ТЕХНИКАЛЫҚ ҒЫЛЫМДАР
ТЕХНИЧЕСКИЕ НАУКИ
TECHNICAL SCIENCE

CENTRAL ASIAN SCIENTIFIC JOURNAL
ISSN 3135-3061
2026. №4 (32), Том 2. С. 559–562
DOI: https://doi.org/10.5281/zenodo.24417686
Сайт журнала: https://cajournal.kz

УДК 004.056

ПРОТОТИП КАСКАДНОГО ДЕТЕКТОРА ПОДДЕЛЬНЫХ ВЕБ-САЙТОВ НА ОСНОВЕ СВЕРКИ БРЕНДА С ДОМЕНОМ

Э.Т. Сибагатуллин, А.С. Калмыков, В.И. Дахно
Satbayev University, Алматы, Казахстан

Сибагатуллин Эльдар Тагирович — студент 4 курса образовательной программы «Системы информационной безопасности» (6B06301), Satbayev University, Алматы, Казахстан.

Калмыков Андрей Сергеевич — студент 4 курса образовательной программы «Системы информационной безопасности» (6B06301), Satbayev University, Алматы, Казахстан.

Дахно Влад Игоревич — студент 4 курса образовательной программы «Системы информационной безопасности» (6B06301), Satbayev University, Алматы, Казахстан.

© Э.Т. Сибагатуллин, А.С. Калмыков, В.И. Дахно, 2026

Аннотация: Поддельные (фишинговые) веб-сайты копируют визуальный облик известных брендов, чтобы похитить учётные данные пользователей, и существуют считанные часы, из-за чего списки опасных адресов не успевают их блокировать. Цель работы — разработать прототип детектора, который принимает решение не по визуальному сходству страницы с эталоном, а по рассогласованию бренда, определённого по изображению и тексту страницы, с её доменным именем. Реализована каскадная схема из четырёх шагов (фильтр URL, снимок экрана и оптическое распознавание текста, определение бренда двумя независимыми каналами, сверка бренда с доменом) на языке Python, а также расширение для браузера. На демонстрационном наборе страниц прототип верно пометил поддельные страницы казахстанских брендов как опасные (уровень риска до 99 %), а легитимный и официальный сайты — как безопасные. Показано, что критерий «бренд не соответствует домену» устойчив к смене макета страницы, которая обходит детекторы визуального сходства.

Ключевые слова: обнаружение фишинга, поддельные веб-сайты, мультимодальный анализ, определение бренда, оптическое распознавание символов, расширение для браузера, информационная безопасность.

Введение

Фишинг остаётся одной из самых массовых киберугроз: в 2023 году в мире зафиксировано более пяти миллионов фишинговых атак, а убытки организаций в США от фишинга превысили 12,5 млрд долларов [1]. Поддельный веб-сайт копирует внешний вид известного бренда, чтобы пользователь ввёл логин, пароль или платёжные данные.

Такие сайты живут недолго. По результатам пятимесячного наблюдения за 286 237 фишинговыми адресами медианное время жизни страницы составило около 5,5 часов, при этом сервис Google Safe Browsing обнаруживал в среднем лишь 18,4 % сайтов и в среднем через 4,5 суток [2]. Защита, основанная на списках уже известных опасных адресов, поэтому запаздывает, и саму страницу нужно оценивать в момент её открытия.

Страницу можно оценить по двум группам признаков. Визуальные признаки (снимок экрана, логотип, макет, цветовая гамма) отражают то, что видит пользователь. Текстовые

признаки (URL, HTML-код, структура DOM, видимый и распознанный OCR текст) отражают то, как страница устроена и что она просит сделать. Злоумышленник может запутать код, сохранив внешний вид, или изменить макет, сохранив код, поэтому по отдельности каждая группа признаков обходится [3].

Эталонные (reference-based) методы определяют изображённый на странице бренд и считают страницу фишинговой, если домен не принадлежит этому бренду [4, 5]. Их слабое место — зависимость от фиксированного списка брендов и уязвимость визуального сходства: страницы, сохраняющие логотип и цвета бренда, но использующие другой макет, обходят детекторы визуального сходства в 95–100 % случаев [6]. Цель настоящей работы — разработать прототип детектора, в котором решение принимается по согласованности бренда, определённого по двум каналам, с доменом страницы, и показать работоспособность такого критерия.

Материалы и методы

Детектор построен как каскад из четырёх шагов (рисунок 1). Лёгкий фильтр URL пропускает очевидно легитимные адреса без дальнейшего анализа. Для подозрительных страниц выполняется рендеринг, снимается скриншот и собирается HTML. Визуальный канал извлекает текст логотипа и надписей со снимка экрана; текстовый канал анализирует HTML, структуру DOM и поля ввода. Оба канала независимо определяют бренд, после чего принимается решение.



Рисунок 1 – Каскадная архитектура прототипа детектора поддельных веб-сайтов

Пусть $s_в(b)$ и $s_т(b)$ — оценки бренда b, полученные визуальным и текстовым каналами. Согласованный бренд выбирается по формуле (1), где α — вес визуального канала:

$$\hat{b} = \arg\max [\alpha \cdot s_в(b) + (1 - \alpha) \cdot s_т(b))] \quad (1)$$

Страница с доменом d относится к поддельным ($y = 1$) по формуле (2), где τ — порог уверенности, $D(\hat{b})$ — множество легитимных доменов бренда $\hat{b}$, а $I(x) = 1$, если страница запрашивает учётные данные:

$$y = 1, \text{ если } s(\hat{b}) \geq \tau,\ d \notin D(\hat{b}) \text{ и } I(x) = 1; \text{ иначе } y = 0 \quad (2)$$

В отличие от правил, основанных на сходстве, формула (2) не зависит от того, насколько макет похож на эталон: страница с новым макетом, но узнаваемым брендом на чужом домене всё равно классифицируется как поддельная.

Прототип реализован на языке Python. HTML и структура DOM разбираются библиотекой BeautifulSoup, рендеринг страницы и снимок экрана выполняются через Playwright (headless Chromium), оптическое распознавание текста — через Tesseract (pytesseract) с языковыми моделями для русского, казахского и английского языков. Фильтр URL выявляет подмену символов-гомоглифов, домены в кодировке punycode, опечатки в доменном имени (по расстоянию Левенштейна), подозрительные доменные зоны и слова-приманки. Текстовый канал анализирует заголовок, метаданные, видимый текст, поля ввода и форму отправки данных, оценивая намерение собрать учётные данные (поля пароля, номера карты, одноразового кода, ИИН). Визуальный канал определяет бренд по тексту, распознанному на снимке экрана. База брендов хранится в формате JSON и включает местные бренды Казахстана (банки, портал электронного правительства, маркетплейсы). Помимо консольного и веб-интерфейса (на базе Flask) реализовано расширение для браузера (Manifest V3), которое применяет тот же каскад к открытой странице и показывает предупреждающий баннер при обнаружении подделки.

© Central Asian Scientific Journal, 2026

Результаты и обсуждение

Работоспособность прототипа проверена на демонстрационном наборе страниц: поддельных страницах, имитирующих казахстанские бренды, а также легитимном и официальном сайтах. Результаты приведены в таблице 1.

Таблица 1 – Результаты проверки прототипа на демонстрационных страницах

Страница	Проверяемый адрес	Вердикт	Риск	Бренд
Поддельный Kaspi	kaspi-secure-login.xyz	Поддельный сайт	99%	Kaspi.kz
Поддельный Homebank	halyk-bonus.online	Поддельный сайт	высокий	Halyk Bank
Интернет-магазин	toysworld.kz	Похоже на настоящий	0%	—
Официальный сайт	kaspi.kz	Официальный сайт	0%	Kaspi.kz

На поддельных страницах оба канала согласованно определили имитируемый бренд (например, Kaspi.kz), а поскольку домен страницы ему не принадлежал и страница запрашивала учётные данные, прототип присвоил вердикт «поддельный сайт» с высоким уровнем риска. Легитимный магазин без признаков имитации помечен как безопасный, а официальный домен из базы брендов — как доверенный без дополнительной проверки. Таким образом, демонстрация подтверждает, что критерий рассогласования бренда с доменом применим на практике.

Следует подчеркнуть, что представленные результаты носят характер демонстрации работоспособности (proof-of-concept) на иллюстративных страницах и не являются полной экспериментальной оценкой на эталонных наборах данных. Прототип имеет ряд ограничений: база брендов небольшая и формируется вручную; бренд определяется по ключевым словам и распознанному тексту без обученного детектора логотипа; не обрабатываются приёмы сокрытия содержимого (клоакинг) и страницы с CAPTCHA; скомпрометированные легитимные домены правилом «бренд–домен» не выявляются. Устранение этих ограничений и количественная оценка на открытых наборах данных составляют предмет дальнейшей работы.

Заключение

Разработан рабочий прототип детектора поддельных веб-сайтов, реализующий каскадную схему с принятием решения по рассогласованию бренда, определённого по изображению и тексту страницы, с её доменом. Прототип включает консольный и веб-интерфейсы, а также расширение для браузера. Демонстрация на тестовых страницах подтвердила применимость выбранного критерия и его устойчивость к смене макета, обходящей детекторы визуального сходства. Дальнейшие шаги — построение мультимодального набора данных с базой местных брендов, добавление обученного детектора логотипа и полная экспериментальная оценка метода.

Список литературы:

1. Hwang J., Min M. Survey of AI-based threat detection for illicit web ecosystems: models, modalities, and emerging trends // Computer Modeling in Engineering & Sciences. – 2026. – Vol. 146, № 3. – DOI: 10.32604/cmes.2026.078940.

2. Lee K., Lim K., Kim H., Kwon Y., Kim D. 7 days later: analyzing phishing-site lifespan after detected // Proceedings of the ACM Web Conference 2025 (WWW ’25). – New York: ACM, 2025. – P. 945–956. – DOI: 10.1145/3696410.3714678.

3. Wangchuk T., Gonsalves T. Multimodal phishing detection on social networking sites: a systematic review // IEEE Access. – 2025. – Vol. 13. – DOI: 10.1109/ACCESS.2025.3579584.

4. Liu R., Lin Y., Teoh X., Liu G., Huang Z., Dong J. S. Less defined knowledge and more true alarms: reference-based phishing detection without a pre-defined reference list // Proceedings of the 33rd USENIX Security Symposium. – Berkeley: USENIX Association, 2024. – P. 523–540.

© Central Asian Scientific Journal, 2026

5. Cao T., Huang C., Li Y., Wang H., He A., Oo N., Hooi B. PhishAgent: a robust multimodal agent for phishing webpage detection // Proceedings of the AAAI Conference on Artificial Intelligence. – Palo Alto: AAAI Press, 2025. – Vol. 39.

6. Mishra R., Varshney G., Singh C., Arora P. Poster: evading visual phish detectors via intelligent visual transformations // Proceedings of the ACM Asia Conference on Computer and Communications Security (ASIA CCS '26). – New York: ACM, 2026. – P. 1886–1888. – DOI: 10.1145/3779208.3804882.

© Central Asian Scientific Journal, 2026