибербезопасности.

Хотя он предлагает новый подход к обнаружению фишинга в режиме реального времени, существуют потенциальные ограничения, которые могут повлиять на его применение в будущих исследованиях:

1) Методологические ограничения

Сложность реализации: генерация и вставка ETV могут включать сложные алгоритмы и требовать значительных вычислительных мощностей, что может ограничить масштабируемость или применимость в средах с ограниченными ресурсами.

Эволюция тактики фишинга: фишеры постоянно совершенствуют свою тактику обхода мер безопасности. Возможно, потребуется регулярное обновление метода, чтобы соответствовать новым методам фишинга, что может стать проблемой для исследователей и практиков.

2) Эмпирические ограничения

Поведение и взаимодействие пользователя: на эффективность метода может влиять поведение пользователя. Если пользователи не взаимодействуют с веб-страницей должным образом, ETV и дополнительные вставки будут работать не так, как предполагалось, что потенциально ограничивает эффективность метода.

Ложноположительные результаты / негативы: метод потенциально может давать ложноположительные результаты или негативы при обнаружении попыток фишинга, что повлияет на доверие пользователей и общую надёжность системы.

3) Аналитические ограничения

Анализ и интерпретация данных: метод основан на анализе веб-взаимодействий, которые могут быть подвержены ошибкам интерпретации. Точность обнаружения фишинга ограничена используемыми аналитическими инструментами и методами.

4) Вопросы этики и конфиденциальности

Конфиденциальность пользователей: отслеживание и анализ взаимодействий пользователей вызывает опасения по поводу конфиденциальности. Для решения этих проблем важно обеспечить согласие пользователя и поддерживать прозрачность в отношении использования данных.

5) Обобщаемость

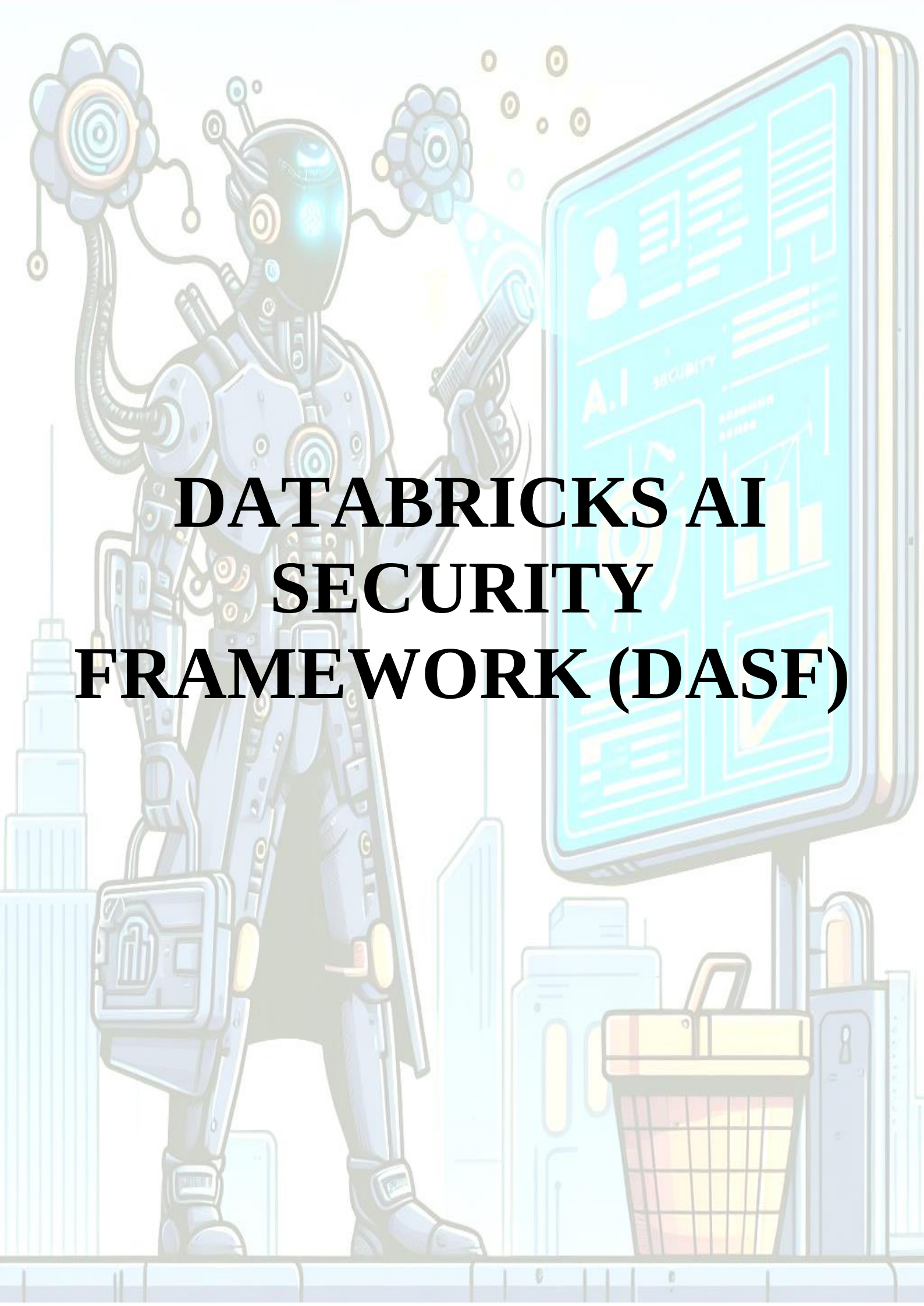
Применимость на различных платформах: метод был разработан с учётом определённых типов веб-страниц или сервисов. Его эффективность на различных платформах, устройствах или браузерах может быть ограниченной и требовать дальнейших исследований.

6) Технологический прогресс

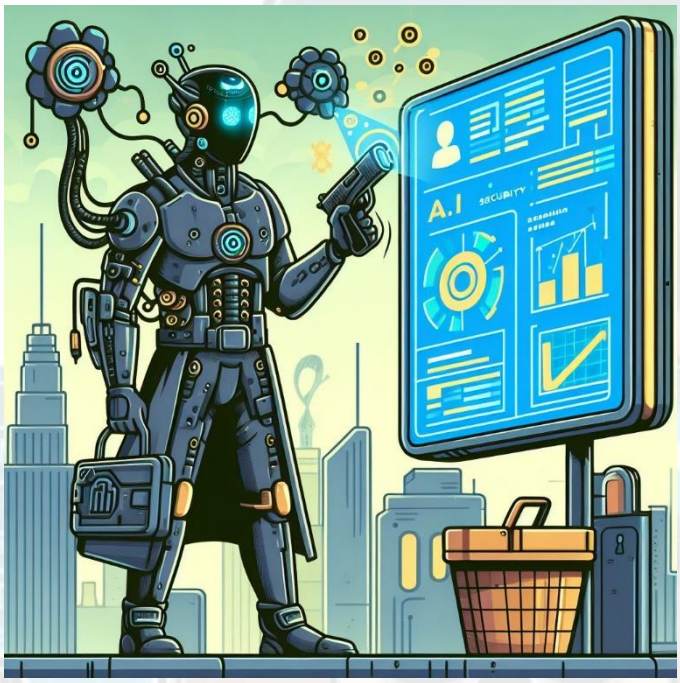
Адаптация к новым технологиям: по мере развития веб-технологий метод потребуется адаптировать, чтобы он оставался эффективным. Это может включать исследование того, как этот он применяется к новым веб-стандартам или технологиям.

H. Заключение

Предлагаемое решение представляет собой метод, который вносит значительный вклад в область кибербезопасности, демонстрируя упреждающий и динамичный подход к обнаружению и предотвращению фишинговых атак в режиме реального времени. Сосредоточив внимание на взаимодействии между клиентским устройством и сервером и используя кодированное значение отслеживания (ETV) наряду с возможностью дополнительных вставок безопасности, метод обеспечивает надёжную основу для повышения безопасности веб-коммуникаций. Такой подход не только помогает выявлять попытки фишинга по мере их возникновения, но и добавляет уровень верификации и проверки целостности, что крайне важно в нынешнюю цифровую эпоху, когда фишинговые атаки становятся все более изощренными и их труднее обнаружить



DATABRICKS AI SECURITY FRAMEWORK (DASF)



Аннотация – В этом документе представлен анализ DASF, изучается его структура, рекомендации и практические приложения, которые он предлагает организациям, внедряющим решения в области искусственного интеллекта. Этот анализ не только служит качественной экспертизой, но также подчёркивает его важность и практическую пользу для экспертов по безопасности и профессионалов из различных секторов. Внедряя руководящие принципы и средства контроля, рекомендованные DASF, организации могут защитить свои активы искусственного интеллекта от возникающих угроз и уязвимостей.

A. Введение

Databricks AI Security Framework (DASF) представляет собой всеобъемлющее руководство, разработанное для устранения возникающих рисков, связанных с повсеместной интеграцией ИИ по всему миру и направлено на предоставление действенных рекомендаций по защитному контролю для систем ИИ, охватывающих весь жизненный цикл ИИ и облегчающих сотрудничество между бизнесом, ИТ, данными, ИИ и командами безопасности. DASF не ограничивается моделями защиты или конечными точками, но применяет целостный подход к снижению кибер-рисков в системах ИИ.

DASF идентифицирует 55 технических рисков безопасности в 12 основополагающих компонентов общей системы ИИ, ориентированной на данные, включая необработанные данные, подготовку данных, наборы данных, управление каталогом данных, алгоритмы машинного обучения, оценку, модели машинного обучения, управление моделями, обслуживание моделей и вывод, реакцию на вывод, операции машинного обучения (MLOP), а также безопасность данных и платформы искусственного интеллекта. Каждый риск сопоставляется с набором мер по смягчению последствий, которые ранжируются в приоритетном порядке, начиная с обеспечения безопасности периметра и заканчивая безопасностью данных.

Фреймворк анализа данных выделяется как ключевой компонент DASF, предлагающий единую основу для всех данных и управления и включает в себя Mosaic AI, Unity, архитектуру и безопасность платформы Databricks. Mosaic AI охватывает сквозной рабочий процесс ИИ, в то время как Unity Catalog предоставляет унифицированное решение для управления данными и активами ИИ. Архитектура представляет собой гибридный PaaS, не зависящий от данных, а безопасность основана на принципах доверия, технологий и прозрачности.

DASF предназначен для групп безопасности, практиков ML, руководителей и инженерных команд DevSecOps. Это обеспечивает структурированный подход к новым угрозам и способах их устранения, не требуя привлечения глубоких экспертных знаний. DASF также включает подробное руководство по пониманию безопасности и соответствия конкретным системам ML, предлагающее информацию о том, как ML влияет на безопасность системы, применение принципов разработки безопасности к ML и предоставляющее подробное руководство по пониманию безопасности и соответствия конкретным системам ML.

DASF завершается рекомендациями о том, как безопасно управлять моделями искусственного интеллекта и внедрять их в соответствии с основными принципами внедрения машинного обучения: определения бизнес-сценария использования ML, определения модели развёртывания ML, перечисления угроз и рисков для каждого риска и выбора средства контроля для внедрения. В нем также содержится дополнительная информация для расширения знаний в области искусственного интеллекта и фреймворков, рассмотренных в рамках анализа.

Ключевые моменты:

- **Совместное использование**: DASF разработан для совместного использования командами обработки данных и искусственного интеллекта вместе с их коллегами по безопасности. Это подчёркивает важность совместной работы этих команд на протяжении всего жизненного цикла искусственного интеллекта для обеспечения безопасности и соответствия требованиям систем искусственного интеллекта.
- **Применимость в разных командах**: Концепции DASF применимы ко всем командам, независимо от того, используют ли они Databricks для создания своих решений в области ИИ. Такая инклюзивность гарантирует, что фреймворк может быть использован широкой аудиторией для повышения безопасности искусственного интеллекта.
- **Руководство по типам моделей ИИ**: предлагается, чтобы организации сначала определили, какие типы моделей искусственного интеллекта создаются или используются. В нем модели в широком смысле подразделяются на прогнозирующие модели ML, современные открытые модели и внешние модели,

обеспечивая основу для понимания конкретных соображений безопасности для каждого типа.

- **Понимание компонентов системы ИИ**: организациям рекомендуется ознакомиться с основополагающими компонентами общей системы искусственного интеллекта, ориентированной на данные, как описано в документе.
- **Идентификация рисков и снижение их последствий**: DASF помогает организациям выявлять соответствующие риски и определять применимые средства контроля на основе всеобъемлющего списка, представленного в документе. Такой структурированный подход помогает расставить приоритеты в мерах безопасности на основе конкретных потребностей организации.
- **Документация и функции в терминологии Databricks**: Цель подхода сделать документ полезным для более широкой аудитории, сохраняя при этом его практичность для пользователей Databricks.

B. Целевая аудитория

- **Команды безопасности**: CISO, руководители служб безопасности, DevSecOps, SRE-инженеры и другие лица, ответственные за безопасность систем. Они могут использовать DASF, чтобы понять, как машинное обучение (ML) повлияет на безопасность системы, и понять основные механизмы ML.
- **Инженеры ML**: инженеры по обработке данных, архитекторы данных, инженеры по обработке данных и специалисты по обработке данных. DASF помогает им понять, как инженерия безопасности и менталитет "защищённости по замыслу" могут быть применены к ML.
- **Governance-сотрудники**: отвечают за обеспечение соответствия данных и методов ИИ в организации соответствующим законам, нормативным актам и политике. DASF предоставляет рекомендации о том, как ML влияет на безопасность системы и соответствие требованиям.
- **Команды инженеров DevSecOps**: отвечают за интеграцию безопасности в процессы разработки и эксплуатации. DASF предлагает этим командам структурированный способ обсуждения новых угроз и мер по их устранению, не требующий обмена глубокими знаниями.

C. Преимущества и Недостатки

DASF предлагает всеобъемлющее и практическое руководство для организаций, стремящихся понять риски безопасности искусственного интеллекта и снизить их. Однако его сложность и ориентированное на блоки данных руководство могут представлять проблемы для некоторых организаций.

1) Преимущества

- **Целостный подход**: DASF применяет целостный подход к безопасности ИИ, устраняя риски на протяжении всего жизненного цикла ИИ и всех компонентов универсальной системы ИИ, ориентированной на данные. Такой комплексный подход помогает организациям более эффективно выявлять риски безопасности и снижать их уровень.
- **Сотрудничество**: Фреймворк предназначен для облегчения взаимодействия между бизнесом, ИТ, данными, искусственным интеллектом и командами безопасности. Это поощряет единый подход к обеспечению безопасности искусственного интеллекта и помогает преодолеть разрыв между различными дисциплинами.
- **Практические рекомендации**: DASF предоставляет практические рекомендации по защитному контролю для каждого выявленного риска, которые могут обновляться по мере появления новых рисков и появления дополнительных средств контроля. Это гарантирует, что организации смогут оставаться в курсе возникающих угроз безопасности искусственного интеллекта.
- **Применимость**: DASF применим к организациям, использующим различные модели ИИ, включая прогнозирующие модели ML, генеративные модели искусственного интеллекта и внешние модели. Такая широкая применимость делает его ценным ресурсом для широкого круга организаций.
- **Интеграция с платформой анализа данных Databricks**: для организаций, использующих платформу анализа данных Databricks, DASF предлагает конкретные рекомендации по использованию средств управления рисками искусственного интеллекта платформы. Это помогает организациям максимально использовать преимущества платформы в области безопасности.

2) Недостатки

- **Сложность**: DASF охватывает широкий спектр рисков для безопасности ИИ и мер по их снижению, которые могут оказаться непосильными для организаций, не знакомых с безопасностью ИИ или имеющих ограниченные ресурсы, а внедрение системы может потребовать значительных затрат времени и усилий.
- **Руководство, ориентированное на Databricks**: хотя DASF предлагает рекомендации для организаций, использующих платформу Databricks Data Intelligence Platform, некоторые рекомендации могут быть менее применимы или неосуществимы для организаций, использующих другие платформы или инструменты искусственного интеллекта.
- **Меняющийся ландшафт**: поскольку ландшафт безопасности ИИ продолжает развиваться, организациям, возможно, потребуется постоянно обновлять свои средства контроля и практики

обеспечения безопасности, чтобы оставаться актуальными.

- **Отсутствие конкретных примеров**: DASF предоставляет высокоуровневый обзор рисков безопасности ИИ и средств контроля за их снижением, но в нем отсутствуют конкретные примеры или тематических исследований, иллюстрирующих, как эти риски и средства контроля применяются в реальных сценариях.
- **Фокус на технических рисках**: DASF в первую очередь фокусируется на технических рисках безопасности и средствах контроля за их снижением. Хотя это важный аспект безопасности искусственного интеллекта, организациям следует также учитывать нетехнические риски, такие как этические, юридические и социальные последствия искусственного интеллекта, которые недостаточно подробно рассматриваются в DASF.

D. Связь с индустриальными документами

DASF предназначена для дополнения и интеграции с другими практиками безопасности, такими как NIST, HITRUST, ISO / IEC 27001 и 27002, а также критически важными средствами контроля безопасности CIS. DASF применяет целостный подход к снижению рисков безопасности ИИ вместо того, чтобы сосредотачиваться только на безопасности моделей или конечных точек модели. Такой подход соответствует принципам этих фреймворков, которые обеспечивают структурированный процесс выявления, оценки и снижения рисков безопасности.

E. Фреймворк DASF

Фреймворк подразделяет систему ИИ на 12 основных компонентов, каждый из которых связан с конкретными рисками безопасности, выявленными в результате тщательного анализа. Этот анализ включает прогнозирующие модели ML, генеративные базовые модели и внешние модели, основанные на запросах клиентов, оценках безопасности и т.д. Затем идентифицированные риски сопоставляются с соответствующими средствами контроля в рамках фреймворка анализа данных Databricks со ссылками на подробную документацию продукта по каждому риску.

В документе описываются компоненты системы искусственного интеллекта и связанные с ними риски следующим образом:

- **Операции с данными**: этап включает первоначальную обработку необработанных данных, включая приём, преобразование и обеспечение безопасности данных и управления ими. В общей сложности в этой категории идентифицировано 19 конкретных рисков, начиная от недостаточного контроля доступа и заканчивая отсутствием комплексного управления жизненным циклом ML.
- **Операции с моделями**: этап включает в себя создание моделей ML, будь то путём построения прогнозирующих моделей, приобретения моделей на торговых площадках или использования API, таких как OpenAI. Для этого требуется серия экспериментов и механизмы отслеживания для сравнения различных условий и результатов. Выявлено 14 конкретных рисков, включая такие проблемы, как недостаточная воспроизводимость эксперимента и отклонение модели.
- **Развёртывание и обслуживание модели**: основное внимание уделяется безопасному развёртыванию образов моделей, обслуживанию моделей и управлению такими функциями, как автоматическое масштабирование и ограничение скорости. Всего выделено 15 конкретных рисков, включая оперативный ввод и инверсию модели.
- **Операции и платформа**: заключительный этап включает управление уязвимостями платформы, исправление ошибок, изоляцию модели и обеспечение авторизованного доступа к моделям со встроенной в архитектуру защитой. Это также включает в себя операционный инструментарий для CI / CD для поддержания безопасных MLOP в средах разработки, промежуточных и производственных средах. Определены семь конкретных рисков, таких как отсутствие стандартов MLOP и управление уязвимостями.

F. Необработанные данные

- **Важность необработанных данных**: Необработанные данные являются основой систем ИИ, охватывая корпоративные данные, метаданные и оперативные данные в различных формах, таких как полуструктурированные или неструктурированные данные, пакетные данные или потоковые данные.
- **Безопасность данных**: Защита необработанных данных имеет первостепенное значение для целостности алгоритмов машинного обучения и любых технических деталей развёртывания. Это сопряжено с уникальными проблемами, и весь сбор данных в системе искусственного интеллекта сопряжён как со стандартными проблемами безопасности данных, так и с новыми.
- **Меры по снижению рисков**: описываются конкретные риски, связанные с необработанными данными, и приводятся подробные меры по снижению рисков для каждого из них. Эти средства контроля включают эффективное управление доступом, классификацию данных, обеспечение качества данных, хранение и шифрование, управление версиями данных, происхождение данных, достоверность данных, юридические соображения, обработку устаревших данных и журналов доступа к данным.

- **Управление доступом**: Обеспечение того, чтобы только авторизованные лица или группы могли получить доступ к определённым наборам данных, имеет фундаментальное значение для безопасности данных. Это включает аутентификацию, авторизацию и точно настроенные средства контроля доступа.
- **Классификация данных**: Классификация данных имеет решающее значение для управления, позволяя организациям сортировать и категоризировать данные по степени чувствительности, важности и критичности, что важно для реализации соответствующих мер безопасности и политик управления.
- **Качество данных**: Высокое качество данных имеет решающее значение для принятия надёжных решений на основе данных и является краеугольным камнем управления данными. Организации должны тщательно оценивать ключевые атрибуты данных для обеспечения точности анализа и экономической эффективности.
- **Хранение и шифрование**: Шифрование данных в состоянии покоя и при передаче имеет жизненно важное значение для защиты от несанкционированного доступа и соблюдения отраслевых правил безопасности данных.
- **Управление версиями данных и их происхождение**: Управление версиями данных и отслеживание журналов изменений важны для отката или отслеживания исходных данных в случае повреждения. Data lineage помогает обеспечить соответствие требованиям и готовность к аудиту, обеспечивая чёткое понимание и отслеживаемость данных, используемых для ИИ.
- **Достоверность и юридические аспекты**: Обеспечение достоверности данных и соблюдения юридических требований, таких как GDPR и CCPA, имеет важное значение. Это включает в себя возможность "удалять" определённые данные из систем машинного обучения и переобучать модели, используя чистые наборы данных, подтверждённые владельцами.
- **Устаревшие данные и журналы доступа**: Устранение рисков, связанных с устаревшими данными и отсутствием журналов доступа к данным, важно для поддержания эффективности и безопасности бизнес-процессов. Надлежащие механизмы аудита имеют решающее значение для обеспечения безопасности данных и соблюдения нормативных требований.

G. Подготовка данных

- **Определение и важность**: Подготовка данных определяется как процесс преобразования необработанных входных данных в формат, который могут интерпретировать алгоритмы машинного обучения. Этот этап имеет решающее значение, поскольку он напрямую влияет на безопасность и объяснимость системы ML.
- **Риски безопасности и меры по их устранению**: В разделе описываются различные риски безопасности, связанные с подготовкой данных, и приводятся подробные меры по их устранению для каждого. Эти риски включают целостность предварительной обработки, манипулирование функциями, критерии исходных данных и состязательные разделы.
- **Целостность предварительной обработки**: Обеспечение целостности предварительной обработки включает числовые преобразования, агрегирование данных, кодирование текста или изображений и создание новых функций. Меры по смягчению последствий включают настройку единого входа (SSO) с помощью поставщика идентификационных данных (IdP) и многофакторной аутентификации (MFA), ограничение доступа с использованием списков доступа IP и реализацию частных ссылок для ограничения источника входящих запросов.
- **Манипулирование объектами**: Этот риск связан с возможностью того, что злоумышленники могут манипулировать тем, как данные аннотируются к объектам, что может поставить под угрозу целостность и точность модели. Элементы управления включают защиту функций модели для предотвращения несанкционированных обновлений и использование ориентированных на данные MLOP и LLMOP для продвижения моделей в виде кода.
- **Критерии необработанных данных**: Понимание критериев отбора необработанных данных важно для предотвращения внесения злоумышленниками вредоносного ввода, который ставит под угрозу целостность системы. Элементы управления включают использование списков контроля доступа и ориентированного на данные MLOP для модульного тестирования и интеграции.
- **Состязательные разделы**: это связано с риском того, что злоумышленники повлияют на разделение наборов данных, используемых при обучении и оценке, потенциально косвенно контролируя систему ML. Смягчение последствий включает отслеживание и воспроизведение обучающих данных, используемых для обучения модели ML, и идентификацию моделей ML и запусков, полученных на основе определённого набора данных.
- **Комплексные стратегии смягчения последствий**: В разделе подчёркивается важность комплексного подхода к обеспечению безопасности процесса подготовки данных, включая использование строгих мер безопасности для защиты от манипуляций, которые могут подорвать целостность и надёжность систем ML

H. Наборы данных

- **Значимость наборов данных**: Наборы данных имеют решающее значение для обучения, валидации и тестирования моделей машинного обучения. Ими необходимо тщательно управлять, чтобы обеспечить целостность и эффективность систем искусственного интеллекта.
- **Риски безопасности**: В разделе описываются различные риски безопасности, связанные с наборами данных, включая отравление данных, неэффективное хранение и шифрование, а также переворачивание этикеток. Эти риски могут поставить под угрозу надёжность и производительность моделей машинного обучения.
- **Отравление данными**: Этот риск связан с тем, что злоумышленники манипулируют обучающими данными, чтобы повлиять на выходные данные модели на этапе вывода. Стратегии смягчения последствий включают надёжный контроль доступа, проверки качества данных и мониторинг цепочки данных для предотвращения несанкционированных манипуляций с данными.
- **Неэффективное хранение и шифрование**: Надлежащее хранение и шифрование данных имеют решающее значение для защиты наборов данных от несанкционированного доступа и утечек. Фреймворк рекомендует шифрование данных в состоянии покоя и при передаче, а также строгий контроль доступа.
- **Переключение меток**: Этот специфический тип отравления данными включает изменение меток в обучающих данных, что может ввести модель в заблуждение во время обучения и снизить её производительность. Для снижения этого риска рекомендуется использовать шифрование и безопасный доступ к наборам данных.
- **Меры по смягчению последствий**: для каждого выявленного риска DASF предоставляет подробные меры по смягчению последствий. Эти средства контроля включают использование единого входа (SSO) с поставщиками идентификационных данных (IdP), многофакторной аутентификации (MFA), списков доступа по IP, частных ссылок и шифрования данных для повышения безопасности наборов данных.
- **Комплексное управление рисками**: В этом разделе подчёркивается важность комплексного подхода к управлению безопасностью набора данных, начиная с первоначального сбора данных и заканчивая внедрением моделей машинного обучения. Это включает регулярные аудиты, обновления протоколов безопасности и постоянный мониторинг целостности данных.

I. Управление каталогом данных

- **Комплексный подход к управлению**: Каталог данных и управление включают управление информационными активами организации на протяжении всего их жизненного цикла, что включает принципы, практики и инструменты эффективного управления.
- **Централизованный контроль доступа**: Управление данными и активами искусственного интеллекта обеспечивает централизованный контроль доступа, аудит, происхождение, данные и возможности обнаружения моделей, что ограничивает риск дублирования данных или моделей, ненадлежащего использования секретных данных для обучения, потери происхождения и кражи моделей.
- **Конфиденциальность и безопасность данных**: при работе с наборами данных, которые могут содержать конфиденциальную информацию, крайне важно обеспечить надлежащую защиту личной информации (PII) и других конфиденциальных данных для предотвращения взломов и утечек. Это особенно важно в секторах с жесткими нормативными требованиями.
- **Контрольные журналы и прозрачность**: Надлежащее управление каталогом данных позволяет проводить контрольные журналы и отслеживать происхождение и преобразования данных, используемых для обучения моделей искусственного интеллекта. Такая прозрачность способствует укреплению доверия и подотчётности, снижает риск предвзятости и улучшает результаты искусственного интеллекта.
- **Соответствие нормативным требованиям**: Обеспечение надлежащей защиты конфиденциальной информации в наборах данных имеет важное значение для соблюдения таких нормативных актов, как GDPR и CCPA. Это включает в себя возможность демонстрировать безопасность данных и вести журналы аудита.
- **Панель мониторинга совместной работы**: для проектов компьютерного зрения с участием нескольких заинтересованных сторон наличие простого в использовании инструмента маркировки с панелью мониторинга совместной работы важно для того, чтобы все были в курсе событий в режиме реального времени и не допускали искажения миссии.
- **Автоматизированные конвейеры данных**: для проектов с большими объемами данных автоматизация конвейеров данных путём подключения наборов данных и моделей с помощью API может упростить процесс и ускорить обучение моделей ML.
- **Рабочие процессы контроля качества**: важно иметь настраиваемые и управляемые рабочие

процессы контроля качества для проверки меток и аннотаций, уменьшения ошибок и предвзятости, а также исправления ошибок в наборах данных. Автоматизированные инструменты аннотирования могут помочь в этом процессе

J. Алгоритмы машинного обучения

- **Техническое ядро систем ML**: Алгоритмы машинного обучения описываются как техническое ядро любой системы ML, имеющее решающее значение для функциональности и безопасности системы.
- **Меньший риск для безопасности**: отмечается, что атаки на алгоритмы машинного обучения обычно представляют значительно меньший риск для безопасности по сравнению с данными, используемыми для обучения, тестирования и последующей эксплуатации.
- **Автономные и онлайновые системы**: В этом разделе проводится различие между автономными и онлайновыми алгоритмами машинного обучения. Автономные системы обучаются на фиксированном наборе данных и затем используются для прогнозирования, в то время как онлайн-системы постоянно обучаются и адаптируются посредством итеративного обучения с новыми данными.
- **Преимущества автономных систем в плане безопасности**: считается, что автономные системы обладают определёнными преимуществами в плане безопасности из-за их фиксированного, статичного характера, который уменьшает поверхность атаки и со временем сводит к минимуму подверженность уязвимостям, связанным с данными.
- **Уязвимости онлайн-систем**: Онлайн-системы постоянно подвергаются воздействию новых данных, что повышает их восприимчивость к атакам отравления, состязательному вводу данных и манипулированию процессами обучения.
- **Тщательный выбор алгоритмов**: подчёркивается важность тщательного рассмотрения выбора между автономными и онлайн-алгоритмами обучения на основе конкретных требований безопасности и операционной среды системы ML

K. Оценка

- **Критическая роль оценки**: Оценка необходима для оценки эффективности систем машинного обучения в достижении их предполагаемых функциональных возможностей. Это включает в себя использование выделенных наборов данных для систематического анализа производительности обученной модели с учётом её конкретной задачи.
- **Отравление оценочных данных**: существует риск атак на данные, когда данные подделываются перед их использованием для машинного обучения, что значительно усложняет обучение и оценку моделей ML. Эти атаки могут повредить или изменить данные таким образом, что исказит процесс обучения, что приведёт к созданию ненадёжных моделей.
- **Неполнота данных для оценки**: Наборы данных для оценки также могут быть слишком маленькими или слишком похожими на данные для обучения, чтобы быть полезными. Некачественные оценочные данные могут привести к предвзятости, галлюцинациям и токсическому эффекту. Трудно эффективно оценивать большие языковые модели (LLM), поскольку эти модели редко имеют маркировку объективной истинности.
- **Меры по смягчению последствий**:
  - Внедрение единого входа (SSO) с поставщиком идентификационных данных (IdP) и многофакторной аутентификации (MFA) для ограничения доступа к данным и платформе искусственного интеллекта.
  - Использование списков IP-доступа для ограничения IP-адресов, которые могут проходить аутентификацию в Databricks.
  - Шифрование данных в состоянии покоя и при передаче.
  - Отслеживать изменения в данных и системе искусственного интеллекта с помощью единого окна и принимать меры при возникновении изменений.
- **Важность надёжной оценки**: Эффективная оценка имеет решающее значение для обеспечения надёжности и точности моделей машинного обучения. Это помогает выявить расхождения или аномалии в процессе принятия решений в модели и даёт представление о производительности модели.

L. Модели машинного обучения

- **Безопасность модели**: Модели машинного обучения являются ядром систем ИИ, и их безопасность имеет решающее значение для обеспечения целостности и надёжности системы. В этом разделе обсуждаются различные риски, связанные с моделями машинного обучения, и предлагаются меры по снижению каждого риска.
- **Бэкдорное машинное обучение / Троянская модель**: риск связан с внедрением злоумышленником бэкдора в модель во время обучения, который может быть использован позже для манипулирования поведением модели. Меры по смягчению последствий включают мониторинг производительности модели, использование надёжных обучающих данных и внедрение средств контроля доступа.
- **Утечка ресурсов модели**: риск связан с несанкционированным раскрытием ресурсов модели, таких как архитектура модели, веса и

обучающие данные. Меры по смягчению последствий включают шифрование, контроль доступа и мониторинг на предмет несанкционированного доступа.

- **Уязвимости цепочки поставок ML**: риск возникает из-за уязвимостей в цепочке поставок ML, таких как библиотеки сторонних производителей и зависимости. Меры по смягчению последствий включают регулярные оценки уязвимостей, использование надёжных источников и внедрение безопасных методов разработки.
- **Атака под контролем исходного кода**: риск связан с получением несанкционированного доступа к хранилищу исходного кода и модификацией кода для внедрения уязвимостей или бэкдоров. Меры по смягчению последствий включают контроль доступа, проверку кода и мониторинг на предмет несанкционированного доступа.
- **Указание принадлежности к модели**: риск связан с несанкционированным использованием модели без надлежащего указания принадлежности к её первоначальным создателям. Меры по смягчению последствий включают использование цифровых водяных знаков, ведение надлежащей документации и обеспечение соблюдения лицензионных соглашений.
- **Кража модели**: риск связан с кражей злоумышленником модели путём реверс-инжиниринга её поведения или прямого доступа к её коду. Меры по смягчению последствий включают шифрование, контроль доступа и мониторинг на предмет несанкционированного доступа.
- **Жизненный цикл модели без HITL**: риск возникает из-за отсутствия участия человека в цикле (HITL) в жизненном цикле модели, что может привести к предвзятым или неверным прогнозам. Меры по смягчению последствий включают регулярную валидацию модели, анализ со стороны персонала и непрерывный мониторинг.
- **Инверсия модели**: риск связан с тем, что злоумышленник получает конфиденциальную информацию об обучающих данных путём анализа поведения модели. Меры по смягчению последствий включают использование дифференцированной конфиденциальности, контроль доступа и мониторинг на предмет несанкционированного доступа.

M. Управление моделями

- **Управление моделями**: Управление моделями — это процесс организации, отслеживания и поддержки моделей машинного обучения на протяжении всего их жизненного цикла, от разработки до развёртывания и вывода из эксплуатации.
- **Риски безопасности**: риски безопасности связаны с управлением моделями, включая атрибуцию модели, кражу модели, жизненный цикл модели без участия человека в цикле (HITL) и инверсию модели.
- **Указание принадлежности к модели**: риск связан с несанкционированным использованием модели без надлежащего указания принадлежности к её первоначальным создателям. Меры по смягчению последствий включают использование цифровых водяных знаков, ведение надлежащей документации и обеспечение соблюдения лицензионных соглашений.
- **Кража модели**: риск связан с кражей злоумышленником модели путём реверс-инжиниринга её поведения или прямого доступа к её коду. Меры по смягчению последствий включают шифрование, контроль доступа и мониторинг на предмет несанкционированного доступа.
- **Жизненный цикл модели без HITL**: риск возникает из-за отсутствия участия человека в цикле (HITL) в жизненном цикле модели, что может привести к предвзятым или неверным прогнозам. Меры по смягчению последствий включают регулярную валидацию модели, анализ со стороны персонала и непрерывный мониторинг.
- **Инверсия модели**: риск связан с тем, что злоумышленник получает конфиденциальную информацию об обучающих данных путём анализа поведения модели. Меры по смягчению последствий включают использование дифференцированной конфиденциальности, контроль доступа и мониторинг на предмет несанкционированного доступа.

N. Запросы на обслуживание моделей

- **Обслуживание модели**: Обслуживание модели – это процесс развёртывания обученной модели машинного обучения в производственной среде для генерации прогнозов на основе новых данных.
- **Запросы на вывод**: Запросы на вывод — это входные данные, отправляемые в развёрнутую модель для генерации прогнозов.
- **Риски безопасности**: различные риски безопасности, связанные с обслуживанием модели и запросами вывода, включая оперативный ввод, инверсию модели, прерывание модели, циклический ввод, определение принадлежности к обучающим данным, обнаружение онтологии модели ML, отказ в обслуживании (DoS), галлюцинации LLM, контроль входных ресурсов и случайное попадание неавторизованных данных в модели.
- **Оперативное внедрение**: Этот риск связан с тем, что злоумышленник вводит вредоносный ввод в

модель для манипулирования её поведением или извлечения конфиденциальной информации.

- **Инверсия модели**: Этот риск связан с попыткой злоумышленника восстановить исходные обучающие данные или конфиденциальные функции путём наблюдения за выходными данными модели.
- **Нарушение модели**: Этот риск связан с использованием злоумышленником уязвимостей в среде, обслуживающей модель, для получения несанкционированного доступа к базовой системе или данным.
- **Циклический ввод**: Этот риск связан с тем, что злоумышленник вводит повторяющийся или закольцованный ввод в модель, что приводит к исчерпанию ресурсов или снижению производительности системы.
- **Определение принадлежности к обучающим данным**: Этот риск связан с попыткой злоумышленника определить, использовалась ли конкретная точка данных в обучающих данных модели.
- **Обнаружение онтологии модели ML**: Этот риск связан с попыткой злоумышленника извлечь информацию о внутренней структуре или функциональности модели.
- **Отказ в обслуживании (DoS)**: Этот риск связан с тем, что злоумышленник отправляет большой объем запросов на вывод, чтобы перегрузить инфраструктуру, обслуживающую модель, и вызвать перебои в обслуживании.
- **Галлюцинации LLM**: Этот риск связан с тем, что модель генерирует неверные или вводящие в заблуждение выходные данные из-за присущей ей неопределённости или ограничений базовых алгоритмов.
- **Контроль входных ресурсов**: Этот риск связан с тем, что злоумышленник манипулирует входными данными для использования чрезмерных ресурсов в процессе вывода.
- **Случайное предоставление неавторизованных данных моделям**: Этот риск связан с непреднамеренным предоставлением конфиденциальных или неавторизованных данных модели в процессе вывода.
- **Меры по смягчению последствий**: для каждого выявленного риска DASF предоставляет подробные меры по смягчению последствий. Эти средства контроля включают использование единого входа (SSO) с поставщиками идентификационных данных (IdP), многофакторной аутентификации (MFA), списков доступа по IP, частных ссылок и шифрования данных для повышения безопасности обслуживания модели и вывода запросов

O. Обслуживание модели

- **Обслуживание модели**: Обслуживание модели — это процесс развёртывания обученной модели машинного обучения в производственной среде для генерации прогнозов на основе новых данных.
- **«Ответ на логический вывод»**: относится к выходным данным, генерируемым развёрнутой моделью в ответ на входные данные, отправленные для прогнозирования.
- **Риски безопасности**: различные риски безопасности, связанные с обслуживанием модели, включая отсутствие аудита и мониторинга качества вывода, манипулирование выводом, обнаружение онтологии модели ML, обнаружение семейства моделей ML и атаки с использованием черного ящика.
- **Недостаточное качество аудита и мониторинга выводов**: риск связан с отсутствием надлежащих механизмов мониторинга и аудита для обеспечения качества и точности прогнозов модели.
- **Манипулирование выходными данными**: риск связан с тем, что злоумышленник манипулирует выходными данными модели для получения неверных или вводящих в заблуждение прогнозов.
- **Обнаружение онтологии модели ML**: риск связан с попыткой злоумышленника извлечь информацию о внутренней структуре или функциональности модели путём анализа выходных данных.
- **Обнаружение семейства моделей ML**: риск связан с попыткой злоумышленника идентифицировать конкретный тип или семейство моделей, используемых в системе, путём анализа выходных данных.
- **Атаки с использованием черного ящика**: риск связан с тем, что злоумышленник использует уязвимости модели, рассматривая её как черный ящик и манипулируя входными данными для получения желаемых результатов.
- **Меры по смягчению последствий**: для каждого выявленного риска DASF предоставляет подробные меры по смягчению последствий. Эти средства контроля включают использование единого входа (SSO) с поставщиками идентификационных данных (IdP), многофакторной аутентификации (MFA), списков доступа по IP, частных ссылок и шифрования данных для повышения безопасности обслуживания модели и вывода ответа

P. Машинное обучение (MLOps)

- **MLOps Определение**: MLOps – это практика объединения машинного обучения (ML), DevOps и разработки данных для автоматизации и стандартизации процесса развёртывания, обслуживания и обновления моделей ML в производственных средах.

- **Риски безопасности**: различные риски безопасности, связанные с MLOP, включая отсутствие MLOP, повторяющиеся принудительные стандарты и несоответствие требованиям.
- **Отсутствие MLOP**: риск связан с отсутствием стандартизированного и автоматизированного процесса развёртывания, обслуживания и обновления моделей ML, что может привести к несоответствиям, ошибкам и уязвимостям в системе безопасности.
- **Стандарты**: Соблюдение стандартов имеет решающее значение для обеспечения безопасности и надёжности моделей ML в производственных средах. Это включает внедрение системы контроля версий, автоматизированного тестирования и конвейеров непрерывной интеграции и развёртывания (CI / CD).
- **Несоблюдение требований**: риск связан с несоблюдением соответствующих нормативных актов и отраслевых стандартов, что может привести к юридическим и финансовым последствиям для организации.
- **Меры по смягчению последствий**: для каждого выявленного риска DASF предоставляет подробные меры по смягчению последствий. Эти средства контроля включают использование единого входа (SSO) с поставщиками идентификационных данных (IdP), многофакторной аутентификации (MFA), списков доступа по IP, частных ссылок и шифрования данных для повышения безопасности MLOP

Q. Безопасность данных и платформы ИИ

- **Неотъемлемые риски и выгоды**: Выбор платформы, используемой для создания и развёртывания моделей ИИ, может иметь неотъемлемые риски и выгоды. Реальные данные свидетельствуют о том, что злоумышленники часто используют простые тактики для компрометации систем, основанных на ML.
- **Отсутствие реагирования на инциденты**: Приложения AI / ML критически важны для бизнеса, и поставщики платформ должны быстро и эффективно решать проблемы безопасности. Рекомендуется сочетание автоматического мониторинга и ручного анализа для устранения общих угроз и угроз, специфичных для ML (DASF 39 Platform security — Incident Response Team).
- **Несанкционированный привилегированный доступ**: Внутренние злоумышленники, такие как сотрудники или подрядчики, могут представлять серьёзную угрозу безопасности. Они могут получить несанкционированный доступ к частным учебным данным или ML-моделям, что приведёт к утечке конфиденциальной информации, злоупотреблениям бизнес-процессами и потенциальному саботажу ML-систем. Внедрение строгих мер внутренней безопасности и протоколов мониторинга имеет решающее значение для снижения инсайдерских рисков (Безопасность платформы DASF 40 — внутренний доступ).
- **Низкий уровень безопасности в жизненном цикле разработки ПО (SDLC)**: Безопасность программной платформы является важной частью любой прогрессивной программы обеспечения безопасности. Хакеры часто используют ошибки в платформе, на которой построен ИИ. Безопасность ИИ зависит от безопасности платформы (DASF 41 Platform security — secure SDLC).
- **Несоблюдение требований**: По мере того, как приложения с ИИ становятся все более распространёнными, они становятся все более объектом пристального внимания и нормативных актов, таких как GDPR и CCPA. Использование сертифицированной платформы может стать значительным преимуществом для организаций, поскольку эти платформы специально разработаны для соответствия нормативным стандартам и предоставляют необходимые инструменты и ресурсы, помогающие организациям создавать и развёртывать приложения ИИ, соответствующие этим требованиям

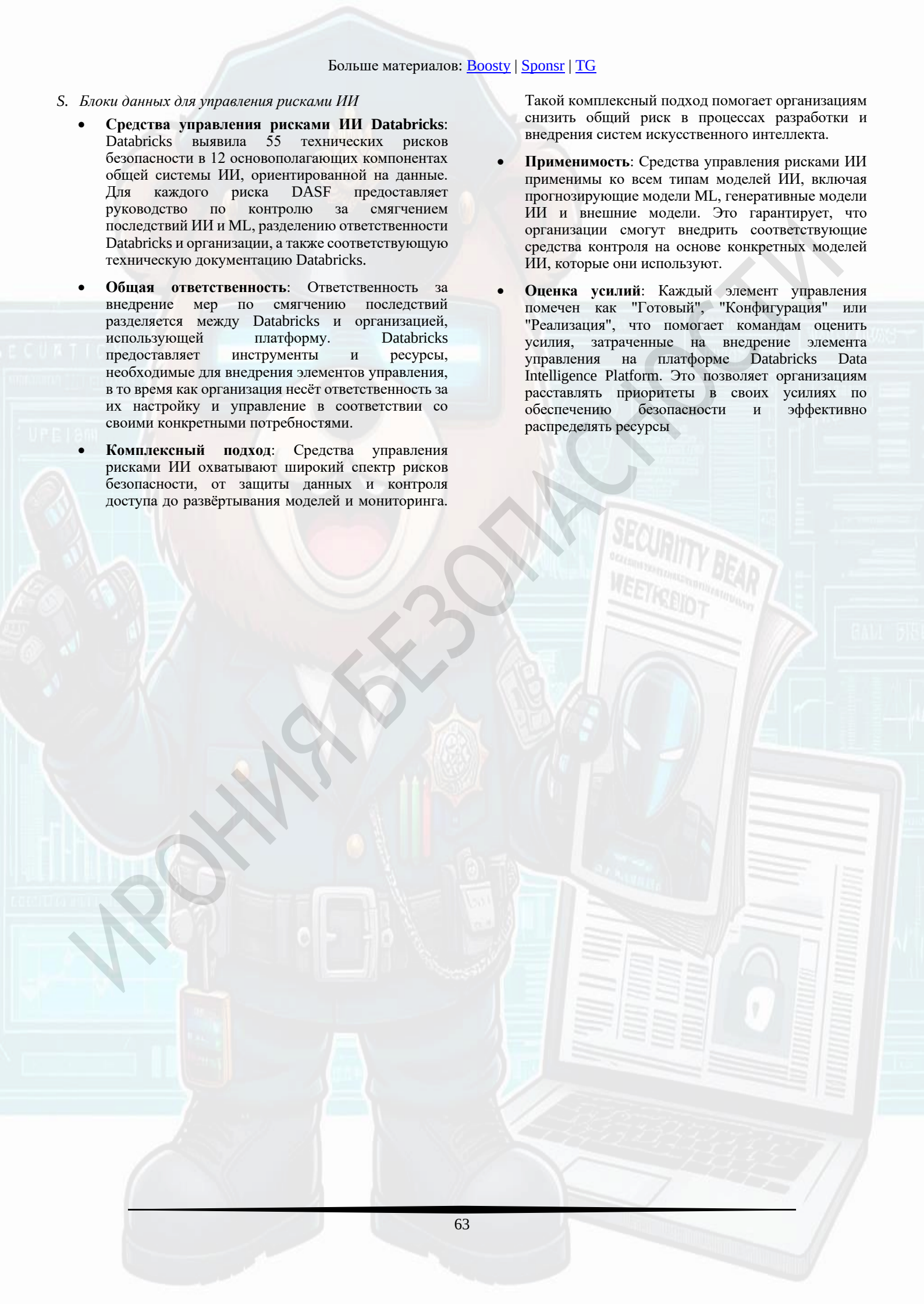
R. Фреймворк сбора данных Databricks

Databricks Data Intelligence Platform — это комплексное решение для ИИ и управления данными.

- **Mosaic AI:** компонент платформы охватывает комплексный рабочий процесс искусственного интеллекта, от подготовки данных до развёртывания модели и мониторинга.
- **Каталог Unity**: унифицированное решение для управления данными и активами искусственного интеллекта. Он обеспечивает обнаружение данных, их привязку и детальный контроль доступа.
- **Архитектура**: представляет собой гибридный PaaS, не зависящий от данных и поддерживающий широкий спектр типов данных и источников.
- **Безопасность**: Безопасность платформы основана на принципах доверия, технологии и прозрачности. Он включает в себя такие функции, как шифрование, контроль доступа и мониторинг.
- **Средства контроля за снижением рисков ИИ**: Databricks выявила 55 технических рисков безопасности в 12 основополагающих компонентах общей системы ИИ, ориентированной на данные. Для каждого риска фреймворк предоставляет руководство по контролю за смягчением последствий с помощью ИИ и ML, общую ответственность Databricks и организации, а также соответствующую техническую документацию Databricks.

S. *Блоки данных для управления рисками ИИ*

- **Средства управления рисками ИИ Databricks**: Databricks выявила 55 технических рисков безопасности в 12 основополагающих компонентах общей системы ИИ, ориентированной на данные. Для каждого риска DASF предоставляет руководство по контролю за смягчением последствий ИИ и ML, разделению ответственности Databricks и организации, а также соответствующую техническую документацию Databricks.
- **Общая ответственность**: Ответственность за внедрение мер по смягчению последствий разделяется между Databricks и организацией, использующей платформу. Databricks предоставляет инструменты и ресурсы, необходимые для внедрения элементов управления, в то время как организация несёт ответственность за их настройку и управление в соответствии со своими конкретными потребностями.
- **Комплексный подход**: Средства управления рисками ИИ охватывают широкий спектр рисков безопасности, от защиты данных и контроля доступа до развёртывания моделей и мониторинга. Такой комплексный подход помогает организациям снизить общий риск в процессах разработки и внедрения систем искусственного интеллекта.
- **Применимость**: Средства управления рисками ИИ применимы ко всем типам моделей ИИ, включая прогнозирующие модели ML, генеративные модели ИИ и внешние модели. Это гарантирует, что организации смогут внедрить соответствующие средства контроля на основе конкретных моделей ИИ, которые они используют.
- **Оценка усилий**: Каждый элемент управления помечен как "Готовый", "Конфигурация" или "Реализация", что помогает командам оценить усилия, затраченные на внедрение элемента управления на платформе Databricks Data Intelligence Platform. Это позволяет организациям расставлять приоритеты в своих усилиях по обеспечению безопасности и эффективно распределять ресурсы



ПАТЕНТ US11611582B2

Аннотация – В этом документе представлен анализ патента US11611582B2, описывающего компьютерный метод обнаружения фишинговых угроз. Анализ охватывает различные аспекты патента, включая его технические детали, потенциальные области применения и последствия для специалистов по кибербезопасности и других секторов промышленности.

Актуальность для развивающегося ландшафта DevSecOps подчёркивает вклад в более безопасные и эффективные жизненные циклы разработки программного обеспечения, поскольку патент предлагает методический подход к обнаружению фишинга, который может быть применён различными инструментами и сервисами для защиты пользователей и организаций от вредоносных действий в Интернете. Специалистам по кибербезопасности следует рассмотреть возможность включения таких методов в свои стратегии защиты для упреждения возникающих угроз.

A. Введение

Патент US20220232015A1 описывает способ динамического обнаружения фишинговых угроз с использованием заранее определённой статистической модели. Метод основан на машинном обучении и позволяет анализировать сетевые запросы в режиме реального времени и выявлять потенциальные попытки фишинга, чтобы проактивно защищать пользователей и системы от таких атак. Статистическая модель и набор признаков позволяют адаптироваться к новым фишинговым схемам.

B. Основная идея

Основная идея патента заключается в предоставлении масштабируемого и автоматизированного подхода к обнаружению попыток фишинга в режиме реального времени с использованием машинного обучения с целью упреждающей защиты пользователей от становления жертвами все более изощренных фишинговых атак. Динамический анализ атрибутов веб-запросов позволяет выявлять новые фишинговые сайты, которые могут отсутствовать в статических списках.

- Описывается реализованный метод динамического обнаружения фишинговых угроз с использованием заранее определённой статистической модели. Цель состоит в том, чтобы в режиме реального времени определить, представляет ли запрашиваемый сетевой ресурс потенциальную угрозу фишинга.
- При получении запроса на доступ к сетевому ресурсу извлекается набор признаков, связанных с запросом. Эти характеристики могут включать доменное имя, возраст домена, его регистратор, IP-адрес, географическое местоположение и т.д.
- Извлечённые характеристики загружаются в предварительно обученную модель, которая выдаёт оценку вероятности того, что запрошенный ресурс представляет собой фишинговую угрозу. Если оценка превышает заранее определённый порог, формируется оповещение.
- Модель обучается на наборах данных, содержащих известные фишинговые и нефишинговые примеры с периодическим обновлением данных.

C. Область применения

Конкретные детали реализации и точки интеграции будут варьироваться в зависимости от требований каждой отрасли и существующего технологического стека. Однако основные возможности динамического обнаружения фишинга с использованием машинного обучения могут быть адаптированы для обеспечения значительных преимуществ в области безопасности в широком спектре секторов, сталкивающихся с растущей угрозой фишинговых атак.

1) Телекоммуникации:

Телекоммуникационные компании могут интегрировать систему обнаружения фишинга в свою сетевую инфраструктуру для защиты клиентов от атак, осуществляемых с помощью SMS, MMS или других служб обмена сообщениями.

Возможности обнаружения в режиме реального времени помогут блокировать фишинговые ссылки до того, как они дойдут до конечных пользователей, снижая риск взлома учётной записи и кражи личных данных.

Телекоммуникационные провайдеры могут предлагать защиту от фишинга в качестве дополнительной услуги, позволяющей выделиться на рынке и завоевать доверие клиентов.

2) Информационные технологии:

ИТ-компании могут внедрять решение для обнаружения фишинга в рамках своих предложений по безопасности для клиентов, помогая защитить от атак, нацеленных на сотрудников и клиентов.

Поставщики услуг управляемой безопасности (MSSP) интегрируют эту технологию в свои службы мониторинга угроз и реагирования на инциденты, чтобы обнаруживать и блокировать попытки фишинга в режиме реального времени.

Поставщики программного обеспечения как услуги (SaaS) могут встроить функцию обнаружения фишинга в свои платформы для сканирования подозрительных URL-адресов и вложений, повышая безопасность своих приложений.

3) Финансовый сектор:

Финансовые учреждения могут использовать систему обнаружения фишинга для защиты своих клиентов от целенаправленных фишинговых атак, направленных на кражу учётных данных для входа в систему, номеров кредитных карт и других конфиденциальных финансовых данных.

Решение может быть интегрировано в платформы онлайн-банкинга, мобильные приложения и системы электронной почты для сканирования и выявления потенциальных попыток фишинга в режиме реального времени.

Благодаря активному обнаружению и блокированию фишинговых угроз финансовые компании снизят потери от мошенничества, сохранить доверие клиентов и соблюдать нормативные требования по защите данных.

4) Здравоохранение:

Организации здравоохранения могут использовать технологию обнаружения фишинга для защиты конфиденциальных данных пациентов и предотвращения фишинговых атак, которые могут поставить под угрозу конфиденциальность, целостность и доступность систем здравоохранения.

Решение может быть развёрнуто для мониторинга сообщений электронной почты, порталов пациентов и других цифровых каналов на предмет признаков попыток фишинга, нацеленных на медицинский персонал или пациентов.

Обнаруживая и блокируя фишинговые угрозы, поставщики медицинских услуг могут снизят риск утечки данных, защитить конфиденциальность пациентов и обеспечить непрерывность критически важных медуслуг.

5) Электронная коммерция:

Интернет-магазины могут интегрировать возможности обнаружения фишинга в свои платформы электронной коммерции, чтобы защитить клиентов от фишинговых атак, которые приведут к захвату аккаунта, мошенническим транзакциям и краже личных данных.

Обнаружение в режиме реального времени может помочь идентифицировать и блокировать попытки фишинга, отправляемые с помощью поддельных электронных писем с подтверждением заказа, запросов на верификацию учётной записи или в службу поддержки клиентов.

Активно противодействуя фишинговым угрозам, компании электронной коммерции смогут поддерживать доверие клиентов, сокращать возвратные платежи и потери от мошенничества, а также защищать репутацию бренда.

D. Предлагаемое решение

Ключевыми аспектами являются извлечение релевантных артефактов из веб-запросов, использование обученной статистической модели для оценки запросов, обновление модели с течением времени и формирование предупреждений, когда оценка превышает пороговое значение. Ключевыми компонентами являются:

Извлечение признаков:

- При получении запроса на доступ к сетевому ресурсу извлекается набор признаков, связанных с запросом.
- Эти признаки могут включать полное доменное имя (FQDN), возраст домена, регистратора домена, IP-адрес, географическое местоположение и т.д.
- Извлечение признаков позволяет представить ключевые атрибуты веб-запроса, которые могут указать, является ли он потенциальной попыткой фишинга.

Статистическая модель:

- Извлечённые признаки вводятся в предварительно обученную статистическую модель, которая выдаёт оценку вероятности.
- Модель обучается с использованием методов машинного обучения на наборах данных, содержащих известные фишинговые и нефишинговые примеры.
- Могут использоваться различные модели ML, такие как логистическая регрессия, деревья принятия решений, нейронные сети и т.д.
- Модель распознает шаблоны и комбинации значений признаков, указывающие на фишинг.

Обучение и обновление модели:

- Статистическая модель изначально обучается на помеченном наборе данных перед развёртыванием.
- Набор периодически обновляется с использованием новых обучающих данных, чтобы адаптироваться к развивающимся моделям фишинга.
- Обновление модели позволяет ей распознавать новые методы фишинга и сохранять точность с течением времени.

Установление порогового значения и формирование предупреждений:

- Результатом работы модели является оценка вероятности того, что веб-запрос является попыткой фишинга.
- Если оценка превышает заранее определённый порог, генерируется оповещение.
- Пороговое значение может быть скорректировано для настройки чувствительности системы на основе желаемого соотношения частоты ложноположительных и ложноотрицательных срабатываний.

- Могут быть предприняты защитные действия, такие как блокировка веб-запроса при срабатывании оповещения.

E. Технологический процесс

Технологический процесс охватывает полный жизненный цикл предлагаемой системы обнаружения фишинга, от первоначального сбора данных и разработки модели до развёртывания в режиме реального времени, формирования предупреждений и непрерывного обновления модели. Ключевыми этапами являются извлечение признаков, обучение и оценка модели, оценка сетевых запросов в режиме реального времени, формирование предупреждений и ответов, а также периодическая переподготовка модели для адаптации к меняющимся тактикам фишинга.

Сбор и предварительная обработка данных:

- Сбор набор данных известных фишинговых и легитимных запросов к сетевым ресурсам.
- Предварительная обработка необработанных данных запроса для извлечения соответствующих признаков, таких как URL, возраст домена, регистратор, IP-адрес, географическое местоположение и т.д.
- Разметка запроса на фишинговый или безвредный.

Извлечение признаков:

- Определение набора отличительных признаков, которые могут отличить попытки фишинга от легнтимных запросов, на основе знаний предметной области и предварительных исследований.
- Реализация логики извлечения объектов для анализа соответствующих атрибутов из предварительно обработанных данных запроса.
- Преобразование извлечённых значений признаков в подходящий формат (например, числовые векторы) для ввода в модель машинного обучения.

Обучение модели:

- Выбор алгоритма машинного обучения для задачи классификации фишинга (например, случайный лес, SVM, нейронные сети).
- Разделение наборов данных на обучающие и тестирующие подмножества.
- Обучение выбранной модели на шаблонах, которые сопоставляют входные признаки с фишинговыми / вредоносными метками.
- Настройка параметров модели с помощью таких методов, как перекрёстная проверка, для оптимизации производительности.

Оценка модели:

- Оценка производительности обученной модели на длительном тестировании.
- Расчёт оценочных показателей, например точности, прецизионности, F1-параметра и т.д.
- Анализ производительности модели для оценки её эффективность в обнаружении попыток фишинга и определения области для улучшения.

Развёртывание модели:

- Интеграция обученной модели обнаружения фишинга в систему оперативного сетевого мониторинга.
- Извлечение признаков (характеристик) из входящих сетевых запросов в режиме реального времени.
- Применение модели к признакам каждого запроса, чтобы получить оценку вероятности фишинга.
- Сравнение полученного значения с заданным пороговым, чтобы классифицировать запрос как фишинговый или доброкачественный.

Формирование оповещений и реагирование на них:

- Если показатель фишинг-запроса превышает пороговое значение, формируется оповещение с соответствующими сведениями, такими как URL, IP источника, оценка риска и т.д.
- Доставка оповещения группам безопасности по соответствующим каналам, таким как электронная почта, SMS, интеграция SIEM и т.д.
- Запуск автоматических ответных действий в зависимости от серьёзности предупреждения, такие как блокировка запроса или помещение связанного сетевого трафика на карантин.
- Проведение ручного расследования и исправления высокоприоритетных событий ИБ-аналитиками.

Обновление модели:

- Накопление и сбор новых примеров фишинговых и вредоносных запросов в рабочей среде.
- Переобучение модели обнаружения фишинга на обновлённом наборе данных.
- Оценка производительности обновлённой модели и развёртывание для замены существующей модели в случае выявления повышенной точности.
- Отслеживание прогнозов модели с течением времени для обнаружения отклонения от значений или снижение производительности, которые могут потребовать дальнейших обновлений.

F. Извлечение признаков

Извлечение признаков является ключевым этапом процесса обнаружения фишинга. Оно включает в себя идентификацию и выбор соответствующих характеристик или атрибутов из необработанных данных запроса сетевого ресурса. Извлечённые характеристики, такие как полное доменное имя, возраст домена, регистратор, IP-адрес и

местоположение, служат входными данными для статистической модели динамической оценки риска фишинга.

Цель состоит в том, чтобы преобразовать данные запроса в набор информативных характеристик, которые могут быть введены в статистическую модель для определения того, является ли запрос потенциально вредоносным.

- **Полное доменное имя (FQDN)**: полное доменное имя запрашиваемого ресурса, которое включает имя хоста, поддомен (при наличии), домен второго уровня и домен верхнего уровня (TLD). Например, "mail.example.com" — это полное доменное имя, где "mail" — это имя хоста, "example" — это домен второго уровня, а ".com" — это TLD.
- **Возраст домена**: относится к тому, как давно было зарегистрировано доменное имя. Недавно зарегистрированные домены с большей вероятностью будут связаны с попытками фишинга.
- **Регистратор домена**: организация, через которую было зарегистрировано доменное имя. Определённые регистраторы могут чаще использоваться фишинговыми сайтами.
- **IP-адрес**: числовая метка, присвоенная серверу, на котором размещён запрашиваемый ресурс.
- **Географическое местоположение**: физическое местоположение сервера на основе его IP-адреса. Запросы, исходящие из неожиданных географических регионов, могут указывать на более высокий риск фишинга.

Извлечение этих составных-признаков позволяет представить ключевые элементы запроса в структурированном формате, который может быть проанализирован с помощью статистической модели. Значения признаков преобразуются и нормализуются, чтобы сделать их пригодными для ввода в алгоритм машинного обучения.

Дополнительные признаки могут также быть извлечены в зависимости от конкретной реализации. Процесс извлечения признаков, по сути, преобразует необработанные данные запроса в вектор релевантных атрибутов, которые кратко отражают информацию, необходимую для оценки риска фишинга.

Путём тщательной разработки и выбора признаков можно оптимизировать точность и эффективность последующей модели обнаружения фишинга. Выделенные признаки предназначены для сбора шаблонов и сигналов, которые отличают легитимные запросы от попыток фишинга на основе домена, сервера и характеристик запроса.

G. Статистическая модель

Статистическая модель является ключевым элементом динамической системы обнаружения фишинга. Он принимает извлечённые характеристики запроса сетевого ресурса в качестве входных данных и выводит оценку вероятности, указывающую на вероятность того, что запрошенный ресурс представляет собой угрозу фишинга.

Тип модели: предлагается использовать ML-методы для обучения статистической модели, в частности, упоминается метод случайного леса как одна из возможных реализаций. Метод случайного леса — это метод коллективного обучения, который создаёт несколько деревьев решений и выводит класс, который является способом вывода классов отдельными деревьями. Он известен своей способностью хорошо обобщать новые данные.

Входные данные модели: входными данными для модели является набор признаков, извлечённых из запроса сетевого ресурса, таких как полное доменное имя, возраст домена, регистратор, IP-адрес, географическое местоположение и т.д. Эти объекты преобразуются и нормализуются в подходящий формат (например, вектор объектов) перед загрузкой в модель.

Выходные данные модели: выходные данные модели представляют собой оценку вероятности от 0 до 1, которая предполагает вероятность того, что запрошенный ресурс является попыткой фишинга. Если оценка превышает заранее установленный порог (например, 0,8), ресурс классифицируется как потенциальная угроза фишинга.

Обучение модели: Статистическая модель обучается на наборе данных, содержащем примеры известных фишинговых и нефишинговых (доброкачественных) сетевых ресурсов. Модель учится распознавать шаблоны и комбинации значений признаков, указывающих на фишинг. Алгоритм случайного леса корректирует параметры модели, чтобы свести к минимуму ошибки неправильной классификации.

Оценка модели: производительность обученной модели оценивается с использованием таких показателей, как точность, прецизионность, оценка F1 и т.д., в отдельном наборе тестов. Это помогает понять, насколько хорошо модель обобщается на невидимые данные, и направляет выбор модели и настройку параметров.

Обновление модели: для адаптации к меняющимся тактикам фишинга статистическую модель можно периодически переподготовлять с использованием новых помеченных данных. Это позволяет модели изучать новые шаблоны и сохранять свою точность с течением времени по мере изменения характеристик попыток фишинга.

Статистическая модель представляет собой классификатор машинного обучения, лежащий в основе динамической системы обнаружения фишинга. Она обучена прогнозировать вероятность того, что сетевой ресурс представляет собой фишинговую угрозу, на основе его выделенных характеристик. Архитектура модели, процедура обучения и стратегия обновления разработаны таким образом, чтобы обеспечить точное, адаптивное выявление попыток фишинга в режиме реального времени.

Использование статистического подхода, основанного на данных, позволяет системе извлекать сложные

закономерности из исторических данных о фишинге и обобщать их для обнаружения новых, ранее невиданных попыток. Это обеспечивает более динамичную и надёжную защиту по сравнению со статическими методами, основанными на правилах.

H. Обучение и обновление модели

Обучение и обновление модели относятся к процессам первоначального построения статистической модели на основе обучающего набора данных и последующего её уточнения с течением времени по мере поступления новых данных. Это важнейшая часть конвейера машинного обучения, которая позволяет системе обнаружения фишинга адаптироваться и поддерживать точность перед лицом возникающих угроз.

Начальное обучение модели:

- Перед развёртыванием статистическая модель (например, классификатор случайного леса) обучается на помеченном наборе данных, содержащем примеры известных фишинговых и вредоносных запросов к сетевым ресурсам.
- Каждый обучающий пример состоит из извлечённых признаков (полное доменное имя, возраст домена, регистратор, IP, местоположение и т.д.) и соответствующего ярлыка (фишинговый или вредоносный).
- Во время обучения модель учится распознавать шаблоны и комбинации значений признаков, которые отличают попытки фишинга от легитимных запросов.
- Параметры модели оптимизированы для минимизации ошибок прогнозирования в обучающих данных.

Периодическое обновление модели:

- Подчёркивается важность периодического обновления модели новыми помеченными данными для адаптации к меняющимся тактикам фишинга.
- По мере появления новых типов фишинговых атак характеристики их запросов со временем могут меняться.
- Обновление модели позволяет изучить эти новые шаблоны, сохраняя при этом информацию о ранее замеченных признаках фишинга.
- Частоту обновлений модели можно регулировать в зависимости от объёма и скорости сбора новых фишинговых данных.

Непрерывное обучение:

- Некоторые архитектуры машинного обучения, такие как онлайн-обучение или инкрементное обучение, специально разработаны для поддержки непрерывного обновления модели по мере поступления новых данных.
- Вместо переподготовки всего совокупного набора данных эти методы постепенно корректируют параметры модели на основе мини-пакетов новых примеров.
- Непрерывное обучение помогает снизить вычислительную нагрузку, связанную с повторным переобучением, и позволяет быстрее адаптироваться к новым угрозам.

Управление данными:

- Эффективное обновление модели требует тщательного управления обучающими данными с течением времени.
- Набор данных необходимо дополнить новыми примерами фишинга и вредоносными примерами при сохранении баланса между классами.
- Такие методы, как активное обучение, используют для стратегического выбора наиболее информативные примеры для маркировки, оптимизируя использование человеческих усилий по аннотированию.

Оценка и мониторинг:

- После каждого обновления переподготовленную модель следует оценивать с помощью отдельного набора тестов, чтобы убедиться в её производительности и отсутствии ухудшений
- Постоянный мониторинг прогнозов модели в процессе производства также важен для выявления отклонений от концепции или ошибок, которые могут потребовать дальнейших обновлений.

Обучение и обновление модели необходимы для долгосрочной эффективности системы обнаружения фишинга. Начальный процесс обучения формирует базовые знания модели, в то время как периодические обновления позволяют ей со временем адаптироваться к новым моделям фишинга, а непрерывное обучение, активный отбор данных и мониторинг производительности, помогают оптимизировать процесс обновления и поддерживать точность модели перед лицом возникающих угроз.

I. Установление порогового значения и формирования предупреждений

Установление порогового значения и формирование предупреждений относятся к процессу принятия решения о том, следует ли классифицировать данный запрос сетевого ресурса как попытку фишинга, на основе оценки вероятности, выводимой статистической моделью, и выдачи соответствующего предупреждения, если решение положительное. Это шаг, который преобразует прогнозы модели в фактические решения по обеспечению безопасности и уведомления.

Порог оценки вероятности:

- Статистическая модель выводит оценку от 0 до 1 для каждого запроса сетевого ресурса, указывающую на

предполагаемую вероятность того, что это попытка фишинга.

- Для принятия окончательного решения о классификации используется предварительно заданное пороговое значение (например, 0,8).
- Если оценка превышает пороговое значение, запрос классифицируется как потенциальная угроза фишинга; иначе - считается безопасным.

Выбор порогового значения:

- Выбор порогового значения предполагает компромисс между ложноположительными результатами (легитимные запросы ошибочно классифицируются как фишинговые) и ложноотрицательными результатами (попытки фишинга ошибочно классифицируются как безвредные).
- Более высокий порог снижает количество ложных срабатываний, но может пропустить некоторые реальные попытки фишинга. Более низкий порог улавливает больше фишинговых запросов, но также помечает больше безопасных запросов.
- Оптимальный порог определяется на основе конкретных требований безопасности и относительной стоимости ложных срабатываний и ложноотрицательных результатов в контексте развёртывания.

Формирование оповещений:

- Когда оценка запроса превышает пороговое значение фишинга, формируется предупреждение, указывающее на потенциальную угрозу.
- Оповещение может включать соответствующие сведения о запросе, такие как запрошенный URL-адрес, IP-адрес источника, соответствующий показатель вероятности и т.д.
- Оповещения доставляются по различным каналам, таким как журналы консоли, уведомления по электронной почте, SMS-сообщения, системы управления инцидентами и событиями безопасности (SIEM) и т.д.

Проверка и фильтрация оповещений:

- Чтобы уменьшить количество ложных срабатываний, сформированные оповещения могут проходить дополнительные этапы проверки перед их эскалацией.
- Это может включать сравнение сведений о предупреждении со списками разрешений известных безопасных ресурсов, проверку на наличие потока предупреждений из того же источника или применение других эвристических фильтров.
- Ручная проверка подмножества предупреждений аналитиками безопасности может помочь со временем настроить пороговые значения и правила проверки.

Действия по реагированию на предупреждение:

- В зависимости от серьёзности и достоверности классификации фишинга предупреждения могут инициировать различные ответные действия.
- Предупреждения с меньшей степени серьёзности регистрируются для последующего анализа, в то время как предупреждения с большей степени серьёзности вызывают немедленную блокировку запроса ресурса и помещение связанного сетевого трафика на карантин.
- Автоматические реакции дополнены действиями по расследованию и исправлению, выполняемыми вручную, на основе сведений о предупреждении.

Установление порогового значения и формирование предупреждений устраняют разрыв между вероятностными прогнозами модели обнаружения фишинга и детерминированными решениями и действиями в области безопасности, необходимыми для защиты пользователей и систем. Выбирая соответствующие пороговые значения, формируя информативные предупреждения и запуская пропорциональные ответные действия, этот компонент вводит в действие разведданные, собранные моделью, для обеспечения эффективной защиты от фишинга.

J. Преимущества,-недостатки и значимость предлагаемого решения

Этот патент иллюстрирует важную эволюцию от реактивного обнаружения фишинга на основе сигнатур к более динамичному адаптивному подходу, основанному на статистическом моделировании.

Патент представляет автоматизированный подход, основанный на данных, для обнаружения попыток фишинга в режиме реального времени путём изучения обобщённых шаблонов вместо использования статических правил. Динамический характер позволяет адаптироваться к развивающимся методам фишинга. Формирование вероятностных оценок риска позволяет определять приоритетность наиболее подозрительных случаев.

Описывая гибкий конвейер машинного обучения с извлечением признаков, обновлением модели и формированием предупреждений, патент обеспечивает основу для создания более эффективных антифишинговых систем. Предлагаемый метод может значительно улучшить способность организации активно выявлять и блокировать фишинговые угрозы до того, как они станут жертвами пользователей. Однако для его внедрения и обслуживания требуется значительный сбор данных и инженерные усилия.

Статистическая модель обучается на исторических примерах фишинга и неопасных примерах для изучения закономерностей, которые различают эти два класса. Его можно периодически переподготовлять на основе новых

данных, чтобы адаптироваться к меняющимся тактикам фишинга.

Основные преимущества:

- Обеспечивает упреждающее обнаружение попыток фишинга в режиме реального времени, включая новые, невиданные ранее атаки, путём анализа шаблонов в атрибутах URL / домена
- Предоставляет оценку вероятности, позволяющую определить приоритетность наиболее опасных угроз
- Адаптируется к меняющимся тактикам фишинга с течением времени посредством периодической переподготовки модели
- Формирует информативные оповещения с ключевыми запросами для расследования группами безопасности
- Позволяет настраивать чувствительность обнаружения путём настройки порога оповещения

Недостатки:

- Требуются значительные исторические и достоверные данные о фишинге для начального обучения модели
- Необходим постоянный сбор помеченных данных для переподготовки и обновления модели с течением времени
- Могут отсутствовать некоторые новые шаблоны фишинга, не отражённые в обучающих данных
- Извлечение эффективного набора признаков требует тщательного проектирования и экспертных знаний в предметной области
- Может генерировать ложноположительные результаты, которые требуют дополнительной фильтрации / проверки

1) Извлечение признаков

Извлечение признаков является важным шагом, который позволяет создавать эффективные модели ML для обнаружения фишинга путём представления данных запроса в информативном формате. Однако для разработки и поддержания надёжного набора признаков требуются значительные знания и усилия. Сочетание ручной разработки признаков с автоматическим обучением представлению может помочь устранить некоторые из этих недостатков и создать более мощные гибридные модели обнаружения.

a) Преимущества:

- Предоставляет ключевые характеристики запросов сетевых ресурсов в структурированном формате, подходящем для анализа с помощью моделей машинного обучения. Извлечение соответствующих признаков имеет решающее значение для построения точных моделей обнаружения фишинга.
- Фиксирует дискриминационные шаблоны, которые отличают попытки фишинга от легитимных запросов. Тщательно спроектированные признаки могут обеспечивать надёжные сигналы для классификации.
- Уменьшает размерность необработанных данных запроса, делая их обработку более эффективной с точки зрения вычислений. Работать с компактным набором информационных признаков быстрее, чем анализировать полное содержимое запроса.
- Специалисты по извлечению признаков из предметной области используют свои знания для создания высокоэффективных признаков для конкретной задачи обнаружения фишинга. Ручная разработка признаков, основанная на опыте, может дать очень эффективные наборы признаков.
- Извлечённые признаки можно комбинировать с автоматически изучаемыми признаками в процессе глубокого обучения для создания мощных гибридных моделей. Это позволяет получить максимум пользы как от ручного проектирования объектов, так и от обучения представлению.

b) Недостатки:

- Требуется значительный опыт работы в предметной области и ручные усилия для определения и внедрения эффективных признаков. Разработка хорошего набора признаков для обнаружения фишинга требует много времени и в значительной степени зависит от экспертных знаний.
- Разработанные признаки могут не отражать все релевантные шаблоны, особенно новые в развивающихся фишинговых атаках. Существует риск пропустить важные сигналы, о которых эксперты не подумали.
- Код извлечения признаков нуждается в регулярном обновлении, чтобы соответствовать изменениям в веб-технологиях и методах фишинга. Обслуживание конвейера признаков может быть постоянной инженерной нагрузкой.
- Извлечённые признаки специфичны для определённых типов фишинга, что ограничивает способность модели обобщаться на новые варианты атак. Чрезмерно специализированные признаки могут привести к хрупкости моделей.
- Использование исключительно признаков, разработанных вручную, может привести к снижению производительности по сравнению со сквозным глубоким обучением на необработанных данных. Для некоторых задач заученные представления могут превосходить созданные вручную признаки.

2) Статистическая модель

Статистические модели, особенно гибридные подходы, сочетающие инженерные признаки и глубокое обучение,

предлагают мощные возможности для динамического и адаптивного обнаружения фишинга. Однако они также создают проблемы, связанные с качеством данных, проектированием признаков, сложностью вычислений и устойчивостью к атакам противника. Эффективное развертывание требует тщательного устранения этих ограничений посредством постоянного сбора данных, обновления моделей и экспертного надзора.

a) Преимущества:

- Обеспечивает динамическое и адаптивное обнаружение фишинговых угроз путём изучения шаблонов из исторических данных. Статистическая модель может распознавать сложные комбинации признаков, указывающих на фишинг, помимо простых правил.
- Выводит показатель вероятности, который количественно определяет риск того, что запрос является попыткой фишинга. Это обеспечивает более детальную информацию, чем двоичная классификация, позволяя проводить детальную оценку рисков и расставлять приоритеты.
- Может обновляться с течением времени путём переподготовки на основе новых данных для адаптации к меняющимся тактикам фишинга. Прогностическая способность модели может сохраняться по мере того, как злоумышленники меняют свои методы.
- Подходит для обнаружения в режиме реального времени благодаря быстрому выводу результатов после обучения модели. Позволяет интегрировать в системы оперативного мониторинга и предотвращения.
- Гибридные модели, сочетающие ручную разработку признаков и глубокое обучение, показали более высокую точность обнаружения фишинга по сравнению с традиционными моделями ML. Использует сильные стороны как человеческого опыта, так и обучения на основе данных.

b) Недостатки:

- Для начального обучения требуется большой маркированный набор данных, получение которого может быть дорогостоящим и отнимать много времени. Наборы данных о фишинге должны постоянно обновляться, чтобы включать новые шаблоны атак.
- Производительность модели в значительной степени зависит от качества и репрезентативности обучающих данных. Предвзятые или неполные наборы данных могут привести к искаженным прогнозам и "слепым зонам".
- Разработка признаков по-прежнему играет решающую роль в построении эффективных моделей ML для обнаружения фишинга. Соответствующие признаки должны создаваться вручную, что требует значительного опыта в предметной области.
- Традиционные модели ML, такие как Random Forest, снижают производительность и не обнаруживают новые схемы фишинга, не замеченные во время обучения. Поддержание моделей в актуальном состоянии является постоянной задачей.
- Обучение моделей глубокого обучения может быть дорогостоящим с точки зрения вычислений и потребовать специализированного оборудования. Повышенная сложность также затрудняет интерпретацию и отладку моделей.
- Риск враждебных атак, при которых фишеры намеренно создают сообщения, чтобы избежать обнаружения моделью. Модели ML могут быть хрупкими и уязвимыми для манипуляций.

3) Обучение и обновление модели

Обучение и обновление модели необходимы для поддержания эффективности системы обнаружения фишинга по мере появления новых угроз. Однако этот процесс также создает операционные сложности, связанные со сбором данных, маркировкой, вычислительными ресурсами и управлением изменениями. Тщательная разработка схемы переподготовки, средств контроля качества данных и механизмов мониторинга имеет решающее значение для реализации преимуществ при одновременном смягчении недостатков.

a) Преимущества:

- Позволяет модели обнаружения фишинга адаптироваться к развивающимся угрозам, со временем изучая новые помеченные примеры. Периодическая переподготовка помогает модели распознавать новые схемы фишинга.
- Методы непрерывного обучения позволяют постепенно обновлять модель новыми данными, снижая вычислительные затраты по сравнению с полной переподготовкой, что обеспечивает более частое и эффективное обновление модели.
- Стратегии активного обучения могут оптимизировать отбор новых примеров для маркировки, сводя к минимуму ручные затраты на аннотирование. Это помогает управлять текущим процессом обработки данных.
- Регулярная оценка модели на новых наборах тестов гарантирует, что обновления действительно повышают производительность и не приводят к регрессиям. Мониторинг поведения модели в рабочей среде выявляет потенциальные проблемы на ранней стадии.
- Обновление модели разнообразным набором новых примеров фишинга и вредоносных программ повышает её надежность и универсальность для различных вариантов атак. Широкий набор обучающих программ помогает модели справляться с широким спектром угроз.

b) Недостатки:

- Требуется постоянный поток новых помеченных как фишинговые и безвредные примеров для

переобучения модели, что может быть сложным и дорогостоящим для получения в масштабе. Маркировка новых обучающих примеров требует ручной работы экспертов предметной области и занимает много времени. Разработка эффективных рабочих процессов аннотирования и интерфейсов имеет решающее значение.

- Если распределение новых обучающих данных значительно отличается от исходных, в обновлённой модели может наблюдаться снижение производительности или нестабильность.
- Частые обновления моделей могут быть дорогостоящими с точки зрения вычислений, особенно для больших моделей глубокого обучения. Методы инкрементного обучения помогают, но все ещё могут требовать значительных ресурсов.
- Обновление модели изменяет её поведение, что негативно сказывается на последующих системах и рабочих процессах, основанных на её прогнозах.
- Существует риск того, что модель будет переоснащена недавним учебным примерам и потеряет производительность при использовании старых фишинговых шаблонов. Сбалансировать сочетание старых и новых данных во время переподготовки непросто.

4) Установление порогового значения и формирование предупреждений

Определение порога и формирование предупреждений играют решающую роль в реализации модели обнаружения фишинга путём преобразования её вероятностных результатов в конкретные действия по обеспечению безопасности. Однако этот процесс также сопряжен с проблемами, связанными с настройкой порога, управлением ложными срабатываниями и переутомлением при оповещении. Тщательный дизайн и постоянное совершенствование логики определения пороговых значений в сочетании с производительностью модели являются ключом к достижению баланса между снижением рисков и операционной эффективностью.

a) Преимущества:

- Позволяет преобразовать вероятностные выходные данные статистической модели в практические решения по обеспечению безопасности. Сравнивая показатель вероятности фишинга модели с заданным порогом, система может автоматически определить, следует ли помечать запрос как потенциальную угрозу.
- Предоставляет настраиваемый параметр (пороговое значение) для балансирования компромисса между ложноположительными и ложноотрицательными результатами. Настройка порогового значения позволяет контролировать чувствительность оповещений на основе их толерантности к риску и операционных ограничений.
- Позволяет генерировать информационные оповещения с соответствующими сведениями о подозрительном запросе, такими как URL-адрес, IP-адрес источника и соответствующая оценка риска. Эта контекстуальная информация помогает службам безопасности быстро выявлять и расследовать потенциальные случаи фишинга.
- Поддерживает гибкие каналы доставки оповещений, такие как журналы консоли, электронная почта, SMS или интеграция с системами информации о безопасности и управления событиями (SIEM).
- Позволяет реализовать дополнительную логику проверки и фильтры для дальнейшего уменьшения ложных срабатываний. Например, оповещения могут быть отключены для доменов, внесённых в белый список, или диапазонов IP-адресов, или если показатель достоверности модели ниже определённого уровня.

b) Недостатки:

- Выбор соответствующего порогового значения требует тщательной настройки и может быть связан с методом проб и ошибок. Слишком низкое значение порога приведёт к большому количеству ложных срабатываний, в то время как слишком высокое значение – к пропуску реальных попыток фишинга.
- Требуется регулярно корректировать оптимальный порог по причине изменения с течением времени характеристик фишинговых атак, что, в свою очередь, требует постоянного мониторинга и анализа производительности системы и меняющегося ландшафта угроз.
- Пороговое значение сводит обширную информацию, предоставляемую оценкой вероятности модели, к бинарному решению (оповещение или отсутствие оповещения). Это приведёт к потере нюансов и детализации при оценке риска пограничных случаев.
- Предупреждения, сформированные системой, по-прежнему могут требовать ручной проверки и расследования аналитиками безопасности. Хотя установление порогового значения помогает определить приоритетность наиболее подозрительных случаев, оно не устраняет полностью необходимость в суждениях и вмешательстве человека.
- Эффективность оповещений зависит от точности лежащей в основе статистической модели. Если прогнозы модели неправильно откалиброваны, даже хорошо настроенный порог может привести к неоптимальным результатам.

ПАТЕНТ US9071600B2

Аннотация – документ содержит анализ патента US9071600B2, ориентированного на фишинг и предотвращению онлайн-мошенничества, для изучения различных аспектов, включая техническую область, проблему, решаемую изобретением, предлагаемое решение и его основные области применения.

Подробный анализ патента показывает его потенциал влияния на сферу кибербезопасности и различные отрасли, зависящие от безопасных онлайн-операций, подчёркивая его полезность для специалистов, стремящихся повысить безопасность в Интернете и предотвратить мошеннические действия. Для экспертов по кибербезопасности понимание механизмов такой системы может помочь в разработке более надёжных протоколов для борьбы с развивающимися онлайн-угрозами. Для профессионалов в области ИТ и DevOps особое внимание в патенте уделяется VPN и защищённым каналам связи.

A. Введение

Патент US9071600B2 затрагивает важнейшую проблему онлайн-безопасности, уделяя особое внимание методам предотвращения фишинга и мошенничества. В нём описывается система, которая устанавливает туннель виртуальной частной сети (VPN) между компьютером пользователя и сервером для повышения безопасности во время онлайн-транзакций. Техническая классификация изобретения относится к разделам сетевой безопасности, аутентификации объектов и контрмер против вредоносного трафика.

B. Основная идея

Основная идея последствий патента заключается в том, чтобы распространить его на отрасли, которые в значительной степени зависят от онлайн-транзакций, такие как финансы и электронная коммерция. Предоставляя метод защиты от фишинга и мошенничества, патент способствует повышению общей надёжности онлайн-сервисов, что важно для доверия потребителей и бесперебойного функционирования цифровых торговых площадок. Он даёт представление о проектировании и внедрении защищённых сетей, что является фундаментальным аспектом поддержания операционной безопасности в различных организационных контекстах. В контексте кибербезопасности актуальность патента имеет первостепенное значение. Он предлагает метод защиты конфиденциальной пользовательской информации и предотвращения несанкционированного доступа, что имеет решающее значение для поддержания целостности онлайн-систем.

C. Ключевые аспекты патента

- **Цель**: патент посвящён методам и системам предотвращения фишинга и мошеннических действий в Интернете
- **Классификация**: патент подпадает под несколько классификаций, связанных с сетевой безопасностью, аутентификацией объектов и мерами противодействия вредоносному трафику, что указывает на его актуальность.
- **Инновации в области безопасности**: патент представляет собой инновационный подход к повышению безопасности в Интернете путём выявления и снижения рисков, связанных с несанкционированным доступом и мошенническими транзакциями.
- **Технический вклад**: упомянутые патенты демонстрируют технический вклад US9071600B2 в более широкую область кибербезопасности и его постоянную актуальность для новых технологий безопасности.
- **Последствия истечения срока действия**: истечение срока действия патента открывает возможности для других частных лиц и компаний исследовать ранее защищённую технологию и потенциально развивать её, не опасаясь нарушения.
- **Исследования и разработки**: патент является частью более широкой экосистемы исследований и разработок в области кибербезопасности, а содержащиеся в нем ссылки на уровень техники и последующие цитаты указывают на совместное развитие знаний и технологий в этой области.

D. Область применения

Патент имеет большое значение для отраслей, занимающихся онлайн-деятельностью, требующей безопасной аутентификации, защиты данных и мер по предотвращению мошенничества. Эти отрасли выиграют от внедрения систем и методов для повышения своей кибербезопасности и защиты от фишинга и онлайн-мошенничества.

1) Банковский финансовый сектор

Финансовые учреждения управляют огромными объёмами конфиденциальных финансовых данных и ежедневно проводят множество онлайн-транзакций. Этот сектор в значительной степени зависит от безопасных

онлайн-транзакций и защиты финансовой информации клиентов. Направленность патента на предотвращение фишинга и мошеннических действий имеет решающее значение для защиты учётных записей клиентов и поддержания доверия к системам онлайн-банкинга. Внедрение запатентованных методов поможет банкам выявлять и смягчать угрозы, обеспечивая безопасность онлайн-транзакций и защищая от финансовых потерь, связанных с мошенничеством.

2) Технологии и программное обеспечение

Технологические компании и компании-разработчики ПО, в том числе специализирующиеся на решениях в области кибербезопасности, получат значительную выгоду от инноваций. Компании этого сектора разрабатывают и предоставляют платформы и программное обеспечение, которые позволяют осуществлять онлайн-транзакции и хранить данные. Меры безопасности, изложенные в патенте, необходимы для поддержания целостности этих платформ и защиты от кибер-угроз. Эти компании могут интегрировать патентные методологии в свои платформы безопасности, предлагая своим клиентам улучшенную защиту от фишинга и мошенничества. Актуальность патента распространяется на разработчиков веб-браузеров, служб электронной почты и других приложений, где критически важны аутентификация пользователя и целостность данных. Принимая эти меры безопасности, технологические компании обеспечат более надёжную защиту от все более изощренных кибер-угроз.

3) Электронная коммерция

Интернет-магазины и поставщики услуг являются основными объектами фишинга и мошенничества. Индустрия электронной коммерции в значительной степени зависит от доверия потребителей и безопасной обработки личной и платёжной информации. Онлайн-магазины и поставщики услуг часто становятся объектами фишинговых атак, направленных на кражу данных клиентов. Превентивные меры могут сыграть важную роль в обеспечении безопасности платформ электронной коммерции, защите транзакций клиентов от мошеннического вмешательства и обеспечении конфиденциальности личной информации. Внедряя протоколы безопасности, предприятия электронной коммерции повысят свою репутацию в области безопасности и надёжности, поощряя постоянное взаимодействие с потребителями.

4) Здравоохранение

С ростом оцифровки медицинских записей и услуг эта отрасль требует надежных мер безопасности для защиты информации о пациентах и обеспечения конфиденциальности и целостности медицинских данных, которыми делятся онлайн. Организации управляют конфиденциальными данными пациентов, что делает их критически важной областью для применения патентных мер безопасности. Технологии, предусмотренные патентом, могут помочь защитить электронные медицинские записи (EHRS), порталы пациентов и другие цифровые медицинские услуги от несанкционированного доступа и мошенничества. Обеспечение конфиденциальности и неприкосновенности медицинской информации является не только вопросом соблюдения нормативных требований, но и необходимым условием доверия пациентов и эффективного оказания медицинской помощи. Внедрение этих решений безопасности может внести значительный вклад в защиту медицинских данных во все более цифровом медицинском пространстве.

5) Государственный и муниципальные сектор

Государственные и муниципальные учреждения часто обрабатывают конфиденциальную информацию и предоставляют услуги, требующие безопасного онлайн-взаимодействия. Технологии и методы, описанные в патенте, могут помочь защитить от мошеннических действий, нацеленных на веб-сайты государственного сектора и онлайн-сервисы. Проблемы безопасности, с которыми сталкиваются эти организации, включают защиту от несанкционированного доступа к конфиденциальным данным и обеспечение целостности онлайн-сервисов. Эти методы и системы предлагают ценные решения для повышения уровня кибербезопасности государственных веб-сайтов и цифровых сервисов, защиты от попыток фишинга и предотвращения онлайн-мошенничества.

E. Предлагаемое решение

Патент представляет собой многогранный подход к борьбе с фишингом и онлайн-мошенничеством. Сочетая аутентификацию пользователя, верификацию веб-сайта, безопасную коммуникацию, мониторинг в режиме реального времени, передовые алгоритмы обнаружения угроз, обучение пользователей и механизм обратной связи, предлагаемое решение обеспечивает надёжную защиту от растущих угроз в цифровом ландшафте. Эти компоненты работают вместе для защиты пользователей и организаций от финансового и репутационного ущерба, связанного с онлайн-мошенничеством и фишинговыми атаками.

В патенте описываются система и метод, предназначенные для выявления и смягчения угроз в режиме реального времени, защиту пользовательских данных и безопасные транзакции.

Ключевые компоненты предлагаемого решения:

- **Аутентификация пользователя**: важнейший компонент решения включает проверку личности пользователей, пытающихся получить доступ к сервису или выполнить транзакцию. Процесс гарантирует, что доступ предоставляется только легитимным пользователям, тем самым снижая риск несанкционированного доступа.
- **Проверка веб-сайта**: система включает механизмы для проверки подлинности веб-сайтов. Это имеет решающее значение для предотвращения направления пользователей на мошеннические веб-сайты или взаимодействия с ними, предназначенные для имитации легитимных веб-сайтов с целью фишинга.
- **Безопасные каналы связи**: установление безопасных каналов связи между пользователями и

службами является ещё одним жизненно важным аспектом. Это включает в себя использование шифрования и безопасных протоколов для защиты данных при передаче, предотвращая перехват или манипулирование злоумышленниками.

- **Мониторинг и анализ в режиме реального времени**: предлагаемое решение включает мониторинг действий пользователей и транзакций в режиме реального времени. Анализируя шаблоны и поведение, система может выявлять потенциальные угрозы или мошеннические действия, обеспечивая своевременное вмешательство.

- **Алгоритмы обнаружения угроз**: для обнаружения попыток фишинга и мошеннических действий используются передовые алгоритмы. Эти алгоритмы используют различные индикаторы и эвристику для выявления подозрительных действий, таких как необычные попытки входа в систему или транзакции, которые отличаются от типичного поведения пользователя.

- **Обучение и осведомлённость пользователей**: частью решения является информирование пользователей о рисках фишинга и мошенничества. Это включает оповещения при обнаружении потенциальной угрозы, побуждающие пользователей предпринимать соответствующие действия для защиты своей информации.

- **Механизм обратной связи**: система позволяет получать обратную связь от пользователей относительно потенциальных угроз или ложных срабатываний. Обратная связь используется для постоянного повышения точности и эффективности алгоритмов обнаружения угроз.

1) Аутентификация пользователя

Компонент "Аутентификация пользователя" включает в себя различные методы и системы безопасной аутентификации пользователей для предотвращения несанкционированного доступа и защиты от фишинга и онлайн-мошенничества. Эти методы содержат встроенные формы аутентификации, хранимые данные аутентификации, аутентификацию идентификационных атрибутов, протокол 3-D Secure и многоуровневые системы безопасности контроля доступа:

- **Встроенная форма аутентификации**: один из подходов к аутентификации пользователя предполагает использование встроенной формы аутентификации. Эта форма представляется пользователю асинхронно и может быть встроена в iFrame на странице оформления заказа продавца после проверки того, что компоненты системы аутентификации её поддерживают. Встроенная форма аутентификации используется, если компоненты системы могут её поддерживать, а если нет, используется другой процесс аутентификации.

- **Сохраненные аутентификационные данные**: другой метод аутентификации пользователя предполагает использование платформы аутентификации, которая может хранить данные, полученные от сервера контроля доступа эмитента. Платформа аутентифицирует пользователей и портативные устройства от имени сервера контроля доступа эмитента, используя сохраненные данные. Такой подход гарантирует, что сервер контроля доступа эмитента может полагаться на платформу для проведения аутентификации.

- **Аутентификация идентификационных атрибутов**: в патенте также рассматриваются системы и методы аутентификации различных идентификационных атрибутов сторон, участвующих в транзакции. Атрибуты могут включать такие элементы, как имя участника, адрес, номер социального страхования, дата рождения или любые другие идентифицирующие атрибуты. В некоторых вариантах осуществления все участники транзакции могут аутентифицировать свою идентификационную информацию.

- **3DS протокол**: патент расширяет и улучшает 3DS протокол и структуру для обеспечения возможности аутентификации сторон, участвующих в транзакции. Протокол гарантирует аутентификацию участников транзакции, обеспечивая дополнительный уровень безопасности.

- **Многоуровневая система безопасности контроля доступа**: в патенте также упоминается система безопасности контроля доступа, которая используется для аутентификации пользователя. Система обеспечивает несколько уровней безопасности, гарантирующих, что только авторизованные пользователи могут получить доступ к защищенным ресурсам.

2) Проверка веб-сайта

Компонент предлагаемого решения включает в себя различные методы проверки подлинности веб-сайтов и предотвращения взаимодействия пользователей с мошенническими сайтами. Методы включают использование общего секрета, создание VPN-туннеля, использование предварительно предоставленных ключей или частных сертификатов для аутентификации в VPN-туннеле и проверку информации пользователя, связанной с веб-сайтом. Реализуя данные методы, решение направлено на смягчение последствий фишинговых атак и онлайн-мошенничества, обеспечивая безопасность пользовательских данных и транзакций:

- **Проверка подлинности веб-сайтов**: один из подходов к проверке веб-сайта предполагает использование общего секрета между устройством пользователя и веб-сайтом. Общий секрет используется для аутентификации веб-сайта и обеспечения того, что пользователь взаимодействует с легитимным сайтом.

- **Создание VPN-туннеля**: другой метод включает в себя создание VPN-туннеля между устройством пользователя и доверенным сервером. VPN-туннель обеспечивает безопасную связь между устройством и сервером, предотвращая несанкционированный доступ и защищая от фишинговых атак. Этот метод обсуждается в патентном документе, хотя он явно не упоминается как метод проверки веб-сайта.
- **Межсайтовая аутентификация VPN-туннеля**: метод предполагает использование предварительно предоставленных ключей или частных сертификатов от AWS Private Certificate Authority для аутентификации конечных точек VPN-туннеля. Это гарантирует, что только авторизованные устройства смогут установить VPN-соединение и получить доступ к ресурсам на другом конце туннеля.

Проверка информации о пользователе: в патенте US8037316B2, на который ссылается US9071600B2, обсуждаются метод и система уточнения информации о пользователе, которые адаптированы для проверки подлинности веб-сайтов.

3) Защищенные каналы связи

Защищённые каналы связи имеют решающее значение для защиты данных во время передачи в различных контекстах, включая кибербезопасность.:

- **Сквозное шифрование**: метод включает шифрование данных в источнике и дешифрование их в пункте назначения, гарантируя, что только предполагаемый получатель сможет получить доступ к информации. Сквозное шифрование может быть реализовано с использованием различных криптографических методов, таких как симметричное или асимметричное шифрование.
- **Уровень защищённых сокетов (SSL) и безопасность транспортного уровня (TLS)**: протоколы обеспечивают безопасную связь через Интернет путём установления безопасного соединения между двумя сторонами, такими как веб-браузер и веб-сервер. Протоколы SSL и TLS используют как симметричное, так и асимметричное шифрование для проверки личности и шифрования данных, которыми обмениваются стороны.
- **SSH**: SSH — это протокол, который обеспечивает безопасный удалённый доступ к другой операционной системе по сети. Он использует шифрование с открытым ключом для аутентификации пользователя и хоста, а затем создаёт безопасный канал, который шифрует все данные, которыми они обмениваются.
- **Виртуальная частная сеть (VPN)**: VPN создаёт безопасный туннель между двумя или более операционными системами по сети, обеспечивая безопасную передачу данных. VPN используется для защиты данных при передаче, особенно при использовании сетей общего пользования.
- **Протоколы аутентификации**: протоколы аутентификации, такие как CHAP, PAP и EAP, используются для защиты каналов связи путём проверки личности сторон, участвующих в обмене данными.
- **Ограничения брандмауэра и шифрование данных**: для предотвращения несанкционированного участия, подслушивания, шпионажа, утечки данных и перехвата коммуникаций используются смягчающие технологии, такие как ограничения брандмауэра, шифрование данных и меры безопасности аутентификации.

4) Мониторинг и анализ в режиме реального времени

Компонент включает в себя постоянный мониторинг действий пользователей и транзакций, анализ моделей и поведения, а также выявление потенциальных угроз или мошеннических действий. Поступая таким образом, система может предпринять соответствующие действия для снижения рисков, связанных с фишингом и онлайн-мошенничеством.

5) Алгоритмы обнаружения угроз

Компонент использует передовые алгоритмы для выявления подозрительных действий, таких как необычные попытки входа в систему или транзакции, которые отличаются от типичного поведения пользователя. Применяя различные индикаторы и эвристику, алгоритмы могут обнаруживать потенциальные угрозы и мошеннические действия в режиме реального времени.

Одним из ключевых аспектов алгоритмов обнаружения угроз является их способность анализировать шаблоны и поведение в действиях пользователей и транзакциях. Устанавливая критерий нормального поведения пользователя, алгоритмы могут выявлять аномалии, которые указывают на потенциальную угрозу. Например, если пользователь входит в систему из определённого географического местоположения и внезапно пытается получить доступ к своей учётной записи из другой страны, алгоритм может пометить это действие как подозрительное и выдать предупреждение.

Алгоритмы обнаружения угроз также могут отслеживать конкретные признаки фишинга и мошенничества, такие как наличие известных вредоносных URL-адресов или использование подозрительного содержимого электронной почты. Поддерживая базу данных известных угроз и постоянно пополняя её новой информацией, алгоритмы быстро выявляют возникающие угрозы и реагируют на них.

Другим важным аспектом алгоритмов обнаружения угроз является их способность адаптироваться и обучаться с течением времени. По мере появления новых угроз и изменения злоумышленниками своей тактики алгоритмы должны иметь возможность развиваться, чтобы идти в ногу со временем. Благодаря внедрению методов машинного обучения алгоритмы постоянно повышают свою точность и эффективность на основе обратной связи и новых данных.

В патенте также упоминается использование мониторинга и анализа в режиме реального времени в сочетании с алгоритмами обнаружения угроз. Постоянно отслеживая действия пользователей и транзакции, система обнаруживает потенциальные угрозы по мере их возникновения и принимать немедленные меры для снижения риска. Эта функция в режиме реального времени необходима для предотвращения несанкционированного доступа и мошеннических действий до того, как они смогут нанести значительный ущерб.

6) Механизм обратной связи

Компонент позволяет пользователям предоставлять обратную связь относительно потенциальных угроз или ложноположительных результатов, которые могут использоваться для постоянного повышения точности и эффективности алгоритмов обнаружения угроз. В сочетании с другими компонентами, такими как алгоритмы обнаружения угроз и мониторинг в режиме реального времени, механизм обратной связи помогает создать более надёжную и адаптируемую систему безопасности, которая может идти в ногу с постоянно меняющимся ландшафтом кибер-угроз. Этот цикл обратной связи гарантирует, что система остаётся актуальной и эффективной перед лицом развивающихся кибер-угроз.

Другим важным аспектом механизма обратной связи является то, что он предоставляет пользователям возможность активно участвовать в процессе обеспечения безопасности. Предоставляя пользователям возможность сообщать о потенциальных угрозах, система использует коллективный интеллект своей базы пользователей для более быстрого выявления новых угроз и реагирования на них. Такой совместный подход к обеспечению безопасности особенно эффективен при обнаружении целенаправленных атак или сложных фишинговых кампаний, которые могут обходить традиционные меры безопасности.

Механизм обратной связи также может помочь уменьшить количество ложных срабатываний, которые являются серьёзной проблемой в автоматизированных системах обнаружения угроз. Ложные срабатывания возникают, когда система неправильно идентифицирует легитимную активность как потенциальную угрозу, что приводит к ненужным предупреждениям и сбоям в работе пользователей. Позволяя пользователям оставлять отзывы об этих ложноположительных результатах, система со временем учится более точно различать легитимные и вредоносные действия.

Чтобы механизм обратной связи был эффективным, он должен быть простым в использовании и доступным для всех пользователей. Это включает предоставление чётких инструкций о том, как сообщать о потенциальных угрозах или ложноположительных результатах, а также предложение нескольких каналов для отправки отзывов, таких как электронная почта, веб-формы или мобильные приложения. Система также должна своевременно реагировать на отзывы пользователей, подтверждая получение отчёта и предоставляя обновлённую информацию о любых действиях, предпринятых в результате.

F. Технологический процесс

Технологический процесс предлагаемого патентного решения включает в себя несколько этапов для обеспечения безопасности пользовательских данных и предотвращения несанкционированного доступа и мошеннических действий.

- **Установка VPN-туннеля**: компьютер пользователя устанавливает VPN-туннель между собой и сетью. Безопасное соединение гарантирует, что данные, передаваемые между пользователем и сетью, зашифрованы и защищены от несанкционированного доступа.
- **Аутентификация**: аутентификация пользователя осуществляется с использованием различных методов, таких как проверка информации о пользователе или протокол 3-D Secure. Этот шаг гарантирует, что только авторизованные пользователи смогут получить доступ к сети и выполнять транзакции.
- **Проверка веб-сайта**: подлинность веб-сайтов проверяется для предотвращения взаимодействия пользователей с мошенническими сайтами. Этого можно достичь, используя общий секрет между устройством пользователя и веб-сайтом или установив VPN-туннель.
- **Защищённые каналы связи**: каналы устанавливаются с использованием таких методов, как сквозное шифрование, SSL/ TLS или SSH. Эти каналы гарантируют, что данные, передаваемые между сторонами, защищены и не могут быть перехвачены злоумышленниками.
- **Мониторинг и анализ в режиме реального времени**: действия пользователей и транзакции отслеживаются в режиме реального времени, а для обнаружения потенциальных угроз или мошеннических действий используются передовые алгоритмы. Это позволяет своевременно вмешиваться и снижать риски.
- **Алгоритмы обнаружения угроз**: для выявления подозрительных действий, таких как необычные попытки входа в систему или транзакции, которые отличаются от типичного поведения пользователя, используются продвинутые алгоритмы. Эти алгоритмы используют различные индикаторы и эвристику для обнаружения потенциальных угроз и предотвращения несанкционированного доступа и мошеннических действий.
- **Механизм обратной связи**: пользователи могут предоставлять обратную связь относительно потенциальных угроз или ложноположительных результатов, которые используются для повышения точности и эффективности алгоритмов обнаружения угроз. Цикл обратной связи гарантирует, что система

остаётся актуальной и эффективной перед лицом развивающихся кибер-угроз.

Шаги 4–7 (Защищённые каналы связи, мониторинг и анализ в режиме реального времени, алгоритмы обнаружения угроз, механизм обратной связи) выполняются последовательно, чтобы обеспечить непрерывную адаптивную защиту от возникающих угроз фишинга и мошенничества во время сеанса пользователя.

G. Преимущества,-ы недостатки и значимость предлагаемого решения

Патент иллюстрирует важную эволюцию от реактивного обнаружения фишинга на основе сигнатур к более динамичному адаптивному подходу, основанному на статистическом моделировании. Предлагаемое патентное решение демонстрирует комплексный подход к обеспечению безопасности онлайн-транзакций и защите пользователей от несанкционированного доступа и мошеннических действий. Решение включает в себя несколько компонентов, таких как аутентификация пользователя, верификация веб-сайта, безопасные каналы связи, мониторинг и анализ в режиме реального времени, алгоритмы обнаружения угроз и механизм обратной связи.

Преимущества

- **Повышенная безопасность**: предлагаемое решение обеспечивает многоуровневый подход к обеспечению безопасности, гарантируя защиту пользовательских данных и транзакций от несанкционированного доступа и мошеннических действий.
- **Обнаружение угроз в режиме реального времени**: компонент мониторинга и анализа в режиме реального времени позволяет системе обнаруживать потенциальные угрозы, обеспечивая своевременное вмешательство и снижение рисков.
- **Аутентификация пользователя**: компонент аутентификации пользователя гарантирует, что только авторизованные пользователи могут получать доступ к сети и выполнять транзакции, предотвращая несанкционированный доступ.
- **Проверка веб-сайта**: компонент проверки веб-сайта гарантирует, что пользователи взаимодействуют с легитимными веб-сайтами, предотвращая фишинговые атаки.
- **Безопасные каналы связи**: компонент безопасных каналов связи обеспечивает защиту данных, передаваемых между сторонами, предотвращая перехват или манипулирование злоумышленниками.
- **Механизм обратной связи**: механизм обратной связи позволяет пользователям сообщать о потенциальных угрозах или ложных срабатываниях, позволяя системе постоянно повышать свою точность и эффективность.

Ограничения:

- **Сложность**: предлагаемое решение включает в себя несколько компонентов, для внедрения и обслуживания которых могут потребоваться значительные ресурсы и опыт.
- **Ложноположительные результаты**: алгоритмы обнаружения угроз иногда помечают легитимные действия как потенциальные угрозы, что приводит к ненужным предупреждениям и сбоям в работе пользователей.
- **Расходы**: поддержание работоспособности системы и оплата платы за обслуживание в течение 20 лет могут быть дорогостоящими, что потенциально ограничивает ее доступность для небольших предприятий или частных лиц.

Значение

Предлагаемое патентное решение имеет важное значение в контексте кибербезопасности, поскольку оно устраняет растущую угрозу фишинга и онлайн-мошенничества. Многоуровневый подход решения к обеспечению безопасности и обнаружение угроз в режиме реального времени делают его ценным инструментом для защиты пользовательских данных и транзакций в эпоху цифровых технологий. Однако его сложность и дороговизна ограничивают его применение небольшими предприятиями или частными лицами.

1) Аутентификация пользователя

Компонент предназначен для проверки личности пользователей перед предоставлением им доступа к защищённым ресурсам и играет жизненно важную роль в обеспечении безопасности конфиденциальных данных и систем. Несмотря на наличие ограничений и проблем, связанных с аутентификацией пользователя, её преимущества и значимость в контексте кибербезопасности делают её важнейшим аспектом любой комплексной стратегии обеспечения безопасности.

Преимущества

- **Повышенная безопасность**: аутентификация пользователя помогает защитить системы, приложения и сети, идентифицируя личность пользователя и гарантируя, что только авторизованные пользователи могут получить доступ к конфиденциальным данным.
- **Улучшенная подотчётность**: аутентификация пользователей позволяет организациям отслеживать их активность, предоставляя журнал аудита, который можно использовать для расследования подозрительного поведения или разрешения споров.
- **Защита от кражи личных данных**: требуя от пользователей подтверждения своей личности перед доступом к конфиденциальной информации, аутентификация пользователя может помочь предотвратить кражу личных данных.
- **Повышенное доверие**: аутентификация может повысить доверие между пользователями и

организациями, предоставляя безопасный и достоверный способ доступа к информации.

Ограничения

- **Уязвимость к фишинговым атакам:** аутентификация на основе пароля подвержена фишинговым атакам, поскольку многие люди используют простые, легко запоминающиеся пароли.
- **Сложность и удобство использования:** некоторые методы аутентификации пользователей, такие как многофакторная аутентификация, могут быть сложными для пользователей в управлении, что приводит к потенциальному разочарованию и снижению удобства использования.
- **Вероятность ложноположительных результатов:** системы аутентификации пользователей могут иногда помечать легитимные действия как потенциальные угрозы, что приводит к ненужным предупреждениям и сбоям в работе пользователей.

Значение

- **«Бастион» безопасности**: аутентификация пользователя является важнейшим компонентом общей системы кибербезопасности, поскольку она защищает конфиденциальную информацию и предотвращает несанкционированный доступ к системам и данным.
- **Адаптивность**: методы аутентификации пользователей адаптированы к различным ситуациям и средам, таким как удалённая работа или различные отрасли с особыми требованиями соответствия.
- **Интеграция с другими мерами безопасности**: аутентификация пользователя может быть интегрирована с другими мерами безопасности, такими как многофакторная аутентификация, для обеспечения дополнительных уровней защиты и повышения общей безопасности.

2) Проверка веб-сайта

Компонент важен в различных отраслях, особенно в тех, которые в значительной степени зависят от онлайн-транзакций и обмена конфиденциальной информацией. Компонент призван гарантировать, что пользователи взаимодействуют с легитимными веб-сайтами и не становятся жертвами фишинга или других мошеннических действий.

Преимущества

- **Повышенная безопасность**: благодаря проверке подлинности веб-сайтов, пользователи защищены от непреднамеренного обмена конфиденциальной информацией со злоумышленниками. Это особенно важно в таких отраслях, как банковское дело, электронная коммерция и здравоохранение, где часто происходит обмен конфиденциальными данными.
- **Повышение доверия**: проверка веб-сайта может повысить доверие пользователей к онлайн-сервисам, поскольку она обеспечивает уверенность в том, что они взаимодействуют с легитимной организацией.
- **Снижение уровня мошенничества**: предотвращая доступ пользователей к мошенническим веб-сайтам, значительно снижается риск финансовых потерь.

Ограничения

- **Вероятность ложноположительных результатов**: системы проверки веб-сайтов иногда помечают легитимные веб-сайты как потенциально мошеннические. Это вызывает неудобства для пользователей и привести к потере доверия к системе.
- **Зависимость от технологии**: эффективность проверки веб-сайта в значительной степени зависит от используемой технологии. Если технология устарела или недостаточно надёжна, она может не обнаруживать изощренные попытки фишинга.
- **Дополнительные расходы**: внедрение и поддержка системы проверки веб-сайта могут быть дорогостоящими, особенно для небольших предприятий. Это может удержать некоторые организации от внедрения этой технологии.

Значение

В условиях растущей распространённости фишинга и онлайн-мошенничества необходимость эффективной проверки веб-сайта становится более важной, чем когда-либо. Эта технология может обеспечить дополнительный уровень безопасности, помогая защитить пользователей и предприятия от потенциально разрушительных последствий онлайн-мошенничества.

3) Защищенные каналы связи

Компонент играет решающую роль в обеспечении безопасного обмена информацией между сторонами.

Преимущества

- **Защита данных**: безопасные каналы связи помогают защитить конфиденциальные данные от несанкционированного доступа, перехвата и манипуляций. Это важно в отраслях, которые обрабатывают конфиденциальную информацию, таких как финансовые учреждения, поставщики медицинских услуг и государственные учреждения.
- **Соблюдение нормативных актов**: во многих отраслях действуют строгие правила защиты данных. Защищённые каналы связи помогают организациям соблюдать эти правила, обеспечивая безопасную передачу данных.

- **Доверие и репутация**: внедрение безопасных каналов связи повышает репутацию организации и укрепляет доверие с её клиентами и партнёрами. Это приводит к повышению лояльности клиентов и улучшению деловых отношений.

Ограничения

- **Сложность**: внедрение и поддержание безопасных каналов связи может быть сложным и с технической точки зрения, и потребует специальных навыков и ресурсов, что может быть дорогостоящим для небольших организаций.
- **Накладные расходы на производительность**: шифрование и дешифрование данных приводит к задержке и снижению общей производительности каналов связи. Это является проблемой для приложений, которым требуется связь в режиме реального времени или с низкой задержкой.
- **Проблемы с совместимостью**: защищённые каналы связи совместимы не со всеми устройствами, приложениями или сетями. Это ограничивает их удобство использования и эффективность в определённых ситуациях.

Значение

С ростом распространённости кибер-угроз потребность в безопасных каналах связи становится более важной, чем когда-либо. Эта технология может обеспечить дополнительный уровень безопасности, помогая защитить пользователей и предприятия от потенциально разрушительных последствий утечек данных и кибератак.

4) Мониторинг и анализ в режиме реального времени

Компонент предназначен для непрерывного мониторинга и анализа активности системы, сетевого трафика и поведения пользователей для обнаружения потенциальных угроз и аномалий, и реагирования на них в режиме реального времени.

Преимущества

- **Раннее обнаружение угроз**: мониторинг и анализ в режиме реального времени позволяют организациям обнаруживать потенциальные угрозы и аномалии по мере их возникновения, обеспечивая более быстрое реагирование и сводя к минимуму потенциальный ущерб, причиняемый кибератаками.
- **Улучшенное реагирование на инциденты**: благодаря мониторингу в режиме реального времени группы безопасности могут более эффективно реагировать на инциденты, поскольку у них есть немедленный доступ к соответствующим аналитическим данным. Это может значительно сократить время, необходимое для локализации инцидентов безопасности и смягчения их последствий.
- **Проактивная безопасность**: мониторинг и анализ в режиме реального времени позволяют организациям перейти от реактивной системы безопасности к упреждающей. Благодаря постоянному мониторингу и анализу системных действий организации выявляют и устраняют потенциальные уязвимости до того, как ими воспользуются злоумышленники.

Ограничения

- **Сложность**: внедрение и обслуживание систем мониторинга и анализа в режиме реального времени может быть сложным и с технической точки зрения. Это может потребовать специальных навыков и ресурсов, что может быть дорогостоящим для небольших организаций.
- **Ложноположительные результаты**: системы мониторинга и анализа в реальном времени иногда выдаёт ложноположительные результаты, что приводит к ненужным оповещениям и увеличению нагрузки на службы безопасности. Этого можно избежать, выполнив тонкую настройку системы и используя передовые методы аналитики.
- **Проблемы с конфиденциальностью**: мониторинг и анализ в режиме реального времени вызывает проблемы с конфиденциальностью, поскольку они связаны со сбором и анализом конфиденциальных данных. Организации должны обеспечить соблюдение соответствующих правил защиты данных и внедрить соответствующие меры предосторожности для защиты конфиденциальности пользователей.

Значение

Технология предоставляет организациям наглядность и аналитические данные, необходимые им для обнаружения потенциальных угроз и реагирования на них в режиме реального времени, помогая защитить их активы и сохранить доверие их клиентов и партнёров.

5) Алгоритмы обнаружения угроз

Преимущества

- **Автоматическое обнаружение угроз**: алгоритмы обнаружения угроз автоматически анализируют огромные объёмы данных для выявления закономерностей и аномалий, которые могут указывать на кибер-угрозу. Такая автоматизация позволяет быстро обнаруживать потенциальные угрозы, сокращая время, необходимое для реагирования на них и смягчения их последствий.
- **Адаптивность к новым угрозам**: алгоритмы машинного обучения извлекают уроки из прошлых инцидентов и адаптируются к новым угрозам, повышая скорость и точность обнаружения угроз. Такая адаптивность позволяет алгоритмам обнаружения угроз оставаться актуальными в условиях постоянно меняющегося ландшафта кибер-угроз.

- **Улучшенное реагирование на инциденты**: системы кибербезопасности на базе искусственного интеллекта помогает автоматизировать процессы реагирования на инциденты, позволяя быстрее и эффективнее устранять угрозы. Автоматизация помогает снизить воздействие атаки и свести к минимуму причиняемый ущерб.

Ограничения

- **Сложность и неопределённость**: данные по кибербезопасности могут быть обширными, разнообразными и часто трудными для интерпретации. Такая сложность затрудняет точную обработку, анализ и обнаружение потенциальных угроз безопасности алгоритмами машинного обучения. Кроме того, киберпреступники постоянно разрабатывают новые тактики, приёмы и процедуры для обхода мер безопасности, что усложняет обработку данных.
- **Ограниченный контроль со стороны человека**: хотя искусственный интеллект и алгоритмы машинного обучения быстро обрабатывают и анализируют данные, они не всегда могут принимать точные решения независимо. Человеческий контроль по-прежнему необходим для обеспечения того, чтобы алгоритмы работали правильно, и чтобы ложноположительные или отрицательные результаты были сведены к минимуму. Однако из-за большого объёма данных, связанных с кибербезопасностью, людям трудно поспевать за скоростью и точностью искусственного интеллекта.
- **Предвзятость и дискриминация**: алгоритмы искусственного интеллекта и машинного обучения склонны к предвзятости и дискриминации, что может стать серьёзной проблемой в области кибербезопасности. Если алгоритмы обучаются на неполных данных или ошибочных предположениях, они могут принимать неправильные решения, которые имеют серьёзные последствия.

Значение

Важность алгоритмов обнаружения угроз заключается в их способности улучшать защиту кибербезопасности за счёт автоматизации процессов обнаружения угроз и реагирования на инциденты. Поскольку кибер-угрозы продолжают развиваться и становятся все более изощренными, потребность в усовершенствованных алгоритмах обнаружения угроз становится все более важной. Эти алгоритмы могут помочь организациям опережать потенциальные угрозы и более эффективно реагировать на них, что в конечном итоге улучшит их общее состояние кибербезопасности.

6) Механизм обратной связи

Компонент фокусируется на сборе и анализе отзывов пользователей для повышения общей производительности и действенности системы.

Преимущества

- **Постоянное совершенствование**: механизмы обратной связи позволяют организациям постоянно совершенствовать свои системы кибербезопасности путём выявления и устранения потенциальных слабых мест и уязвимостей.
- **Вовлечение пользователей**: вовлекая пользователей в процесс обратной связи, организации повышают вовлеченность пользователей и их удовлетворённость. Пользователи с большей вероятностью будут доверять и внедрять систему, которая учитывает их отзывы и вносит необходимые улучшения.
- **Проактивная безопасность**: механизмы обратной связи помогают организациям перейти от реактивной стратегии обеспечения безопасности к упреждающей. Собирая и анализируя отзывы пользователей, организации выявляют и устраняют потенциальные уязвимости до того, как ими воспользуются злоумышленники.

Ограничения

- **Сложность**: внедрение и поддержание эффективных механизмов обратной связи сложны и с технической точки зрения. Это может потребовать специальных навыков и ресурсов, что может быть дорогостоящим для небольших организаций.
- **Перегрузка обратной связью**: при неправильном управлении механизмы обратной связи приводят к накоплению огромного объёма данных, что затрудняет для организаций выявление наиболее важных проблем и определение их приоритетности. Этого можно избежать, используя передовые методы аналитики и расстановки приоритетов.
- **Проблемы с конфиденциальностью**: механизмы обратной связи вызывают проблемы с конфиденциальностью, т.к. они связаны со сбором и анализом конфиденциальных данных. Организации должны обеспечить соблюдение соответствующих правил защиты данных и внедрить соответствующие меры предосторожности для защиты пользователей.

Значение

Технология предоставляет организациям информацию, необходимую им для постоянного совершенствования своих систем кибербезопасности, помогая защитить их активы и поддерживать доверие их клиентов и партнеров.

БПЛА (МинОбороны США)

Аннотация – документ содержит анализ публикации "Системы противодействия беспилотным летательным аппаратам (CUAS)", опубликованный Штабом, Департаментом сухопутных войск в августе 2023 года. Анализ посвящён различным аспектам, включая их технологические компоненты, тактические рекомендации и последствия для специалистов по безопасности и различных отраслей промышленности.

Документ содержит качественную сводку о C-UAS, детализирующую технологические достижения, операционные стратегии и динамику рынка. Он полезен специалистам по безопасности, поскольку даёт представление о разработке, тестировании и внедрении технологий C-UAS. Анализ подчёркивает важность беспилотных летательных аппаратов в укреплении национальной безопасности, защите критически важной инфраструктуры и поддержании безопасности воздушного пространства. В нем также указывается необходимость постоянных инноваций и сотрудничества между заинтересованными сторонами отрасли для устранения растущих угроз, создаваемых беспилотными авиационными системами. Кроме того, выводы, содержащиеся в документе, ценны для различных отраслей промышленности, позволяя им разрабатывать надёжные механизмы защиты от угроз UAS и оставаться впереди на конкурентном рынке.

A. Введение

Документ под названием «Система противодействия беспилотным аппаратам (C-UAS)» был опубликован в августе 2023 года штабом Министерства армии и заменил предыдущую версию того же документа от 13 апреля 2017 года.

Документ содержит рекомендации для вооружённых сил по противодействию беспилотным авиационным системам (БПЛА) противника и предотвращению выполнения ими своей задачи. Он охватывает ряд тем, включая описание угроз БПЛА, планирование их применения на уровне бригады и ниже, оборонительные и наступательные действия для солдат и подразделений, ресурсы для дополнительной подготовки и примеры оборудования для противодействия беспилотным авиационным системам

Основная аудитория – это бригадные и нижестоящие командиры и штабы, младшие командиры на уровне роты, взвода и отделения. Оно применимо ко всем представителям армейской профессии: командующим, солдатам и гражданским лицам армии, как к действующей армии, Национальной гвардии, так и резерву армии США

Цель документа — установить, как армия предотвращает влияние опасных БПЛА на армейские операции. Подчёркивается, что противодействие БПЛА не является самостоятельным усилием или исключительной обязанностью какого-либо подразделения. Скорее, это часть локальных задач по обеспечению безопасности и контрразведки, за которые отвечает каждый солдат и подразделение. Цель состоит в том, чтобы создать многоуровневую защиту посредством сочетания активных и пассивных мер, которые не позволяют опасным БПЛА обнаружить, нацелить или уничтожить намеченную цель.

- Документ предназначен для того, чтобы предоставить наборы мероприятий по организации и проведению местной безопасности и контрразведки, возможность помешать вражеским беспилотным авиационным системам (БПЛА) выполнить свою задачу.
- Документ включает описание угроз для беспилотных авиационных систем, порядок их планирования на уровне бригады и ниже, оборонительные и наступательные действия, которые должны предпринять солдаты и подразделения, ресурсы для дополнительной подготовки и примеры оборудования для противодействия беспилотным авиационным системам.
- Основная аудитория данного руководства — командиры и штабы бригад и нижестоящих команд, младшие командиры на уровне роты, взвода и отделения.
- Руководство обеспечивает основу для противодействия беспилотным авиационным системам, обучения и учебных программ системы армейского образования, а также будущего развития возможностей в области доктрины, организации, обучения, материальной части, руководства и образования, персонала, средств и политики (известного как DOTMLPF-P).
- Ожидается, что командиры, штабы и подчинённые будут следить за тем, чтобы их решения и действия соответствовали применимым законам и правилам США, международным законам и, в некоторых случаях, законам и правилам принимающей страны, а также всем применимым международным договорам и соглашениям.

B. Угроза беспилотным авиационным системам

1) Введение

Распространение беспилотных авиационных систем (БПЛА) представляет собой серьёзную проблему для вооружённых сил, союзников и партнёров США. Противники используют эти относительно недорогие, гибкие и одноразовые системы, одновременно эксплуатируя присущие им трудности с установлением виновных и их последствиями для сдерживания.

БПЛА бывают разных размеров и возможностей. Более крупные могут иметь такую же смертоносность, как и крылатые ракеты, и могут запускаться из самых разных мест. БПЛА меньшего размера запускаются практически незамеченными, и их трудно обнаружить при маневрировании по полю боя, что делает их все более предпочтительным методом нанесения ударов тактического уровня.

БПЛА могут выполнять несколько различных задач отдельно или одновременно в одном полёте. Эти миссии включают разведку, наблюдение и рекогносцировку; осведомлённость о ситуации; формирование связи; доставка оружия; огневая поддержка; и психологическая атака и война.

БПЛА подразделяются на группы с 1 по 5 в зависимости от веса, рабочей высоты и скорости. Чем больше платформа, тем надёжнее её набор возможностей. Линии дифференциации между различными группами в оперативном отношении не являются жёсткими.

БПЛА состоит из всего необходимого для управления беспилотным летательным аппаратом. Сюда входят личный состав, полезная нагрузка (датчики или вооружение), станция управления, линии связи, система запуска и система эвакуации. Различные эшелоны и возможности сосредоточены на победе над разными частями системы.

Противодействие БПЛА является общей совместной и общевойсковой ответственностью. Командиры и штабы должны быть готовы решать эти проблемы на протяжении всего периода противостояния.

2) Задачи БПЛА

Технологии и возможности БПЛА растут, и, как следствие, расширяется и их военное применение. БПЛА может выполнять несколько различных задач отдельно или одновременно в одном полёте.

- **Разведка, наблюдение и рекогносцировка:** БПЛА предоставляют противникам современные возможности разведки, наблюдения и рекогносцировки практически в реальном времени через нисходящую видеосвязь.
- **Ситуационная осведомлённость:** БПЛА обеспечивают обзор угрозы с воздуха, чтобы узнать, «что находится вокруг холма», и позволить командиру противника корректировать оперативные приказы на основе разведданных в реальном времени.
- **Ретрансляция связи:** БПЛА служит для расширения связи между наземными войсками в ухудшенной или ограниченной среде связи.
- **Доставка оружия:** БПЛА используются либо для доставки боеприпасов к цели, либо сам БПЛА может стать блуждающим боеприпасом. Сюда входят химические и радиологические атаки.
- **Огневая поддержка:** БПЛА используется для обеспечения функции передового наблюдателя, что позволяет корректировать огонь с закрытых позиций.
- **Психологическая война:** БПЛА, рассматриваемые как платформа для доставки оружия или ведения разведки, наблюдения или рекогносцировки перед атакой, могут вызвать панику уже одним своим присутствием.

Блуждающий боеприпас — это тип БПЛА, предназначенный для поражения наземных целей за пределами прямой видимости с помощью взрывной боеголовки. Они оснащены электрооптическими и инфракрасными камерами высокого разрешения, которые позволяют диспетчеру определять местонахождение, наблюдение и направлять транспортное средство к цели. Определяющей характеристикой блуждающих боеприпасов является способность «зависать» в определённой зоне воздушного пространства в течение длительного периода времени перед нанесением удара, что даёт диспетчеру время решить, когда и по чему нанести удар.

3) Группы БПЛА

Представлен обзор различных групп беспилотных авиационных систем (БПЛА) в зависимости от их веса, рабочей высоты и скорости.

БПЛА подразделяются на пять групп: от группы 1 до 5. Классификация основана на весе, рабочей высоте и скорости БПЛА. Чем больше платформа, тем надёжнее её набор возможностей.

- **БПЛА группы 1,** также известные как микро/мини, весят от 0 до 20 фунтов, работают на скорости менее 100 узлов и на высоте менее 1200 футов над уровнем земли (AGL). Как правило, это готовые коммерческие радиоуправляемые платформы с ручным запуском, ограниченной дальностью действия и небольшой полезной нагрузкой.
- **БПЛА группы 2,** или небольшие тактические, весят от 21 до 55 фунтов, работают на скорости от 101 до 250 узлов и на высоте менее 3500 футов над землёй. У них небольшие планеры с низкими радиолокационными характеристиками, обеспечивающие среднюю дальность и долговечность.
- **БПЛА группы 3,** или тактические, весят от 56 до 1320 фунтов, работают на любой скорости и на высоте менее 18 000 футов. Они требуют большего логистического пространства, а их дальность

действия и долговечность значительно различаются в зависимости от платформы.

- **БПЛА группы 4,** или стратегические, весят более 1320 фунтов, работают на любой скорости и на высоте менее 18 000 футов. Это относительно крупные системы, работающие на средних и больших высотах, с увеличенной дальностью и долговечностью. Обычно им требуется взлётно-посадочная полоса для запуска.
- **БПЛА группы 5,** или стратегические БПЛА, весят более 1320 фунтов, работают на любой скорости и на высоте более 18 000 футов. Они действуют на средних и больших высотах и обладают наибольшей дальностью полёта, долговечностью и скоростью полёта. Им требуется большая логистическая база и имеется набор оптики для наведения на цель и вооружения для боевых действий.

Группы БПЛА 1 и 2 широко известны как малые беспилотные авиационные системы (sUAS). У них меньшая радиолокационная эффективность, чем **у БПЛА групп 3, 4 и 5,** что затрудняет их обнаружение с помощью средств раннего предупреждения и обнаружения. Например, DJI MAVIC и Enterprise Dual являются примерами БПЛА группы угроз 1, а RQ-11 Raven — «союзным» примером.

4) Компоненты БПЛА

- БПЛА состоит из беспилотного летательного аппарата, полезной нагрузки (датчиков или вооружения), станции управления, линий связи, системы запуска и системы эвакуации. Различные эшелоны и возможности сосредоточены на победе над разными частями системы.
- Когда используется БПЛА, потенциально задействовано до четырёх различных каналов связи: нисходящий канал глобальной системы позиционирования (GPS) канала L1, канал управления и контроля (C2), нисходящий канал видео и канал передачи данных. Каждая из этих ссылок может быть целью нарушения или эксплуатации.
- Нисходящий канал GPS канала L1 необходим для определения того, какой путь вверх или вниз, а также его высоту. Он необходим, если БПЛА необходимо долететь до определённой точки.
- Канал C2 — это связь между контроллером и БПЛА. Он используется для управления БПЛА, и его можно отключить, чтобы БПЛА вернулся в исходную точку или приземлился.
- Нисходящая линия видео используется для отправки видео в реальном времени с БПЛА на контроллер. Нарушение этой связи может «ослепить» оператора.
- Канал передачи данных используется для отправки других данных с БПЛА на контроллер. Это может включать состояние системы, координаты GPS или другие данные датчиков.
- Целевые ячейки должны сосредоточиться на трех основных компонентах: БПЛА, контроллере и каналах связи.

5) Типы БПЛА

БПЛА подразделяются на группы в зависимости от веса, рабочей высоты и скорости. Каждый тип БПЛА имеет свои преимущества и ограничения. БПЛА с неподвижным крылом обладают большой долговечностью и могут покрывать большие территории, но им требуется взлётно-посадочная полоса. Винтокрылые БПЛА могут взлетать и приземляться вертикально, что делает их пригодными для операций в ограниченных пространствах, но обычно они имеют меньшую дальность полёта и продолжительность полёта по сравнению с БПЛА с неподвижным крылом. БПЛА-воздушные шары могут оставаться в воздухе в течение длительного времени, обеспечивая постоянное наблюдение за территорией, но они зависят от ветра и погодных условий и имеют ограниченную манёвренность.

a) БПЛА с неподвижным крылом

БПЛА с неподвижным крылом обычно относятся к группам 4 и 5, которые характеризуются массой более 1320 фунтов и могут работать на любой скорости. Эти БПЛА работают на средних и больших высотах и обладают наибольшей дальностью полёта, долговечностью и скоростью полёта. Им требуется большая логистическая площадь, аналогичная пилотируемым БПЛА, и они имеют набор оптики для наведения на цель и вооружения для боевых действий. Примеры БПЛА с неподвижным крылом включают MQ-1C Grey Eagle, MQ-1A/B Predator, RQ-4 Global Hawk и MQ-9 Reaper.

b) Винтокрылый / Мультироторный БПЛА

Винтокрылые или мультироторные БПЛА обычно относятся к группам 1 и 2, которые характеризуются массой от 0 до 55 фунтов и скоростью менее 100 узлов. Эти БПЛА работают на высоте менее 1200 футов над уровнем земли (AGL) для Группы 1 и менее 3500 футов над уровнем земли для Группы 2. Обычно они представляют собой запускаемые вручную радиоуправляемые платформы с ограниченной дальностью действия и небольшой полезной нагрузкой. Они предлагают видео в реальном времени и работают в пределах прямой видимости пользователя. Примеры винтокрылых БПЛА включают DJI MAVIC и RQ-11 Raven.

c) БПЛА на воздушном шаре

БПЛА-аэростаты потенциально могут попасть в любую из групп в зависимости от их веса, рабочей высоты и скорости. Они обычно используются для наблюдения и разведки из-за их способности оставаться в воздухе в течение длительного времени.

C. Планирование

Подчёркивается важность комплексного подхода к планированию и реализации БПЛА, включающего координацию всех эшелонов и боевых функций для обеспечения эффективной защиты от угроз.

1) Рекомендации по планированию

Эффективное планирование борьбы с БПЛА (C-UAS) требует общевойскового подхода, который задействует возможности всех боевых функций. Рекомендации при планировании включают многоуровневый подход к обороне, правила ведения боевых действий, контроль воздушного пространства, условия предупреждения ПВО, статус контроля над вооружением, сети раннего предупреждения и список приоритетной защиты (PPL).

2) Многоуровневый подход

Многоуровневая стратегия защиты при противодействии беспилотным авиационным системам (БПЛА) как подход сочетает в себе активные и пассивные меры по предотвращению обнаружения, нацеливания или уничтожения намеченных целей опасными БПЛА. Каждое действие, предпринимаемое на каждом эшелоне, усложняет использование вражеского БПЛА, увеличивая его риск и дальность полёта, на который он перемещается для выполнения своей миссии.

Каждый эшелон способствует выживанию солдат, создавая многоуровневую защиту. Эта многоуровневая защита представляет собой комбинацию активных и пассивных мер, которые не позволяют опасным БПЛА обнаружить, нацелиться или уничтожить намеченную цель. Каждое действие, предпринятое на каждом эшелоне, усложняет использование вражеского БПЛА, увеличивая его риск и дальность полёта, на которую он перемещается для выполнения своей миссии.

Многоуровневая защита обеспечивает множество возможностей для поражения, в идеале начиная с максимального расстояния от «союзных сил» и до того, как атакующий БПЛА сможет выпустить своё оружие.

План контроля воздушного пространства и план зональной противовоздушной обороны должны включать подробные процедуры обнаружения, идентификации, принятия решений и поражения угроз.

3) Правила участия

Излагаются обязанности командиров при противодействии опасным беспилотным летательным аппаратам (БПЛА). Условия предупреждения противовоздушной обороны (ADW) имеют цветовую маркировку, соответствующую степени вероятности воздушной угрозы, и используются для подготовки подразделений с учётом оценённой угрозы.

- На командиров возложена обязанность принимать необходимые меры для защиты своих сил и средств от атак, обеспечивая при этом соблюдение установленных правил ведения боевых действий (ПВД).
- Полномочия по использованию вражеских БПЛА могут быть делегированы на более низкие уровни, чтобы обеспечить более быстрое реагирование. Однако делегирование должно быть сбалансировано с риском ошибочного использования БПЛА при атаке союзных БПЛА.

4) Контроль воздушного пространства

Дивизии и бригады распределяют приказ о координации воздушного пространства (ОПВП), план воздушного пространства подразделения и текущую воздушную картину через системы управления, доступные подчинённым подразделениям.

Контроль воздушного пространства осуществляется дивизиями и бригадами посредством распределения приказа о координации воздушного пространства (АКО), плана воздушного пространства подразделения и текущей воздушной картины. Они распространяются через системы управления и контроля, доступные подчинённым подразделениям. Эти системы включают в себя вычислительную среду командного пункта (CPCE) и объединённую боевую командную платформу (JBC-P). Однако не все бригады и батальоны имеют доступ к тактической системе интеграции воздушного пространства (TAIS), которая представляет собой систему управления и контроля воздушной картины, командование и управление противовоздушной обороной передового района (FAADC2) или систему раннего предупреждения противовоздушной и противоракетной обороны системы (AMDWS). Подразделения, у которых нет ячеек противовоздушной обороны и управления воздушным движением (ADAM) и доступа к этим системам, не могут поддерживать осведомлённость о текущей воздушной обстановке. Они полагаются на высшие эшелоны этих систем для обмена и создания продуктов, которые они могут использовать.

Бригады и батальоны распределяют приказы по координации воздушного пространства и текущую воздушную картину подчинённым подразделениям посредством сочетания планирования, активных и пассивных мер и использования специального оборудования. Фаза планирования включает в себя рассмотрение каждого эшелона, а активные и пассивные меры являются частью многоуровневой стратегии защиты, предотвращающей обнаружение, наведение или уничтожение намеченной цели беспилотными авиационными системами (БПЛА).

Что касается систем управления и контроля, к которым подчинённые подразделения имеют доступ для координации воздушного пространства, в дивизии и выше существует множество систем, предназначенных для противодействия воздушным угрозам противника, каждый эшелон работает над тем, чтобы каждый солдат, независимо от того, где он находится на поле боя, обладает необходимой информацией и способностью обнаруживать, идентифицировать, принимать решения и, при необходимости, отражать любую воздушную угрозу.

Бригады и батальоны распределяют приказы о координации воздушного пространства (АКО) и текущую воздушную картину подчинённым подразделениям через системы управления, доступные этим подразделениям. Системы включают в себя вычислительную среду командного пункта (CPCE) и объединённую боевую командную платформу (JBC-P). Однако не все бригады и батальоны имеют доступ к тактической системе интеграции воздушного пространства (TAIS), которая представляет

собой систему управления и контроля, управляющую воздушной картиной, а также к системе управления и контроля противовоздушной обороны передового района (FAADC2), или воздушной и АРМ противоракетной обороны (AMDWS). Подразделения, у которых нет ячеек ПВО и управления воздушным движением (ADAM) и доступа к этим системам, полагаются на более высокие эшелоны с этими системами для обмена информацией и создания продуктов для их использования.

5) Состояние предупреждения ПВО

Подразделения создают сеть раннего предупреждения о воздушной угрозе, обычно передаваемую посредством частотной модуляции (FM), для обмена информацией о ситуации с воздушной угрозой среди подразделений, не имеющих специальных систем управления и контроля противовоздушной обороны.

Чтобы оценить способность своего подразделения проводить как пассивные, так и активные защитные меры против вражеских БПЛА, командующие могут использовать видео и другие данные, собранные с БПЛА. Данные могут дать представление о производительности подразделения и областях, требующих улучшения.

Подразделения должны интегрировать следующие ключевые задачи в свою подготовку в условиях предупреждения ПВО:

- Обучение наблюдателей тому, как искать и отслеживать беспилотные авиационные системы (БПЛА).
- Проведение обучения визуальному распознаванию угроз в воздухе.
- Практика различных пассивных мер.
- Сеть раннего оповещения

6) Статус управления оружием

Изложены условия, при которых средствам противовоздушной обороны разрешено противодействовать воздушным угрозам, включая беспилотные авиационные системы (БПЛА). Статус контроля над оружием устанавливает условия, при которых средствам противовоздушной обороны разрешено поражать угрозы, с тремя уровнями: оружие свободно, оружие закреплено и оружие удержано.

- **Статус контроля вооружения (WCS):** комплекс мер, определяющих условия борьбы с воздушными угрозами. Он адаптирован к тактической ситуации и может варьироваться в зависимости от системы вооружения, объёма воздушного пространства или типа воздушной платформы.
- Три WCS для C-UAS:
  - **Weapons Free:** подразделениям разрешено вступать в бой с любыми БПЛА, которые не идентифицированы как союзные в соответствии с правилами ведения боя (ROE). Этот статус является наименее ограничительным.
  - **Weapons Tight:** подразделениям разрешено атаковать только те БПЛА, которые однозначно идентифицированы как враждебные в соответствии с ROE.
  - **Weapons Hold:** подразделения могут стрелять только в целях самообороны или по приказу вышестоящего начальства. Этот статус является самым ограничительным.
- **Ячейка противовоздушной и противоракетной обороны бригады:** ячейка противовоздушной и противоракетной обороны (ПРО) бригады может создавать отдельные статусы для различных воздушных угроз или общего статуса управления для любого воздушного боя. Ячейка отвечает за интеграцию этих мер в более широкую стратегию противовоздушной обороны.
- **Принятие решений:** статус отражает необходимый уровень контроля над системами вооружения ПВО и зависит от текущей тактической ситуации. Командиры всех уровней должны сбалансировать необходимость быстрого реагирования с риском огня по своим или других непредвиденных последствий.

Статус контроля вооружения является важнейшим компонентом планирования противовоздушной обороны, гарантируя, что подразделения будут иметь чёткие указания о том, когда и как противостоять потенциальным воздушным угрозам, сводя при этом к минимуму риск огня по своим и сопутствующего ущерба.

7) Сеть раннего предупреждения

- **Создание сети раннего предупреждения:** всем подразделениям рекомендуется создать сеть раннего предупреждения о воздушной угрозе, которая обычно передаётся посредством частотной модуляции (FM). Сеть является средством обмена информацией о ситуации с воздушными угрозами для подразделений, которые не имеют специализированных систем управления и контроля ПВО.
- **Оповещение всех:** сеть раннего предупреждения предназначена для оповещения всех подразделений о потенциальных воздушных угрозах, повышая общую ситуационную осведомлённость и готовность сил.
- **Практика и эффективность:** подразделениям рекомендуется практиковаться в передаче информации с использованием сети, чтобы сократить время, необходимое для уведомления всех о воздушных угрозах. Эта практика имеет решающее значение для обеспечения эффективного и результативного функционирования сети при обнаружении реальных угроз.

8) Список приоритетной защиты (PPL)

Подразделения разрабатывают PPL, чтобы определить приоритетность использования назначенных или выделенных возможностей защиты, уделяя особое внимание защите критически важных активов.

В военных операциях целью списка приоритетной защиты является выявление и определение приоритетности защиты критически важных активов, которые необходимы для успеха миссии. PPL помогает командирам сосредоточить свои ограниченные ресурсы защиты на наиболее важных элементах в пределах своей зоны ответственности, таких как узлы управления и контроля, районы логистики или важные подразделения.

Ключевые компоненты списка включают в себя:

- **Критические активы:** люди, имущество, оборудование, деятельность, операции, информация, объекты или материалы, которые считаются необходимыми для миссии.
- **Критичность:** важность актива для миссии.
- **Уязвимость к угрозам:** восприимчивость актива к потенциальным угрозам.
- **Вероятность угрозы:** вероятность того, что угроза нацелится на актив или повлияет на него.

Списки можно использовать для определения приоритетности мер защиты персонала и оборудования путём:

- **Определение критически важных активов:** определение того, какие активы имеют жизненно важное значение для успеха миссии.
- **Оценка рисков:** оценка уязвимости и вероятности угрозы для каждого критического актива.
- **Приоритизация активов:** ранжирование критически важных активов на основе их критичности и оценённых рисков.
- **Распределение ресурсов:** направление возможностей защиты, таких как средства противовоздушной обороны, меры физической безопасности или усилия по маскировке и сокрытию, на активы с наивысшим приоритетом.
- **Непрерывная оценка:** регулярный анализ и обновление списков приоритетной защиты для отражения изменений в операционной среде, критичности активов или оценке угроз.

Список приоритетной защиты — это динамичный инструмент, который постоянно оценивается и пересматривается на каждом этапе или основном этапе операции. Он разрабатывается с использованием указаний командира бригады и дивизии во время анализа миссии. Рабочая группа по защите рекомендует приоритеты защиты и формирует списки на основе критичности, уязвимости и вероятности угрозы.

Список приоритетной защиты — это наиболее важные активы, которые необходимо защищать. Активы могут быть физическими, такими как здания или оборудование, а также цифровыми, такими как данные или программные системы. Список обычно используется в контексте военных операций или операций по кибербезопасности, где он помогает распределять ресурсы и стратегическое планирование усилий по обороне и защите.

С другой стороны, план защиты — это более широкий термин, который относится к любой стратегии или политике, предназначенной для защиты чего-либо. Это может включать страховые полисы, протоколы безопасности или планы аварийного восстановления. В плане защиты излагаются шаги, которые будут предприняты для защиты активов или отдельных лиц, на которых распространяется план.

Частота обновления списков может зависеть от различных факторов, таких как изменения в ландшафте угроз, введение новых активов или изменения стоимости или важности существующих активов. Однако обычно рекомендуется регулярно пересматривать и обновлять, по крайней мере, ежегодно или при возникновении существенных изменений.

Примеры мер защиты, которые могут быть приоритетными в PPL, включают:

- Внедрение надёжных мер кибербезопасности для критически важных цифровых активов, таких как межсетевые экраны, системы шифрования и обнаружения вторжений.
- Меры физической безопасности для важных зданий или оборудования, такие как системы наблюдения, контроль доступа и персонал службы безопасности.
- Регулярные аудиты и проверки для обеспечения эффективности мер защиты.
- Программы обучения и повышения осведомлённости персонала, обеспечивающие понимание им важности активов и способов их защиты.

9) Возможности планирования по эшелонам

Бригады и вышестоящие штабы интегрируют C-UAS в процесс принятия военных решений, нацеливания, разведывательной подготовки поля боя (ИПБ) и процессов защиты.

В каждом эшелоне используются различные возможности противовоздушной обороны, при этом подразделения и выше анализируют, и планируют смягчение угрозы БПЛА.

Бригаде и высшему штабу поручено включить C-UAS в процесс принятия военных решений, включая нацеливание, разведывательную подготовку поля боя (IPB) и стратегии защиты. Ячейки противовоздушной обороны и управления воздушным пространством (ADAM) и бригадного авиационного элемента (BAE) поддерживают управление воздушным пространством и развёртывание средств

противовоздушной обороны. Для борьбы с БПЛА необходим многоуровневый подход, при этом более высокие эшелоны предоставляют ресурсы, чтобы помочь нижним эшелонам смягчить угрозы БПЛА. Бригады несут ответственность за выполнение мер защиты и живучести от угроз БПЛА, а также за реагирование на любые другие непосредственные угрозы.

Подразделения и высшие эшелоны анализируют и планируют противодействие угрозе БПЛА, направляя возможности C-UAS на повышение живучести подчинённых сил и защиту критически важных активов. Эти средства выделеляются бригаде для обеспечения дублирования и взаимной поддержки с собственными системами вооружения бригады. Подразделения также обеспечивают поддержание общей оперативной картины угроз в воздухе в режиме реального времени. Хотя у большинства бригад отсутствуют специализированные возможности противовоздушной обороны, в их штате есть персонал, который помогает в планировании и координации действий по противовоздушной обороне как с высшими, так и с подчинёнными эшелонами. Батальоны, имеющие менее обширный штат, чем бригады, полагаются на продукцию и системы бригад для поддержки своих рот. Роты, у которых нет специального персонала, относятся к опасным БПЛА так же, как к любой другой угрозе.

10) Рекомендации по планированию уровня бригады

Бригады разрабатывают планы C-UAS для защиты, расположения активов, планирования сенсорного покрытия и проведения передвижения сил в соответствии с планами более высокого эшелона.

Вопросы планирования включают методы отчётности, надёжную идентификацию, распространение оповещений, правила ведения боевых действий и координацию с союзными командными узлами и пользователями воздушного пространства.

Бригады несут ответственность за разработку планов C-UAS для защиты союзных сил в пределах отведённых им территорий. Им поручено стратегическое размещение средств, планирование сенсорного прикрытия и координация движения сил в соответствии с планами и целями дивизии и корпуса. Сюда входит обновление приоритетных задач и обеспечение безопасности жизненно важных активов.

При планировании бригады следует учитывать методы отчётности, чёткое выявление угроз, распространение предупреждений и соблюдение правил ведения боевых действий.

- Распространение предупреждений ПВО и статусов контроля над вооружением.
- Постановка общих и специальных предупреждений ПВО на основе текущих оценок воздушных угроз.
- Корректировка списка приоритетной защиты (PPL) в соответствии с разведывательной подготовкой поля боя, уровнем риска и оценкой командира.
- Уточнение правил применения БПЛА.
- Установление того, кто имеет полномочия выявлять угрозы.
- Обновление и распространение полномочий подразделения.
- Координация сенсорного покрытия, которое может превысить собственные сенсорные возможности бригады.
- Сотрудничество с командными узлами союзных миссий и пользователями воздушного пространства для минимизации риска огня по своим.
- Установление порядка уведомления.
- Формирование подходящих командных или вспомогательных отношений между развёрнутыми возможностями C-UAS.

11) Бригада ADAM/BAE Cell

Ячейка бригады ПВО и управления воздушным пространством (ADAM) и ячейка бригадного авиационного элемента (BAE) работают вместе, чтобы максимизировать боевую эффективность систем противовоздушной обороны и минимизировать риск возникновения огня по своим и сопутствующего ущерба.

ADAM и BAE взаимодействуют для повышения боевой эффективности систем противовоздушной обороны и снижения вероятности возникновения огня по своим и сопутствующего ущерба. В их обязанности входит:

- Создание, управление и выполнение плана многоуровневой защиты C-UAS, который включает в себя планирование использования оборудования, датчиков и возможностей C-UAS, понимание оптимального использования различных систем C-UAS и понимание того, как возможности C-UAS влияют на безопасность. операции.
- Разработка и распространение плана воздушного пространства бригады, создание стандартных оперативных процедур для действий дружественной авиации и реагирования на воздушные угрозы, а также разработка тактики, методов и процедур противовоздушной обороны, адаптированных к предполагаемой угрозе.
- Интеграция возможностей союзных C-UAS в общую оперативную картину бригады.
- Сотрудничество с отделом разведки для разработки шаблона воздушной ситуации противника (SITEMP).
- Внедрение правил применения силы C-UAS вышестоящего штаба (ROE), правил применения силы и специальных инструкций (SPINS).
- Рекомендация командиру бригады РОЭ подразделений, правил применения силы и СПИНС.

- Внедрение и соблюдение необходимых политик и процедур принимающей страны для C-UAS.
- Оценка эффективности многоуровневой защиты C-UAS после боя C-UAS, корректировка по мере необходимости и предоставление обратной связи на основе извлечённых уроков как для более высоких эшелонов, так и для подчинённых подразделений.

Важно отметить, что возможности ADAM в боевой авиационной бригаде и бригаде повышения манёвренности не имеют авиационного оперативного компонента и, следовательно, имеют очень ограниченные возможности для выполнения функций BAE.

Ячейка бригады ADAM/BAE также поддерживает текущую оценку C-UAS, которая включает в себя местоположение и состояние всех средств C-UAS бригады, возможности доступного оборудования C-UAS, а также прошлую, текущую и ожидаемую активность БПЛА противника.

12) Планирование на уровне отдельных частей и подразделений

Батальоны объединяют управление бригадой, чтобы сформировать последовательную схему защиты и соответствующим образом формировать свои планы и действия C-UAS.

Батальоны создают сплочённую схему защиты, интегрируя командование бригад. Для эффективного противодействия неизвестным БПЛА батальонам необходима ситуационная осведомлённость о союзных БПЛА в своём районе. Планирование и действия батальона C-UAS определяются:

- Включение и совместное использование плана воздушного пространства подразделения для поддержания осведомлённости о союзных БПЛА, помощи в идентификации C-UAS и сокращения огня по своим.
- Использование руководства по атаке, процессов таргетинга и требований к отчётности для поддержки процесса таргетинга.
- Следуя инструкциям по координации ПВО и указаниям ПВО, которые информируют о применении средств и возможностей ПВО и C-UAS.
- Выбор наилучшего сочетания возможностей C-UAS для создания многоуровневой защиты.
- Понимание и интеграция усилий по сбору бригад и требований к отчётности.

Отдел разведки батальона в рамках разведывательной подготовки поля боя (IPB) производит материалы, которые помогают батальону разработать концепцию защиты, включая оценку угроз. Эта оценка охватывает:

- Потенциальная угроза группировкам БПЛА в районе действий батальона.
- Угроза возможностям БПЛА.
- Ожидаемое количество вражеских БПЛА.
- Методы применения БПЛА.
- Вероятные места запуска и эвакуации.
- Вероятная полезная нагрузка.
- Угроза планам полётов БПЛА.
- Согласование датчиков с бригадой.

Затем батальон разрабатывает концепцию защиты, которая включает действия C-UAS на основе оценок и анализа разведывательных данных, концентрируя ресурсы на эффективном смягчении последствий БПЛА и других угроз. Дополнительные инструкции для рот, такие как процедуры сообщения об угрозах с БПЛА, статус контроля над оружием и критерии применения, включены в инструкции по координации. Штаб батальона следит за тем, чтобы боевые учения всех подчинённых подразделений C-UAS соответствовали концепции защиты батальона.

Роты и ниже реализуют концепцию защиты, разработанную на уровне батальона, уделяя особое внимание реагированию на боевые учения о воздушном контакте и изучению активных и пассивных мер своего подразделения.

Концепция защиты, разработанная на уровне батальона, реализуется ротами и ниже. Основной акцент во время процедур командования войсками делается на реагирование на боевые учения по воздушному контакту. Командующие уровня роты и ниже проводят учения, и оценивают активные и пассивные меры своего подразделения. В ходе этих учения оцениваются такие аспекты, как расположение воздушной охраны, назначенные сектора, процедуры отчётности о БПЛА, планы связи, статус ADW, статус управления оружием, критерии поражения и идентификация угроз с БПЛА.

D. Защитные действия C-UAS

Основное внимание уделяется оборонительным действиям против беспилотных авиационных систем (БПЛА).

- **Обучение C-UAS:** подчёркивается важность обучения C-UAS, которое представляет собой отдельное ситуационное учение. Однако большая польза от обучения будет получена, если включить его в Образовательный план. Подразделения должны сосредоточиться на возможностях угроз БПЛА опасностях, которые представляют для подразделения, и связанных с ними боевых учениях после обнаружения БПЛА.
- **Ключевые задачи:** примеры ключевых задач для интеграции в обучение подразделений включают обучение визуальных наблюдателей поиску и отслеживанию БПЛА, проведение тренировок по визуальному распознаванию угроз в воздухе, отработку различных пассивных мер, а также

создание и использование сети раннего предупреждения.

- **Учебные пособия и симуляции.** командующие могут использовать специально разработанные учебные пособия, устройства и симуляции из центра поддержки обучения своей установки для повышения качества обучения коллективным задачам по поражению и смягчению угроз CUAS.
- **Оценка защитных мер:** командующие могут использовать видео и другие данные, собранные с летающего вражеского БПЛА, чтобы оценить способность своего подразделения проводить как пассивные, так и активные защитные меры.
- **Обновление обучения и образования:** Угроза БПЛА и методы их применения меняются быстрее, чем доктрина. Командующим рекомендуется обновлять свою подготовку и обучение, используя самую актуальную информацию, основанную на извлечённых уроках, тенденциях противника, а также союзных тактиках, методах и процедурах C-UAS.

1) Пассивные меры

Пассивные меры являются первой линией защиты от воздушных угроз и призваны повысить живучесть за счёт снижения вероятности обнаружения и нанесения ударов по союзным объектам.

Меры включают маскировку, рассредоточение, перемещение, а также усиление и защитное сооружение.

Эффективные методы маскировки имеют решающее значение, особенно против визуальных датчиков, поскольку они затрудняют обнаружение или идентификацию целей вражеских БПЛА.

Подразделения должны учитывать различные типы датчиков, такие как датчики ближнего инфракрасного и ультрафиолетового диапазона, и применять соответствующие контрмеры, например маскировка на местности.

Пассивные меры против угроз противодействия беспилотным авиационным системам (C-UAS) – это те, которые не предполагают активного воздействия или уничтожения угрозы. Они в первую очередь ориентированы на снижение эффективности угрозы с помощью таких методов, как обнаружение, идентификация и предотвращение.

- **Основы:** подчёркивает важность того, чтобы цели напоминали фон для уменьшения вероятности обнаружения БПЛА. Это предполагает навыки маскировки и сокрытия, а также понимание угрозы электромагнитных датчиков.
- **Модификация окружающей среды:** предлагается изменить физическую среду или использовать камуфляж для улучшения маскировки и предотвращения наблюдения.
- **Проблемы с сенсорами:** подчёркивается необходимость планирования действий по маскировке для поражения сенсоров противника во всем электромагнитном спектре.
- **Управление сигналами:** даны рекомендации по удалению источников сигнала, таких как излучение Wi-Fi или Bluetooth, которые могут привести к обнаружению в загородной среде.
- **Датчики визуального и ближнего инфракрасного диапазона:** обсуждается эффективная маскировка против визуальных датчиков и важность соблюдения световой дисциплины для противодействия датчикам ближнего инфракрасного диапазона.
- **Инфракрасные и ультрафиолетовые датчики:** рекомендуются натуральные материалы и местность для защиты источников тепла от инфракрасных датчиков, а также конкретные меры противодействия ультрафиолетовым датчикам в заснеженных районах.
- **Движение:** особое внимание уделяется минимизации движений для снижения риска обнаружения.

a) Оборонительные действия C-UAS

Подчёркивается важность слияния с окружающей средой, чтобы снизить вероятность обнаружения вражескими БПЛА.

- **Принцип камуфляжа и маскировки:** чем больше цель похожа на свой фон, тем труднее БПЛА, представляющему угрозу, различить их. Правильные навыки и осведомлённость об угрозе электромагнитных датчиков имеют решающее значение для эффективной маскировки и маскировки.
- **Изменение окружающей среды:** когда естественной маскировки недостаточно, вооружённые силы могут изменить физическую среду, чтобы улучшить маскировку персонала и активов. Они также могут использовать маскировку, чтобы сбить с толку или ввести противника в заблуждение.
- **Проблемы с датчиками:** камуфляж и маскировка должны учитывать разнообразие датчиков, которые работают во всем электромагнитном спектре. Командующие должны оценить свою тактическую ситуацию и соответствующим образом спланировать поражение сенсоров противника в визуальном, инфракрасном или радиолокационном спектрах.
- **Управление сигналами**: иногда более эффективно удалить источник сигнала, например излучение Wi-Fi или Bluetooth от интеллектуальных устройств, а не пытаться его замаскировать, особенно в средах, где гражданские сигналы не маскируют военные сигнатуры.
- **Визуальные и ближние инфракрасные прицелы:** жизненно важны эффективные методы камуфляжа и

сокрытия в визуальной части электромагнитного спектра. Полевая униформа, маскировочная краска и затемняющие средства на поле боя могут обеспечить эффективную маскировку от визуальных и ближних инфракрасных датчиков.

- **Инфракрасные и ультрафиолетовые датчики.** природные материалы и местность могут защитить источники тепла от инфракрасных датчиков. В заснеженных районах зимняя окраска и маскировка местности имеют решающее значение для защиты от ультрафиолетовых датчиков.
- **Методы камуфляжа:** подразделения должны свести к минимуму передвижение, избегать схем действий и управлять схемами использования оборудования, чтобы уменьшить вероятность обнаружения. При нанесении камуфляжа им также следует учитывать отражательную способность, форму, тень, текстуру и узоры объектов.
- **Дисциплина камуфляжа:** дисциплина камуфляжа и сокрытия является постоянной и применяется к каждому солдату. Это включает в себя регулирование света, тепла, шума, мусора и движения, чтобы не выдать расположение или действия отрядов.
- **Методы камуфляжа и сокрытия:** методы включают в себя сокрытие, смешивание, маскировку, разрушение и приманку. Они используются для экранирования, изменения или устранения характеристик и создания ложных целей, чтобы отвлечь внимание противника от реальных средств.
- **Обман с помощью ложных целей:** приманки можно использовать для привлечения внимания противника и отвода огня от реальных целей, повышая дружественную выживаемость и вводя противника в заблуждение относительно силы и местоположения.
- **Рассредоточение и перемещение:** рассредоточение распределяет войска и материалы для снижения уязвимости, тогда как перемещение предполагает избегания дальнейших атак или делает текущую атаку неэффективной.
- **Укрепление и защитная конструкция:** сюда входит усиление физической защиты ключевых активов посредством таких мер, как добавление мешков с песком или строительство бункеров для защиты от боеприпасов, доставляемых с помощью БПЛА.

b) Системы датчиков угроз

Важность эффективных методов маскировки в визуальной части электромагнитного спектра невозможно переоценить, поскольку визуальные датчики являются наиболее распространёнными, надёжными и своевременными. Невидимость часто затрудняет обнаружение, идентификацию и нацеливание. Полевая униформа, стандартные маскировочные раскраски, сверхлёгкая система камуфляжной сети (ULCANS) и затемняющие средства на поле боя эффективны против визуальных датчиков. Полная маскировка, в том числе вертикальная, позволяют избежать визуального обнаружения противником. Когда время ограничено, отдаётся предпочтение камуфляжу и сокрытию, чтобы защититься от наиболее вероятного направления атаки.

Прицелы ближнего инфракрасного диапазона эффективны на более коротких дистанциях. Красные фильтры, сохраняя ночное зрение, не могут помешать датчикам ближнего инфракрасного диапазона обнаруживать свет на больших расстояниях. Таким образом, строгая световая дисциплина является решающей мерой противодействия датчикам ближнего инфракрасного диапазона и визуальным датчикам, таким как усилители изображения. Стандартные маскировочные окраски, затемняющие поля боя и определённая униформа предназначены для противодействия датчикам ближнего инфракрасного диапазона.

Природные материалы и местность могут защитить источники тепла от инфракрасных датчиков и нарушить форму холодных и тёплых военных целей, наблюдаемых с помощью инфракрасных датчиков. Не стоит поднимать капоты транспортных средств, чтобы избежать бликов на лобовом стекле, так как это приводит к появлению горячей точки для инфракрасного обнаружения. Даже если инфракрасная система сможет обнаружить цель, её личность все равно можно замаскировать. Следует избегать разжигания костров, разведения пожаров и использования автомобильных обогревателей. Затеняющие вещества, устойчивые к инфракрасному излучению, химически стойкие краски и определённая униформа созданы для того, чтобы помочь разрушить инфракрасные сигнатуры, но они не подавляют инфракрасные датчики.

Использование противником ультрафиолетовых датчиков представляет значительную угрозу в заснеженных районах. Зимние раскраски, лёгкая камуфляжная система в арктическом стиле (известная как LCSS) и маскировка местности являются важнейшими средствами защиты от этих датчиков. Любой вид дыма нейтрализует ультрафиолетовые датчики. Целесообразные на местах контрмеры, такие как возведение снежных стен, также обеспечивают средство защиты от ультрафиолетовых датчиков.

Чтобы победить различные датчики, подразделениям необходимо свести к минимуму движение и избегать оперативных шаблонов. Движение привлекает внимание противника и оставляет несколько следов (шум, горячие точки, пыль). В операциях, которые по своей сути связаны с движением (например, в наступательных задачах), командующие планируют и управляют движениями так, чтобы сигнатуры были максимально сокращены. Если необходимо совершить движение, медленное, регулярное движение обычно менее очевидно, чем быстрое и беспорядочное.

Противник часто может обнаружить и идентифицировать различные типы подразделений или операций, анализируя характерные черты, сопровождающие их действия. Например, наступлению обычно предшествует продвижение вперёд инженерных средств для уменьшения препятствий. Такие перемещения очень трудно скрыть; поэтому в качестве альтернативы можно изменить схему пополнения запасов. Противник распознает неоднократное использование одних и тех же методов камуфляжа и сокрытия.

Чтобы эффективно замаскироваться от воздушного наблюдения, подразделения учитывают точку зрения угрозы. Предотвратить закономерности в противодействии обнаружению можноприменяя следующие факторы распознавания к тактическим ситуациям: контраст цели с её фоном: отражение, форма, тень, текстура и узоры.

К эффективным методам камуфляжа и сокрытия от визуальных датчиков относятся:

- **Естественный камуфляж:** использование природных элементов, таких как листва, деревья и местность, для слияния с окружающей средой.
- **Искусственный камуфляж:** использование камуфляжных сетей, красок и униформы, соответствующих окружающей среде.
- **Маскировка:** изменение внешнего вида, чтобы он напоминал что-то другое, например природный или безобидный объект.
- **Контроль теней и света:** использование теней и контроль отражающих поверхностей, чтобы избежать обнаружения.
- **Контроль движений:** ограничение ненужных движений, особенно в светлое время суток, чтобы не привлекать внимания.

Для поражения датчиков ближнего инфракрасного диапазона подразделения могут:

- **Использование материалов, блокирующих ИК-излучение:** некоторые материалы могут блокировать или поглощать ИК-излучение, что делает их эффективными для маскировки.
- **Контроль тепловых следов:** минимизация теплового излучения от тел, оборудования и транспортных средств поможет избежать обнаружения датчиками ближнего инфракрасного диапазона.
- **Использование дыма:** некоторые виды дыма блокируют датчики ближнего инфракрасного диапазона.

Меры противодействия ультрафиолетовым датчикам в заснеженных районах включают:

- **Материалы, поглощающие УФ-излучение:** использование материалов, поглощающих УФ-излучение, может помочь замаскироваться от УФ-датчиков.
- **Снежный камуфляж:** использование белого камуфляжа или камуфляжа со снежным рисунком поможет слиться с заснеженной средой.
- **Избегание материалов, отражающих УФ-излучение:** некоторые материалы, например некоторые металлы, могут отражать ультрафиолетовый свет, их следует избегать.

К эффективным методам камуфляжа и сокрытия от датчиков ближнего инфракрасного диапазона относятся:

- **Использование материалов, поглощающих инфракрасное излучение:** некоторые материалы, такие как специальные краски и ткани, могут поглощать инфракрасное излучение, делая объекты, покрытые ими, менее видимыми для датчиков ближнего инфракрасного диапазона.
- **Тепловой камуфляж:** включает в себя управление тепловыми сигнатурами, чтобы они сливались с окружающей средой. Этого можно добиться, используя термоодеяла или костюмы, маскирующие тепло, излучаемое телом человека или оборудованием.
- **Естественное укрытие:** использование природных элементов, таких как деревья, кусты и местность, может помочь разрушить и скрыть инфракрасные сигнатуры.

Эффективные меры противодействия ультрафиолетовым датчикам в незаснеженных районах включают:

- **Материалы, поглощающие УФ-излучение:** использование материалов или покрытий, поглощающих УФ-излучение, снизит видимость для УФ-датчиков.
- **Естественное покрытие:** как и в случае с инфракрасным камуфляжем, использование натуральных элементов поможет скрыть ультрафиолетовые сигнатуры.
- **Дым:** некоторые виды дымаэффективно рассеивают УФ-излучение, что затрудняет обнаружение объектов.

К эффективным способам обнаружения визуальных датчиков, используемых подразделениями противника, относятся:

- **Визуальное наблюдение:** обучение визуальных наблюдателей поиску и отслеживанию БПЛА (беспилотных авиационных систем) может быть эффективным методом обнаружения визуальных датчиков.
- **Пакеты средств электромагнитной борьбы:** помогают в обнаружении вражеских БПЛА, которые часто оснащены визуальными датчиками.

- **Использование радиолокационных систем.** такие системы, как радар управления огнём AN/APG-78 Longbow на ударном вертолёте Apache, помогают в обнаружении вражеских БПЛА.
- **Сеть раннего предупреждения:** создание и использование сети раннего предупреждения обнаруживает визуальные датчики, используемые вражескими подразделениями, и реагируют на них.

2) Активные меры

Активные меры включают в себя многоэтапную последовательность действий по обнаружению, идентификации, принятию решения и потенциальному задействованию неизвестного БПЛА.

Обнаружение затруднено из-за небольшого размера, манёвренности и бесшумности БПЛА. Условия окружающей среды и тактические манёвры опытных операторов могут ещё больше усложнить обнаружение.

Идентификация имеет решающее значение для предотвращения огня по своим и требует раннего определения союзных или враждебных характеристик БПЛА.

Принятие решения включает в себя определение необходимости применения и выбор соответствующих методов, которые могут быть физическими (например, стрелковое оружие, снаряды) или нефизическими (например, глушение, спуфинг).

Активные меры включают в себя тактику, методы и процедуры обнаружения, идентификации, принятия решений и борьбы с любой воздушной угрозой, включая БПЛА. Меры включают использование различных технологий и систем противодействия воздушным угрозам противника. Каждый военнослужащий, независимо от его местоположения на поле боя, должен иметь необходимую информацию и возможность реализовать эти активные меры.

*a) **Обнаружение***

Беспилотные авиационные системы (БПЛА) компактны, манёвренны и бесшумны, поэтому их сложно обнаружить даже обученным наблюдателям. Такие факторы, как время суток, условия освещения, погода и бдительность наблюдателя, могут повлиять на возможность обнаружения потенциально враждебного БПЛА. В связи с такими условиями окружающей среды требуется специализированная технология отслеживания и идентификации.

Опытные операторы БПЛА используют различные тактики, в том числе:

- Полёты на малых высотах, использование рельефа местности, вертикальных препятствий или городской среды для сокрытия приближения к цели.
- Выполнение многократных ложных взлётов и заходов на намеченную цель.
- Принятие беспорядочных схем полёта, чтобы сбить с толку персонал и затруднить визуальное отслеживание.
- Использование солнечного света или облачности, чтобы скрыть БПЛА из поля зрения.
- Полет против ветра для уменьшения заметного шума БПЛА.
- Использование спортивных режимов полёта для увеличения скорости и манёвренности, сокращая время наблюдения.
- Развёртывание нескольких БПЛА для запутывания и подавления наблюдателей, что усложняет отслеживание и нейтрализацию.
- Выполнение полёта по заранее запрограммированной траектории для снижения риска для оператора, позволяющее отключить линию управления в полёте и повторно установить её над целевой областью из другого места.

Способность обнаружения объекта определяется типом и размещением датчиков. На оптимальное размещение и использование датчиков влияют такие факторы, как типы вражеских БПЛА, местность, погода, анализ времени и расстояния, союзные защищаемые средства, желаемая зона поражения, требования к наблюдению и количество доступных средств.

Различные возможности датчиков, включая радиолокационные, радиочастотные, звуковые и оптические устройства, могут использоваться для формирования интегрированной сенсорной сети. Независимо от возможностей сенсоров, которыми обладает подразделение, все солдаты должны знать об угрозах с воздуха и постоянно смотреть вверх до и во время любых движений. Специально выделенные воздушные охранники могут помочь в обнаружении воздушной угрозы и борьбе с ней.

Типы датчиков и их размещение определяют возможности обнаружения устройства. Для размещения датчиков следует применять интеграцию и объединение в сеть для определения ситуации с БПЛА противника. Использование различных типов датчиков оправдано, поскольку в настоящее время не существует одного типа датчиков, который был бы на 100% эффективным.

Различные сенсорные возможности помимо визуальных (наблюдателей) могут включать в себя радиолокационные, радиочастотные, звуковые и оптические устройства. Цель состоит в том, чтобы сформировать интегрированную сенсорную сеть, включающую различные типы датчиков. Возможности датчиков для поддержки воздушных угроз на малом уровне планируются и координируются заранее. Командующему придётся координировать свои действия через более высокие эшелоны для получения дополнительных сенсорных возможностей. Выделенная воздушная охрана - ещё один способ, с помощью которого подразделения могут помочь в обнаружении воздушной угрозы и борьбе с ней.

b) Воздушная гвардия

Воздушная защита играет жизненно важную роль в обнаружении воздушных угроз и обеспечении раннего предупреждения. Гвардия должна быть оснащена необходимым оптическим оборудованием для выполнения методов поиска и сканирования, знать об угрозах и поддерживать визуальный контакт с целью на протяжении всего боя.

Воздушной гвардии поручено поддерживать постоянную бдительность, сосредоточив внимание на горизонте. Они отвечают за выявление воздушных угроз вблизи места расположения подразделения и заблаговременное предупреждение о потенциальных воздушных угрозах. Они прикрывают участки, где возможны подходы для авиации противника, и используются как в конных, так и в пеших наступательных и оборонительных операциях.

При наличии возможностей C-UAS воздушные охранники имеют право поражать цели в соответствии с правилами ведения боя (ROE) и статусом управления оружием. Они должны быть расположены в пределах видимости подразделения, обычно на расстоянии от 500 метров до 1,5 километров, чтобы эффективно обнаруживать, слышать и сообщать об угрозах.

Воздушная охрана должна быть способна действовать в любых условиях и быть оснащена необходимым оптическим оборудованием для проведения методов поиска и сканирования, снижающих возможности противника избежать обнаружения. При поиске БПЛА не должны сосредотачиваться исключительно на горизонте, так как это может привести к тому, что они пропустят БПЛА, летящий выше или ниже. Оптимальная дальность поиска — 20 градусов выше и ниже горизонта.

Метод вертикального сканирования оптимизирует зрение солдата для обнаружения воздушных угроз, перемещая взгляд вверх к небу, а затем вниз к горизонту, продолжая пересекать местность. Горизонтальное сканирование включает в себя движения глаз по небу, движение вверх примерно до 20 градусов, а затем сканирование вниз для обнаружения низколетящих угроз.

Контрольный список включает понимание типов и характеристик вражеских БПЛА, текущих тенденций БПЛА, местных воздушных угроз, оборудования обнаружения, доступного оборудования C-UAS, безопасных радио-операций, позывных подразделений, военных карт, методов ориентации и карт дальности.

c) Предупреждение

Решения о взаимодействии принимаются на основе серьёзности угрозы, потенциального влияния на эффективность подразделения и зоны поражения. Массированный огонь является эффективным методом применения стрелкового оружия против воздушных угроз.

При обнаружении воздушной угрозы крайне важно оперативно привести в готовность все союзные силы. Этого можно достичь с помощью двух стратегий: подхода «сверху вниз» или «снизу вверх». Малые беспилотные летательные аппараты (БПЛА) часто первыми обнаруживаются передовыми подразделениями, поэтому крайне важно отрабатывать использование сети раннего предупреждения подразделений и проводить учения. Независимо от используемого метода для передачи информации используется формат отчёта SALUTE. Получение этого отчёта должно побудить все подразделения предпринять дальнейшие действия, такие как остановка на месте или устранение угрозы летальными или несмертельными средствами. Если это возможно, подразделения, обнаруживающие воздушную угрозу, должны уведомить соседние подразделения.

При нисходящем подходе ячейки противовоздушной и противоракетной обороны (ПРО) на уровне бригады и выше выявляют угрозы и места оповещения, распространяя ранние предупреждения как в цифровом, так и в устном виде всем своим подчинённым подразделениям. Это делается автоматически из инструмента планирования штаба и информирования о боевой обстановке (в настоящее время AMDW) через JBC-P. Однако, поскольку не все цифровые системы функционируют должным образом или контролируются, также используется голосовая связь. Ячейка противоракетной обороны бригады использует радиочастотную модуляцию (FM) для передачи мгновенного сообщения о том, что в районе боевых действий обнаружен вражеский БПЛА, через оперативную и разведывательную сеть бригады. Это сообщение быстро передаётся по своим оперативным и разведывательным сетям батальонами, затем ротами по своей ротной сети и, наконец, взводами по своим внутренним сетям и, при необходимости, по необходимым системам связи отделения, чтобы обеспечить информирование всех. Этот процесс занимает много времени, поэтому чем быстрее передаются эти мгновенные сообщения, тем быстрее силы смогут отреагировать соответствующим образом.

При восходящем подходе любой наблюдатель, обнаруживший воздушную угрозу, инициирует обратный процесс. Они используют локальную сеть взвода для передачи флэш-сообщения, которое затем идёт в сеть роты, затем в оперативную и разведывательную сеть батальона и, наконец, в оперативную сеть бригады. Здесь ячейка ПВО бригады вводит необходимую информацию в соответствующую систему для обеспечения раннего оповещения по всему формированию. Первый эшелон с инструментом информирования о ситуации на поле боя (таким как JBC-P) создаёт цифровое предупреждение, помогающее быстро привести в готовность все формирование.

Независимо от того, как солдат был предупреждён, его первой реакцией при получении предупреждения о воздушной угрозе должно быть замирание, поскольку угроза может обнаружить движение. После быстрой оценки того, что в настоящее время за ними не наблюдают, им следует переместиться в укрытие и дождаться отчёта об отсутствии помех, прежде чем возобновить свою текущую миссию.

Одновременно с предупреждением союзные силы отслеживают цель и контролируют её перемещение. Это отслеживание должно продолжаться до тех пор, пока не

будет принято решение о поражении или отказе от поражения цели. Местоположение — это статический расчётный отчёт или отображение того, где в данный момент находится воздушная угроза. Системный трек — это совокупность отчётов о местоположении за определённый период времени. В зависимости от используемой системы траектория системы может отображаться в виде тепловой карты, предупреждения квадранта или круга для обозначения предполагаемого центра и ошибки местоположения или линии пеленга. План обнаружения напрямую демонстрирует способности подразделения непрерывно и эффективно отслеживать воздушные объекты.

d) Идентификация

Идентификация — это процесс определения того, является ли неизвестный обнаруженный контакт другом или врагом. Для эффективного использования возможностей противодействия беспилотным авиационным системам (БПЛА) решающее значение имеет раннее выявление беспилотных авиационных систем (БПЛА), позволяющее максимально увеличить время боя и предотвратить союзный огонь. Задача заключается в различении союзных, нейтральных и враждебных воздушных объектов при развёртывании различных систем вооружения против вражеских БПЛА, поскольку один и тот же БПЛА может эксплуатироваться как союзными, так и вражескими силами. Точная идентификация позволяет командующим принимать решения о взаимодействии и повышает осведомлённость о ситуации. Оперативная идентификация расширяет возможности применения оружия, помогает сохранить ресурсы и сводит к минимуму риск огня по своим.

Существует два метода идентификации: процедурный и позитивный. Позитивная идентификация, которая является предпочтительным методом, получается на основе наблюдения и анализа характеристик цели, включая визуальное распознавание, системы электронной поддержки, методы некооперативного распознавания целей, системы идентификации «свой-чужой» или другие методы идентификации, основанные на физике. С другой стороны, процедурная идентификация различает пользователей воздушного пространства на основе географии, высоты, курса, времени и манёвра. Обычно используется сочетание позитивной и процедурной идентификации.

Идентификация БПЛА в идеале должна вести к конкретному названию или категории или точной марке и модели БПЛА. Также важно, если возможно, идентифицировать его полезную нагрузку. Процесс присвоения треку идентификации будет зависеть от нескольких критериев.

e) Принятие решения

Фаза включает в себя два ключевых решения. Во-первых, определить, необходимо ли участие. Если решение о вступлении в бой принято, второе решение включает в себя выбор методов смягчения или нейтрализации угрозы, исходящей от БПЛА. Эти методы могут быть физическими или нефизическими, и некоторые организации могут обладать кибер-возможностями, охватывающими оба типа. Уровень делегирования соответствует правилам ведения боевых действий, доступному воздушному пространству, потенциальному побочному ущербу и неотъемлемому праву на самооборону.

Физические методы направлены на уничтожение или повреждение устройства, чтобы вывести его из строя. Примеры физических методов включают в себя:

- Взрывоопасные боеприпасы
- Стрелковое оружие
- Снаряды
- Методы запутывания, например распыляемая пена.
- Методы направленной энергии, такие как лазеры или мощные микроволны.
- Методы захвата, такие как сети

Методы стрелкового оружия, используемые в противовоздушной обороне, предполагают использование массированного огня и правильных точек прицеливания в зависимости от направления цели. Эти методы наиболее эффективны против низколетящих БПЛА из-за ограничений дальности и разрушительной способности стрелкового оружия. Решение о применении стрелкового оружия против вражеских БПЛА принимается командиром подразделения и зависит от ситуации, включая серьёзность угрозы, потенциальное влияние на эффективность подразделения и зону поражения (город или сельская местность).

Массированный огонь является эффективным методом применения огня из стрелкового оружия против воздушных угроз. Ключом к успеху является тушение большого количества огня по непосредственной угрозе. Даже если эти пожары не поражают врага, создание «свинцовой стены» в небе может запугать пилотов БПЛА, потенциально заставляя их прекратить атаку или отвлекая их от правильного прицеливания.

При принятии решения о поражении БПЛА стрелковым оружием каждое оружие (M4, M240, M249 и M2) должно использоваться с целью попадания как можно большего количества пуль на траекторию полёта противника. Это не означает, что все стреляют в каком-то случайном направлении. Вместо этого каждый выбирает точку прицеливания перед целью и стреляет в эту точку. Эта точка прицеливания определяется с помощью методики футбольного поля. Прежде чем вступить в бой, необходимо принять во внимание практические возможности, такие как дальность действия и возможности имеющегося оружия. Например, поражение БПЛА с дальности до 3 километров стрелковым оружием неэффективно, а лучшим вариантом может быть использование основного орудия на танке или гусеничной машине. Стрелковое оружие имеет низкую вероятность поражения атакующих БПЛА из-за его размера, скорости и манёвренности.

f) Техники поражения

Методы поражения применяются после того, как разрешение конфликтов в воздушном пространстве и полномочия по поражению целей передаются на тактический уровень. Эти методы могут быть нелетальными или летальными, и они могут потребовать устранения конфликтов на радиочастотах для предотвращения атаки по своим.

g) Техника футбольного поля

«Техника футбольного поля»– это простой подход к измерению расстояния упреждения. Идея основана на предположении, что большинство людей либо играли, либо смотрели футбол и поэтому имеют представление о длине футбольного поля. Когда им приказывают вести мишень на длину одного футбольного поля, все целятся примерно в одну и ту же точку пространства. Любые неточности в оценке длины футбольного поля одним человеком будут уравновешены оценкой другого человека. Такое изменение точек прицеливания гарантирует, что сосредоточенный огонь ведётся в пространство перед целью, а не в одну точку. Кроме того, различные точки обзора, с которых солдаты наблюдают за целью, будут способствовать дальнейшему распределению огня по большему пространству.

«Точки прицеливания», используемые для поражения угроз. Беспилотные летательные аппараты (БПЛА) различаются, но могут применяться к различным угрозам. Например, если вертолёты противника обнаружены и принято решение о вступлении в бой, их следует рассматривать как винтокрылые БПЛА группы 5. Правила выбора точек прицеливания просты, их легко выучить и запомнить.

«Техника огневой позиции из стрелкового оружия» одинакова для стрельбы из винтовки и противодействия БПЛА с использованием стрелкового оружия, за исключением положения лёжа. При стрельбе по БПЛА солдаты лежат на спине, направляя винтовки в воздух. Если вы находитесь в индивидуальной боевой позиции, оставайтесь там и открывайте ответный огонь из стойки с опорой. Если вы не находитесь на индивидуальной огневой позиции, вам следует поискать дерево, большой камень или поддерживающий объект, который поможет стабилизировать оружие и обеспечить защиту. Соответственно следует использовать следующие огневые позиции.

«Взаимодействие с пулемётами» эффективно против тихоходных БПЛА. Для поддержания громкости огня и поражения цели следует производить стрельбу непрерывной очередью из 20–25 выстрелов методом трассировки по цели, позволяющей наводчику корректировать выстрелы по цели.

«Нефизические методы» выводят из строя устройство, нарушая, блокируя или управляя сигналом между оптической станцией, станцией управления полётом и наземной станцией управления БПЛА. Несмотря на то, что в БПЛА используются нефизические методы, эти методы все равно могут привести к его сбою и нанести сопутствующий ущерб. Примеры нефизических методов включают, помимо прочего, радиочастотные помехи, помехи GPS, подделку GPS, ослепление, а также помехи положения, навигации и времени (известные как PNT).

h) Защита

Процесс поражения небольшой беспилотной авиационной системы (БПЛА) начинается после того, как разрешение конфликтов в воздушном пространстве и полномочия по поражению целей передаются на тактический уровень. Чтобы избежать огня по своим и подтвердить идентичность БПЛА, реализовано несколько процедур и процессов. В зависимости от метода взаимодействия может потребоваться устранение конфликтов на радиочастотах (РЧ). Могут быть случаи, когда рабочие радиочастотные спектры перекрываются с контрольной частотой БПЛА.

Меры поражения могут быть как несмертельными, так и летальными. В случае нелетального реагирования решающее значение имеет непрерывное создание помех до тех пор, пока БПЛА не выйдет из строя. После летального или несмертельного ответа, а также после того, как БПЛА потерял канал управления, следует запросить обезвреживание взрывоопасных боеприпасов, чтобы обеспечить безопасность БПЛА. Как только БПЛА будет признан безопасным, его можно будет отправить на разведку и анализ вооружений.

После принятия решения о задействовании и определения возможностей для этого выбранный потенциал развёртывается. Другие возможности продолжают отслеживать цель в случае неудачи первоначального поражения.

Эксплуатация является ключевым аспектом в разработке мер противодействия БПЛА. Следует предпринять усилия по сбору сбитых систем БПЛА и их компонентов. Когда солдаты сталкиваются со сбитым БПЛА, им следует использовать свою оптику с безопасного расстояния для поиска индикаторов подозрительных предметов, таких как взрывчатка, модификации или другие типы взрывчатых грузов. Если возможно, им следует проверить близлежащую территорию на предмет потенциально упавшего полезного груза или дополнительных приземлившихся БПЛА. Если взрывоопасных объектов не обнаружено, им следует собрать как можно больше БПЛА и ускорить его перемещение в свой более высокий эшелон для эксплуатации.

Если есть подозрение на опасность взрыва, БПЛА следует промаркировать и сообщить о действиях специалистам по обезвреживанию боеприпасов или другому обученному персоналу, как только позволят условия эксплуатации. Подразделения должны обозначить опасность инженерной лентой, панелью ВС-17 или любым другим прочным материалом высокой видимости, который позволит бригаде по обезвреживанию боеприпасов определить местоположение опасности на расстоянии от 50 до 100 метров. Местоположение предмета должно быть отмечено в системе ситуационной осведомлённости подразделения (например, JBC-P) или в системе Joint

Capabilities Release (известной как JCR) десятизначной сеткой. Подразделения запрашивают обезвреживание боеприпасов через своё командование, используя необходимые отчёты.

E. Наступательные действия C-UAS

Подчёркивается важность наступательных действий в противодействии угрозам БПЛА. Он представляет собой комплексное руководство по планированию и проведению наступательных операций C-UAS, подчёркивая необходимость разведки, сбора информации и эффективных стратегий нацеливания. Основное внимание уделяется наступательным действиям C-UAS.

1) Разведывательная подготовка поля боя

IPB имеет решающее значение для определения возможностей БПЛА, концепций использования, стратегий и тактик. Это непрерывный процесс, включающий определение операционной среды, описание воздействия на окружающую среду, оценку угрозы и определение плана действий.

БПЛА небольшие, манёвренные и тихие, что затрудняет их наблюдение (в полёте). Условия окружающей среды, время суток, уровень освещённости и бдительность наблюдателя — все это влияет на способность обнаружить потенциально враждебный БПЛА.

Опытные операторы могут использовать характеристики БПЛА, чтобы повысить их способность оставаться незамеченными. Тактика включает в себя полёт на малых высотах, использование местности и городской среды для маскировки подхода, ложные взлёты и заходы на посадку, использование неустойчивых профилей полёта и использование нескольких БПЛА, чтобы сбить с толку наблюдателей.

Типы датчиков и их размещение определяют возможности обнаружения устройства. Такие факторы, как типы вражеских БПЛА, местность, погода и количество доступных средств, влияют на то, как лучше всего размещать и использовать датчики.

Различные сенсорные возможности помимо визуальных могут включать в себя радиолокационные, радиочастотные, звуковые и оптические устройства. Цель состоит в том, чтобы сформировать интегрированную сенсорную сеть, включающую различные типы датчиков.

2) Сбор информации

Сбор информации скорректирован с учётом требований к информации об угрозах БПЛА, разработанных в ходе IPB. Аналитики определяют области и время, когда угроза, скорее всего, будет использовать БПЛА и средства сбора информации для удовлетворения приоритетных требований разведки.

Воздушная охрана отвечает за обнаружение воздушных угроз в непосредственной близости от места расположения подразделения и за раннее предупреждение, предупреждая подразделение о возможных воздушных угрозах.

Воздушная охрана должна иметь возможность проводить операции в любых условиях. Они должны быть оснащены необходимой оптической аппаратурой для выполнения методов поиска и сканирования, позволяющих снизить возможности противника по уклонению от обнаружения.

Контрольный список воздушной охраны включает понимание типов и характеристик вражеских БПЛА, понимание текущих тенденций БПЛА, конкретные данные о местных воздушных угрозах и названных областях интереса, оборудование обнаружения, безопасные радиосвязи и частоты для отправки раннего предупреждения, а также позывные подразделений. чтобы запросить поддержку.

3) Таргетинг

Эффективное нацеливание на вражеские БПЛА основывается на знаниях, полученных в ходе IPB и выполнении мероприятий по сбору информации. Подразделения согласовывают средства доставки, чтобы обеспечить летальные и несмертельные средства нападения на БПЛА.

Идентификация — это процесс определения союзных или враждебных характеристик неизвестного обнаруженного контакта. Использование возможностей противодействия БПЛА (C-UAS) требует раннего выявления БПЛА, чтобы максимально увеличить время взаимодействия и избежать огня по своим.

Существует два метода идентификации: процедурный и позитивный. Позитивная идентификация — это идентификация, полученная в результате наблюдения и анализа характеристик цели, включая визуальное распознавание, электронные системы поддержки, несовместные методы распознавания целей, системы идентификации «свой» или «передовой» или другие методы идентификации, основанные на физике.

Решение о вступлении в бой принимается на основе серьёзности угрозы в сравнении с потенциальным воздействием эффективности подразделения и зоны действия (городская или сельская). Физические методы воздействуют на устройство и либо разрушают, либо повреждают его, так что оно выходит из строя. Нефизические методы позволяют вывести устройство из строя, нарушая, блокируя или контролируя сигнал между оптической станцией, станцией управления полётом и наземной станцией управления БПЛА.

Методы поражения начинаются после того, как разрешение конфликтов в воздушном пространстве и полномочия по поражению целей передаются на тактический уровень.

4) Совместные обязанности

Борьба с БПЛА является совместной обязанностью: авиация ВВС, ВМС и Корпуса морской пехоты США помогает противостоять более крупным группам БПЛА посредством воздушного пресечения. Датчики повышенной высоты и армейские средства, такие как радар управления огнём AN/APG-78 Longbow на ударном вертолёте Apache, также могут помочь в обнаружении вражеских БПЛА.

F. Пример оборудования C-UAS'

Он предоставляет подробную информацию по обнаружению, идентификации, принятию решений и поражению беспилотных авиационных систем (БПЛА). В нем обсуждаются различные методы и оборудование, используемые в этих процессах, в том числе BLA CHATRI 2, DRONE BUSTER, MODI и SMART SHOOTER.

- **Обнаружение:** БПЛА небольшие, манёвренные и тихие, что затрудняет их наблюдение в полёте. На обнаружение могут влиять условия окружающей среды, время суток, уровень освещённости, погода и бдительность наблюдателя. Подчёркивается важность размещения датчиков и использования интегрированной сенсорной сети.
- **Идентификация:** обсуждается важность определения союзных или враждебных характеристик обнаруженного БПЛА. Точная идентификация позволяет командующим принимать решения о взаимодействии и повышает осведомлённость о ситуации. Идентификация БПЛА должна вести к конкретному названию или категории или точной марке и модели БПЛА.
- **Принятие решений:** включает в себя принятие решения о том, есть ли необходимость во вмешательстве, и, если да, то о методах, используемых для уменьшения или устранения угрозы, исходящей от БПЛА.
- **Поражение:** обсуждаются различные методы поражения БПЛА. К ним относятся физические методы, такие как взрывные боеприпасы, стрелковое оружие, снаряды, запутывание, направленная энергия и захват, а также нефизические методы, такие как радиочастотные помехи, глушение GPS, подмена GPS, ослепление, а также определение местоположения, навигация и время (PNT)

Bal Chatri 2 — это система, предназначенная для пассивного обнаружения радиочастот, в основном используемая для выявления потенциальной угрозы беспилотных авиационных систем (БПЛА). Она использует программно-определяемую систему радиочастотного обнаружения, специально предназначенную для обнаружения и идентификации дронов. Систему можно настроить для личного ношения или для использования в небольшом стационарном помещении.

Bal Chatri — это система обнаружения дронов, пассивно работающая на радиочастотах. Ключевые характеристики системы включают дальность обнаружения 3–5 километров, источник питания, который может представлять собой батарею PRC-148 или подключаемый модуль, срок службы батареи 4 часа и вес 2,5 фунта.

Drone Buster — это портативное устройство с батарейным питанием, предназначенное для противодействия угрозам со стороны беспилотных авиационных систем (БПЛА). Он специально разработан для нейтрализации БПЛА групп 1 и 2. Устройство использует уязвимости коммерческих протоколов связи дронов, позволяя оператору глушить управляющий сигнал и запускать заранее установленные процедуры «потеря сигнала» дрона.

Drone Buster действует на основе прямой видимости, поэтому оператору необходимо держать цель в поле зрения на протяжении всего боя. Если во время боя будет потеряна линия видимости, «угроза может восстановить контроль над БПЛА». Устройство предназначено для того, чтобы вывести из строя БПЛА как с дистанционным управлением, так и с GPS-наведением. Характеристики Drone Buster:

- Дальность: 400 м
- Источник питания: 1 аккумуляторная батарея BB2847.
- Срок службы батареи:
  - Непрерывное глушение: примерно 1 час
  - Непрерывное обнаружение: примерно 4-6 часов
  - Полная разрядка аккумулятора: примерно 10 дней

Modi — это портативная система радиоэлектронной борьбы, предназначенная для использования в спешке. Он предлагает возможность обнаруживать и нейтрализовать угрозы, уделяя особое внимание беспилотным авиационным системам (БПЛА). Система может функционировать независимо или быть дополнена установленным усилителем мощности для использования в фиксированной или навесной конфигурации, а также может быть демонтирована при необходимости. Он работает в диапазоне температур от -4 до 140 градусов по Фаренгейту. Ключевые характеристики системы Modi включают в себя:

- **Дальность действия**: 400 метров.
- **Источник питания:** три батарейки BB2590.
- **Срок службы батареи**: не указано.
- **Вес:** 40,25 фунтов в разобранном и упакованном виде.

Smart Shooter — это прицел для отдельных систем вооружения, предназначенный для противодействия угрозам, исходящим от беспилотных авиационных систем (БПЛА). Он может быть установлен на любой направляющей системы вооружения и совместим с существующими военными винтовками. Smart Shooter позволяет оружию стрелять только при правильном совмещении прицела с целью, включая учёт необходимого «упреждения» движущихся целей. Ключевые характеристики этой системы включают дальность действия 120 метров, источник питания в виде перезаряжаемой интеллектуальной литий-ионной батареи, срок службы батареи 72 часа или до 3600 вспомогательных выстрелов, а также вес 2 фунта 1 унцию.