I. Введение

US20220232015A1 – патент (за авторством Ravi Prasenna и Netskope, Inc.) подан 30 июля 2021 года и опубликован 21 июля 2022 года. Патент описывает решение, которое включает в себя систему сетевой безопасности, расположенную между клиентами и облачными приложениями. Эта система настроена на генерацию синтетического запроса с последующим его внедрением в сеанс приложения для передачи в облачное приложение. Система также включает встроенную логику формирования метаданных, настроенную для выдачи синтетических запросов.

Ниже рассмотрим публикацию US20220232015A1 с целью проанализировать различные аспекты этого документа, углубившись в его технические описания, новизну изобретения, которое в нем раскрывается, и его значение в более широком контексте его области. Также оценим качественную сущность патента, и идеи, которые не только проясняют его содержание, но и подчёркивают его значимость и потенциальное воздействие. Эта работа будет включать критическую оценку структуры документа, формулы изобретения и предлагаемых в нем технологических решений, тем самым обеспечивая детальное понимание его вклада в соответствующую область.

II. Ключевая идея

Основная идея патента заключается в создании системы сетевой безопасности, которая может эффективно отслеживать и контролировать поток файлов (документов) внутри корпоративной сети, уделяя особое внимание выявлению потенциальных угроз безопасности и управлению ими. Система использует встроенный прокси-сервер в качестве посредника между облаком и корпоративной сетью, контролируя файлы, поступающие извне. Он идентифицирует файлы документов, используя различные методы и метаданные, в том числе источник файла документа. Система также классифицирует документы как санкционированные (разрешённые без проверки на наличие угроз), внесённые в черный список (автоматически и навсегда блокируемые) или неизвестные (оценённые и потенциально помещённые в карантин для дальнейшего анализа). В патенте подчёркивается использование правил, основанных на политике, сканирование угроз и "песочница" для неизвестных или потенциально вредоносных документов.

В патенте представлено несколько ключевых моментов:

- **Система сетевой безопасности**: Патент описывает систему сетевой безопасности, которая устанавливается между клиентами и облачными приложениями. Эта система предназначена для повышения безопасности в облачных средах
- **Формирование синтетического запроса**: Система настроена на генерацию синтетического запроса и внедрение его в сеанс приложения, который затем передаётся в облачное приложение
- **Логика формирования встроенных метаданных**: Система включает описание логики формирования встроенных метаданных. Эта логика настроена на выдачу синтетических запросов, что может обеспечить дополнительные меры безопасности
- **Разделение синтетических запросов**: Раскрываемая технология относится к встраиваемому прокси-серверу, сконфигурированному с внедрением синтетического запроса. Он может формировать во время сеанса приложения синтетические запросы, которые отделены от входящих запросов
- **Принудительное применение облачной политики**: Внедрение синтетического запроса используется для извлечения метаданных для принудительного применения облачной политики.

A. Преимущества

Преимуществами предлагаемого решения являются:

- **Повышенная безопасность**: Система обеспечивает механизм мониторинга и управления потоком файлов документов в корпоративной сети, особенно тех, которые передаются через облачное хранилище
- **Проактивное обнаружение угроз**: Используя синтетические запросы для формирования метаданных, система может проактивно обнаруживать потенциальные угрозы безопасности и реагировать на них до того, как они повлияют на сеть
- **Динамическое применение политик**: Логика формирования встроенных метаданных обеспечивает динамическое применение политик облачной безопасности на основе метаданных в реальном времени, которые могут адаптироваться к изменяющимся ландшафтам угроз

- **Эффективность**: Система может повысить эффективность передачи данных за счёт автоматического блокирования известных вредоносных файлов без необходимости глубокого сканирования угроз, уменьшая задержку
- **Эффективное формирование метаданных**: Встроенная логика формирования метаданных выдаёт синтетические запросы для предоставления метаданных второй точке присутствия
- **Стабильность и согласованность**: Использование системой уникальных идентификаторов файлов гарантирует, что файлы можно будет отслеживать и управлять ими последовательно на протяжении всего их жизненного цикла, даже если их имена изменятся
- **Формирование синтетического запроса**: Система настроена с внедрением синтетического запроса, который может формироваться отдельно от входящих запросов во время сеанса приложения. Это может помочь в улучшении мониторинга и управления сетевым трафиком
- **Защита от вредоносных атак**: Система может идентифицировать и блокировать документы с известных вредоносных веб-сайтов, тем самым защищая сеть от потенциальных угроз
- **Гибкость и динамичность**: Система может адаптироваться к различным экземплярам (личным или корпоративным) и может обрабатывать документы из различных источников, таких как Google Drive, Docs, Sheets, и др.
- **Повышенная эффективность передачи данных**: благодаря автоматическому удалению внесённых в черный список URL-адресов, которые, содержат вредоносные объекты или ссылки, система сокращает время ожидания и повышает эффективность передачи данных

B. Недостатки

Недостатками предлагаемого решения являются:

- **Сложность**: Внедрение системы и управление ею могут усложнить сетевую инфраструктуру, требуя специальных знаний и потенциально увеличивая административные издержки
- **Ложные срабатывания**: Система может неправильно классифицировать подлинные документы как угрозы (ложные срабатывания) или не обнаруживать реальные угрозы (ложные негативы), что может нарушить нормальные бизнес-операции или сделать сеть уязвимой
- **Обслуживание и обновления**: Хранилище метаданных и правила политики могут нуждаться в регулярных обновлениях, чтобы соответствовать развивающимся угрозам, которые могут быть ресурсоёмкими и требовать постоянного внимания со стороны групп безопасности
- **Влияние на взаимодействие с пользователем**: Процесс блокировки и карантина документов может повлиять на взаимодействие с пользователем, особенно если подлинные документы задерживаются или если пользователям необходимо выполнить дополнительные шаги по обеспечению безопасности
- **Чрезмерная зависимость от известных угроз**: Эффективность системы против известных вредоносных сайтов и файлов может не распространяться на угрозы нулевого дня или сложные атаки, которые ещё не были идентифицированы и классифицированы
- **Влияние на производительность**: Дополнительная обработка, необходимая для формирования синтетических запросов и анализа метаданных, потенциально может повлиять на производительность сети, особенно в средах с высоким трафиком
- **Адаптивность**: Способность системы адаптироваться к новым типам облачных сервисов и приложений может быть ограничена её текущей конструкцией, что, в свою очередь, может потребовать дальнейшей доработки в связи с новыми технологиями
- **Проблемы с конфиденциальностью**: Сбор и анализ метаданных могут вызывать проблемы с конфиденциальностью, в зависимости от типа собираемых данных и способа их использования в системе
- **Стоимость**: Внедрение и эксплуатация такой системы безопасности могут повлечь за собой значительные затраты, включая аппаратное обеспечение и расходы на персонал

III. Система сетевой безопасности

"Система сетевой безопасности" — это система, предназначенная для повышения безопасности связи между клиентами и облачными приложениями:

- **Взаимодействие**: Система устанавливается между клиентами и облачными приложениями, действуя как посредник или прокси-сервер для мониторинга и потенциального изменения трафика
- **Внедрение синтетических запросов**: Система генерирует синтетические запросы, которые вводятся в сеансы приложения. Эти синтетические запросы используются для взаимодействия с облачными приложениями отдельно от реальных запросов клиентов
- **Встроенное формирование метаданных**: Система включает логику, которая генерирует встраиваемые метаданные в поток трафика. Эти метаданные используются для отправки синтетических запросов, которые могут быть использованы для

различных целей безопасности, таких как применение политики или оценка безопасности

- **Применение облачной политики**: Синтетические запросы используются для извлечения метаданных, которые имеют решающее значение для применения облачной политики безопасности. Это говорит о том, что система может динамически адаптировать и применять меры безопасности
- **Точки присутствия**: Система может включать в себя несколько точек присутствия, которые обеспечивают промежуточный трафик. Эти точки присутствия оснащены встраиваемой логикой формирования метаданных и способны выдавать синтетические запросы
- **Избыточность при синхронизации метаданных**: Система устраняет потенциальные избыточности при синхронизации метаданных между точками присутствия, что важно для поддержания согласованности и эффективности операций по обеспечению безопасности

A. Важность "Системы сетевой безопасности"

Система предназначена для контроля и мониторинга файлов, поступающих извне, особенно тех, которые передаются через облачное хранилище. Система использует встроенный прокси-сервер в качестве посредника между облаком и корпоративной сетью.

Система идентифицирует файлы документов, поступающие в корпоративную сеть, используя различные методы и метаданные, которые идентифицируют источник файла документа. Метаданные размещаются в хранилище метаданных, доступном прокси-серверу. Система позволяет документам, исходящим из санкционированных источников, таких как известные организации с предыдущим опытом работы в корпоративной сети, попадать в сеть без сканирования угроз.

Система также идентифицирует и блокирует файлы документов, полученные с известных вредоносных веб-сайтов. Это веб-сайты и URL-адреса, которые в прошлом были связаны с фишинговыми атаками или каким-либо другим образом ставили под угрозу сетевую безопасность. Хранилище метаданных отслеживает, хранит и поддерживает базу данных всех известных сайтов, внесённых в черный список.

Для неизвестных документов система оценивает их принадлежность и другие свойства метаданных, чтобы идентифицировать источник. Если источник документа не может быть идентифицирован, его доступ в корпоративную сеть временно блокируется. Это включает в себя правила, основанные на политике, и методы сопоставления. Документ помещён в карантин и первоначально проверяется на наличие угрозы. Если будет точно установлено, что может быть задействован вредоносный код, документ попадёт в изолированную среду для дальнейшего анализа

IV. Формирование синтетического запроса

"Формирование синтетических запросов" является ключевым компонентом системы сетевой безопасности, описанной в патенте. Формирование синтетических запросов — это метод, используемый в синтетическом мониторинге или тестировании, где создаются искусственные запросы для имитации реального пользовательского трафика. Эти запросы используются для взаимодействия с системами, такими как облачные приложения, отдельно от реальных запросов клиентов. Целью формирования таких запросов является тестирование и мониторинг производительности и функциональности систем, помогая выявлять потенциальные проблемы до того, как они затронут реальных пользователей.

- **Определение**: Формирование синтетических запросов включает в себя создание искусственных запросов, имитирующих реальный пользовательский трафик.
- **Назначение**: Синтетические запросы используются для тестирования и мониторинга производительности и функциональности систем. Они могут помочь выявить потенциальные проблемы и гарантировать корректную работу систем.
- **Использование в сетевой безопасности**: В контексте патента синтетические запросы вводятся в сеансы приложения и передаются в облачные приложения. Это позволяет системе взаимодействовать с облачными приложениями и извлекать метаданные в рамках принудительного применения облачной политики
- **Процесс формирования**: Синтетические запросы могут формироваться программно, часто с использованием скриптов или инструментов, предназначенных для синтетического мониторинга или тестирования. Эти инструменты могут имитировать различные сценарии, типы объектов и переменные среды
- **Преимущества**: Формирование синтетических запросов позволяет осуществлять упреждающий мониторинг производительности и функциональности системы. Это может помочь выявить проблемы на ранней стадии, прежде чем они затронут реальных пользователей, и может предоставить ценную информацию о времени безотказной работы системы, времени отклика и показателях успешности транзакций
- **Проблемы**: хотя формирование запросов может дать ценную информацию, это также сопряжено с трудностями. Например, может возникнуть ситуация, когда не полностью воспроизводится непредсказуемость реального поведения пользователей. Кроме того, требуется тщательное проектирование и реализация, чтобы гарантировать, что синтетические запросы точно представляют

взаимодействия, которые они призваны имитировать

Формирование синтетического запроса может использоваться в различных целях:

- **Нагрузочное тестирование**: Синтетические запросы могут использоваться для оценки поведения системы при большой нагрузке, помогая определить, есть ли вероятность сбоя веб-сайта или приложения из-за резкого увеличения трафика пользователей.
- **Мониторинг транзакций**: Разработчики или инженеры по контролю качества могут использовать синтетические запросы, чтобы определить, как система обрабатывает определённый тип запроса
- **Мониторинг компонентов**: В распределённых системах, таких как приложения микросервисов, синтетические запросы могут направляться к конкретным компонентам для измерения их отклика
- **Мониторинг API**: Синтетические тесты API позволяют инженерам оценить, управляют ли API запросами так, как требуется
- **Конфиденциальность данных**: Формирование синтетических данных может позволить создавать более крупные наборы данных, повысить производительность модели и защитить конфиденциальность отдельных пользователей.

Потенциальные области применения:

- **Разработка программного обеспечения и обеспечение качества**: Синтетические запросы могут использоваться для тестирования практически любого типа транзакции или запроса пользователя с любой целью. Если реальный пользователь может инициировать запрос, его также можно отслеживать синтетически
- **Сетевая безопасность**: Синтетические запросы могут использоваться для извлечения метаданных для принудительного применения облачной политики
- **Мониторинг производительности**: Компании могут использовать синтетическое тестирование для активного мониторинга доступности своих сервисов, времени отклика своих приложений и функциональности транзакций клиентов
- **Оптимизация взаимодействия с пользователем**: Синтетический мониторинг может использоваться для понимания того, как реальный пользователь может взаимодействовать с приложением или веб-сайтом, помогая выявить возможности для оптимизации

A. Значение

Значение формирования синтетических запросов заключается в её применении в системе сетевой безопасности для улучшения мониторинга и контроля взаимодействий с облачными приложениями:

- **Упреждающие меры безопасности**: Формирование синтетических запросов используется для упреждающего тестирования и мониторинга производительности и функциональности облачных приложений, что крайне важно для выявления и устранения потенциальных проблем безопасности до того, как они повлияют на реальных пользователей
- **Извлечение метаданных**: Встроенная логика формирования метаданных в системе сетевой безопасности выдаёт синтетические запросы на предоставление метаданных. Затем они используются для принудительного применения облачной политики, позволяя системе динамически адаптировать и применять меры безопасности
- **Применение облачной политики**: Синтетические запросы используются для извлечения метаданных, которые имеют решающее значение для применения облачной политики безопасности. Это говорит о том, что система может динамически адаптировать и применять меры безопасности на основе метаданных, полученных в результате синтетических запросов
- **Улучшенный мониторинг**: Синтетический мониторинг, который включает в себя генерацию синтетических запросов, является важнейшим компонентом мониторинга производительности сети и цифрового взаимодействия. Это позволяет командам ИТ-разработчиков, NetOps и DevOps улучшать взаимодействие с пользователями и оптимизировать критически важные для бизнеса функции
- **Универсальность тестирования**: Формирование синтетических запросов может использоваться для тестирования практически любого типа пользовательских транзакций или запросов для любых целей, обеспечивая комплексный подход к системному тестированию и мониторингу.

V. Встроенная логика формирования метаданных

Эта логика формирования встроенных метаданных является частью более широкой тенденции в области инноваций в области кибербезопасности, когда компании инвестируют в R&D для создания передовых решений безопасности, способных защитить от возникающих угроз в облачной и сетевой средах.

"Встроенная логика формирования метаданных" является ключевым компонентом системы сетевой безопасности:

- **Определение**: Логика формирования встроенных метаданных относится к

способности системы формировать метаданные "встраиваемо" или в режиме реального времени по мере прохождения трафика через систему с целью предоставления дополнительного контекста или информацию о обрабатываемых файлов

- **Функция**: Встроенная логика формирования метаданных настроена на выдачу синтетических запросов. Эти синтетические запросы используются для взаимодействия с облачными приложениями и извлечения метаданных для принудительного применения облачной политики.
- **Роль в сетевой безопасности**: система может динамически применять политики безопасности на основе метаданных, полученных в результате синтетических запросов
- **Точки присутствия**: Система включает в себя несколько точек присутствия, которые обеспечивают промежуточный трафик. Каждая из этих точек присутствия оснащена встраиваемой логикой формирования метаданных и способна выдавать синтетические запросы
- **Избыточности при синхронизации метаданных**: Система устраняет потенциальные избыточности при синхронизации метаданных между точками присутствия. Это важно для поддержания согласованности и эффективности операций по обеспечению безопасности

Цель встраиваемой логики формирования метаданных – выдавать синтетические запросы для взаимодействия с облачными приложениями и извлечения метаданных для принудительного применения облачной политики.

Логика формирования встроенных метаданных работает путём мониторинга потока трафика между клиентами и облачными приложениями. По мере прохождения трафика через систему логика генерирует метаданные в режиме реального времени. Затем эти метаданные используются для выдачи синтетических запросов, которые вводятся в сеансы приложения и передаются в облачные приложения.

Ключевыми моментами являются:

- **Создание метаданных в режиме реального времени**: логика предназначена для формирования метаданных в режиме реального времени по мере прохождения сетевого трафика через систему
- **Выдача синтетических запросов**: настройка на выдачу синтетических запросов, которые отделены от реальных запросов клиентов, для взаимодействия с облачными приложениями и извлечения необходимых метаданных
- **Применение облачной политики**: метаданные, формируемые встраиваемой логикой, используются для обеспечения соблюдения облачных политик безопасности, позволяя системе динамически адаптировать и применять меры безопасности
- **Операционная эффективность**: встроенное формирование метаданных помогает поддерживать операционную эффективность, гарантируя, что метаданные формируются и применяются к трафику без значительной задержки
- **Управление резервированием**: система может включать в себя несколько точек присутствия со встраиваемой логикой формирования метаданных, и это устраняет потенциальную избыточность при синхронизации метаданных между этими точками
- **Повышенная безопасность**: благодаря встраиваемому формированию метаданных система может проактивно реагировать на угрозы безопасности и более эффективно применять политики

Потенциальные области применения встраиваемой логики формирования метаданных:

- **Сетевая безопасность**: Встроенная логика формирования метаданных может использоваться для повышения сетевой безопасности путём динамического применения политик безопасности на основе метаданных, полученных из синтетических запросов
- **Разработка программного обеспечения и обеспечение качества**: Встроенная логика формирования метаданных может использоваться при разработке и тестировании программного обеспечения для мониторинга и анализа поведения приложений в режиме реального времени
- **Мониторинг производительности**: Встроенная логика формирования метаданных может использоваться для мониторинга производительности систем и приложений в режиме реального времени, помогая выявлять потенциальные проблемы до того, как они затронут реальных пользователей
- **Управление данными**: Встроенная логика формирования метаданных может использоваться в системах управления данными для отслеживания изменений и поддержания согласованности и эффективности операций
- **Разработка API**: логика формирования встроенных метаданных может использоваться при разработке API для предоставления дополнительного контекста или информации об обрабатываемых данных, повышая

функциональность и удобство использования API

- **R&D**: Поддержка воспроизводимых вычислительных исследований путём предоставления метаданных, документирующих вычислительные процессы и происхождение данных
- **Соответствие требованиям и управление**: обеспечение соответствия обработки данных соответствующим нормативным актам и политике управления

A. Значение встраиваемой логики формирования метаданных

Важность "встраиваемой логики формирования метаданных" заключается в том, что она расширяет возможности системы по обеспечению соблюдения политик облачной безопасности и повышению общей безопасности корпоративных сетей:

- **Формирование метаданных**: Встроенная логика формирования метаданных предназначена для выдачи синтетических запросов на предоставление метаданных. Эти метаданные необходимы для работы системы сетевой безопасности, особенно для обеспечения применения политик облачной безопасности
- **Применение облачной политики**: Метаданные, формируемые встраиваемой логикой формирования метаданных, используются для обеспечения соблюдения политик облачной безопасности.
- **Повышение сетевой безопасности**: Встроенная логика формирования метаданных является важнейшим компонентом системы сетевой безопасности. Генерируя и используя метаданные, система может лучше отслеживать и контролировать взаимодействие с облачными приложениями, тем самым повышая общую безопасность корпоративной сети
- **Эффективность и точность**: Централизация бизнес-логики на уровне метаданных, выполняемая встраиваемой логикой формирования метаданных, может помочь устранить ошибки и повысить эффективность. Это особенно полезно в сложных сетевых средах, где решающее значение имеет точная и эффективная работа

VI. Отдельные синтетические запросы

Термин "Отдельные синтетические запросы" относится к синтетическим запросам, которые генерируются и выдаются отдельно от входящих запросов во время сеанса приложения. Они не являются ответами на запросы клиентов, а независимо генерируются системой.

Система, описанная в патенте, включает встроенный прокси-сервер, настроенный с возможностью ввода синтетических запросов. Этот прокси-сервер может формировать синтетические запросы, которые отделены от входящих запросов во время сеанса подачи заявки. Эти отдельные синтетические запросы используются для взаимодействия с облачными приложениями и извлечения метаданных для применения облачной политики.

Формирование отдельных синтетических запросов позволяет системе взаимодействовать с облачными приложениями независимо от действий клиента. Это может обеспечить дополнительные меры безопасности, поскольку система может извлекать метаданные и применять политики безопасности динамически

Ключевые особенности:

- **Независимость от клиентских запросов**: Эти синтетические запросы не являются ответами на клиентские запросы, а независимо генерируются системой
- **Взаимодействие с облачными приложениями**: Отдельные синтетические запросы используются для взаимодействия с облачными приложениями и извлечения метаданных для применения облачной политики
- **Поиск метаданных в реальном времени**: формирование отдельных синтетических запросов позволяет системе взаимодействовать с облачными приложениями независимо от действий клиента.
- **Повышенная безопасность**: Использование отдельных синтетических запросов может повысить безопасность облачных приложений, позволяя системе активно извлекать метаданные и применять политики безопасности
- **Потенциальные области применения**: Отдельные синтетические запросы могут использоваться в различных областях, включая сетевую безопасность, мониторинг производительности, разработку программного обеспечения и обеспечение качества, управление данными и разработку API

Потенциальные области применения:

- **Сетевая безопасность**: Отдельные синтетические запросы могут использоваться для повышения сетевой безопасности путём динамического применения политик безопасности на основе метаданных, полученных из синтетических запросов
- **Мониторинг производительности**: Отдельные синтетические запросы могут использоваться для мониторинга производительности систем и приложений в режиме реального времени, помогая выявлять потенциальные проблемы до того, как они затронут реальных пользователей
- **Разработка программного обеспечения и обеспечение качества**: Отдельные

синтетические запросы могут использоваться при разработке и тестировании ПО для мониторинга и анализа поведения приложений в режиме реального времени

- **Управление данными**: Отдельные синтетические запросы могут использоваться в системах управления данными для отслеживания изменений в данных и поддержания согласованности и эффективности операций
- **Разработка API**: Отдельные синтетические запросы могут использоваться при разработке API для предоставления дополнительного контекста или информации об обрабатываемых данных, повышая функциональность и удобство использования API

A. Значимость отдельных синтетических запросов

Использование отдельных синтетических запросов в системе сетевой безопасности повышает способность системы применять политики облачной безопасности, заблаговременно выявлять потенциальные проблемы безопасности и повышать общую безопасность корпоративных сетей:

- **Формирование метаданных**: Встроенная логика формирования метаданных использует отдельные синтетические запросы для формирования метаданных. Эти метаданные имеют решающее значение для обеспечения соблюдения политик облачной безопасности и для функционирования системы сетевой безопасности
- **Упреждающие меры безопасности**: Отдельные синтетические запросы позволяют проводить упреждающее тестирование и мониторинг взаимодействия системы с облачными приложениями. Это может помочь выявить и устранить потенциальные проблемы безопасности до того, как они повлияют на реальных пользователей
- **Применение облачной политики**: Метаданные, полученные в результате отдельных синтетических запросов, используются для применения политик облачной безопасности. Это позволяет системе динамически адаптировать и применять меры безопасности
- **Эффективность и точность**: Использование отдельных синтетических запросов может повысить эффективность и точность системы сетевой безопасности. Генерируя и используя метаданные из этих запросов, система может лучше отслеживать и контролировать взаимодействие с облачными приложениями

VII. Принудительное применение облачной политики

"Принудительное применение облачной политики" относится к применению политик безопасности в облачных средах на основе метаданных, извлекаемых из синтетических запросов

Система сетевой безопасности, описанная в патенте, настроена на формирование синтетических запросов и внедрение их в сеанс приложения. Эти синтетические запросы передаются в облачное приложение, а ответы предоставляют метаданные. Затем система применяет политику к входящему запросу на основе этих метаданных.

Принудительное применение облачной политики имеет решающее значение для поддержания безопасности в облачных средах. Политики могут включать правила, касающиеся контроля доступа, защиты данных, сетевой безопасности и многого другого. Применяя эти политики, система может предотвращать несанкционированный доступ, защищать конфиденциальные данные и поддерживать целостность сети.

Система, описанная в патенте, улучшает применение облачной политики за счёт использования синтетических запросов для извлечения метаданных. Это позволяет системе динамически применять политики безопасности на основе метаданных, полученных из синтетических запросов, обеспечивая более упреждающий и адаптивный подход к облачной безопасности.

Ключевые моменты:

- **Динамическое применение политики**: Система динамически применяет политики безопасности на основе метаданных, полученных в результате синтетических запросов. Это говорит о том, что система может адаптировать и применять меры безопасности в режиме реального времени
- **На основе метаданных**: применение облачных политик основано на метаданных, извлекаемых из синтетических запросов. Эти метаданные предоставляют системе необходимый контекст для принятия решения о том, какие политики применять
- **Повышение безопасности**: Применение облачной политики является важнейшим аспектом поддержания безопасности в облачных средах. Политики могут включать правила контроля доступа, защиты данных, сетевой безопасности и многое другое
- **Проактивная безопасность**: Система, описанная в патенте, улучшает применение облачной политики за счёт использования синтетических запросов для извлечения метаданных. Это позволяет системе активно применять политики безопасности, обеспечивая более адаптивный подход к облачной безопасности
- **Потенциальные области применения**: принудительное применение облачной политики может использоваться в различных областях, включая облачную безопасность, контроль доступа, защиту данных, соответствие требованиям и управление рисками

Говоря подробнее про потенциальные области применения стоит выделить:

- **Облачная безопасность**: Применение облачной политики является фундаментальным аспектом облачной безопасности, помогающим защитить данные, приложения и инфраструктуру в облаке
- **Контроль доступа**: Политики могут использоваться для контроля того, кто имеет доступ к определённым ресурсам в облаке, предотвращая несанкционированный доступ
- **Защита данных**: Политики могут использоваться для защиты конфиденциальных данных в облаке, например для шифрования данных в состоянии покоя и при передаче
- **Соответствие требованиям**: применение облачной политики может помочь организациям соблюдать правила и стандарты, связанные с защитой данных и конфиденциальностью
- **Управление рисками**: применяя политики в облаке, организации могут управлять рисками, связанными с безопасностью, конфиденциальностью и соблюдением требований

A. Значимость отдельных синтетических запросов

"Принудительное применение облачной политики" имеет важное значение, поскольку оно относится к принудительному применению политик безопасности в облачной среде. Это предполагает использование синтетических запросов и встраиваемой логики формирования метаданных для обеспечения соответствия трафика данных между клиентами и облачными приложениями установленным политикам безопасности. Это может помочь предотвратить несанкционированный доступ и защитить конфиденциальные данные, тем самым повысив общую безопасность облачной среды.

VIII. Поддержка профиля Google Chrome'

"Поддержка профиля Google Chrome" для обозначения способности системы обрабатывать и интерпретировать информацию о сеансе пользователя, такую как идентификаторы аутентификации и идентификаторы сеанса (cookies), связанные с профилем пользователя Google Chrome:

- **Информация о сеансе пользователя**: когда пользователь открывает файл (например, файл Google Drive, документы, таблицы и т.д.) Из своей корпоративной учётной записи для входа в систему, открытый файл будет содержать информацию об уже вошедшем в систему пользователе, такую как auth_id и SID (файлы cookie)
- **Идентификация файла**: при текущем подходе этот файл будет идентифицирован как уже вошедший в систему пользователь. Это означает, что система может распознать действие и связать его с правильным профилем пользователя
- **Пример сценария**: например, если пользователь входит в Gmail с идентификатором “abc@kkrlog.com” и получает документ от внешнего пользователя “xyz@gmail.com”. Когда пользователь откроет файл, он покажет, что "abc@kkrlog.com" — это пользователь, выполняющий действие, а экземпляр файла - “kkrlog.com”, но "gmail.com” — это фактический экземпляр файла
- **Управление профилем Google Chrome**: Google Chrome позволяет пользователям создавать несколько профилей и управлять ими. У каждого профиля есть свой набор закладок, расширений и настроек для разделения личных действий в Интернете и действий, связанных с работой, обеспечивая конфиденциальность и предотвращая утечку данных.
- **Потенциальные области применения**: Возможность обработки и интерпретации информации о сеансах пользователя, связанной с профилями Google Chrome, может использоваться в различных областях, включая сетевую безопасность, управление данными и оптимизацию взаимодействия с пользователем

IX. Политика обработки файлов вложений»

Политики обработки файлов-вложений описывают подход к обработке файлов в корпоративной сети, особенно в отношении облачных приложений и служб. Эти политики и механизмы предназначены для повышения безопасности и соответствия требованиям в корпоративной среде, особенно при использовании облачных средств обмена файлами и совместной работы:

- **Две основные политики**: Система различает две основные политики для пользователей в отношении вложений файлов: "разрешённый корпоративный экземпляр" и "блокирующий личный экземпляр"
- **Определение корпоративного экземпляра**: корпоративный экземпляр определяется как санкционированный компанией экземпляр облачного приложения. Даже если владельцем общего файла является внешний пользователь, и экземпляр файла считается корпоративным, активируется политика "разрешённого корпоративного экземпляра", позволяющая пользователю выполнять действия с файлами, предоставляемыми извне
- **Идентификация владельца файла**: Системе необходимо идентифицировать владельца созданного файла. Для предотвращения фишинговых атак и несанкционированного доступа внешним файлам запрещён доступ к корпоративной сети или выполнение каких-либо действий
- **Анализ трафика**: когда пользователь получает документ с Google Диска, Docs, Таблиц, по электронной почте или общей ссылке, данные транзакции ответа включают владельца файла. Система использует шаблоны, чтобы определить,

создан ли документ личной учётной записью или корпоративной

- **Извлечение экземпляра**: Система извлекает экземпляр для операции просмотра файла и заполняет его в качестве владельца файла. Для других действий (загрузка / редактирование) владелец может быть неизвестен в трафике, но file_id уникален, по крайней мере, для экземпляра
- **Блокировка личных документов**: Система помогает корпоративным пользователям блокировать просмотр документов, созданных лично, и разрешает просмотр только корпоративных документов. Однако это может заблокировать доступ клиентов к персонально созданным документам из их личного экземпляра
- **Определение экземпляра**: когда пользователи просматривают документы с Google Диска, Docs, таблиц и т.д., данные ответа содержат сведения об экземпляре. Если пользователь входит в личную учётную запись, инстансом будет gmail.com, а если пользователь входит в систему с корпоративной учётной записью – корпоративный инстанс

X. Технологический процесс

Технологический процесс описывается как процедура оценки файлов документов, совместно используемых в корпоративной сети, в частности, в отношении потенциальных угроз безопасности.

- Вредоносный документ
- Встроенный прокси
- Идентификация документа
- Санкционированные документы
- Сайты, внесенные в Черный список
- Неизвестные документы

Вредоносный документ, созданный на вредоносном веб-сайте, передаётся в облачное хранилище, доступное в корпоративной сети. Цель злоумышленника – сделать документ привлекательным, чтобы к нему могли получить доступ несколько пользователей в корпоративной сети или с помощью удалённых корпоративных устройств.

Встроенный прокси-сервер, являющийся частью системы сетевой безопасности, действует как посредник между облаком и корпоративной сетью, контролируя файлы, поступающие извне корпоративной сети.

Файлы документов, пытающиеся поступающие в корпоративную сеть, идентифицируются методами, описанными в патенте, и другими метаданными, которые идентифицируют источник файла документа. Метаданные размещаются в хранилище метаданных, доступном встраиваемому прокси-серверу.

На внутренние корпоративные документы всегда распространяются санкции. Документы, созданные за пределами корпоративной сети, если на них наложены санкции, всегда допускаются в корпоративную сеть без проверки на угрозы. Это документы из известных источников, включая крупные организации и организации, которые ранее имели дело с корпоративной сетью.

Файлы документов, полученные с известных вредоносных веб-сайтов, идентифицируются встроенным прокси-сервером как сайты, внесённые в черный список. Это веб-сайты и URL-адреса, которые в прошлом были связаны с фишинговыми атаками или каким-либо другим образом ставили под угрозу сетевую безопасность. Хранилище метаданных отслеживает, сохраняет и поддерживает в базе данных все известные сайты, внесённые в черный список. Документы, полученные в этой категории, автоматически и навсегда блокируются.

Неизвестные документы оцениваются на предмет их принадлежности и других свойств метаданных, которые позволят идентифицировать источник неизвестного документа. Если источник документа не может быть идентифицирован, его доступ в корпоративную сеть временно блокируется. Для этого используются правила, основанные на политике, включая методы сопоставления. Документ помещается в карантин и первоначально проверяется на наличие угрозы. Большая часть этой работы требует участия администратора сетевой безопасности. Если есть уверенность, что может быть задействован вредоносный код, документ попадёт в изолированную среду для дальнейшего анализа.