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.

I. 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.

II. 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.

III. 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.

A. 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.

1) 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.

B. 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.

1) 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.

2) 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.

3) 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.

4) 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.

C. *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 киберугрозам 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).

1) *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.

2) *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 киберугроз, 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.

3) *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 киберугроз. 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 киберугроз. 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.

IV. 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 киберугрозы продолжают развиваться, такие инновационные подходы будут иметь решающее значение для защиты цифровых активов и укрепления доверия к цифровой экосистеме.

A. *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.

B. *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.

C. *Способность адаптироваться к возникающим угрозам*

Включение «Дополнительных вставок» как части метода обеспечивает гибкую и адаптивную стратегию безопасности. По мере развития киберугроз 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 киберугрозами.

D. *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.

E. *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 киберугрозами.

V. 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:

A. *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.

B. *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.

C. *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 киберугроз.

D. *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.

E. *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.

VI. 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.

A. 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 киберугроз.

B. 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.

C. 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.

D. 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.

E. 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 киберугроз.

VII. 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:

A. 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.

B. *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.

C. *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.

D. *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.

E. *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.

F. *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.

VIII. 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