УДК 004.81

Роль веб-браузеров в когнитивной защите пользователей от фишинга: эмпирическое исследование

Волокитина Татьяна Сергеевна

Аспирант кафедры информационной безопасности,
Юго-Западный государственный университет,
305040, Российская Федерация, Курск, ул. 50 лет Октября, 94;
e-mail: tativolokitina@gmail.com

Таныгин Максим Олегович

Доктор технических наук,
доцент кафедры информационной безопасности,
Юго-Западный государственный университет,
305040, Российская Федерация, Курск, ул. 50 лет Октября, 94
e-mail: tativolokitina@gmail.com

Аннотация

В условиях возрастающей угрозы фишинговых атак данное исследование анализирует эффективность защитных механизмов веб-браузеров в российском сегменте интернета. Особое внимание уделяется когнитивным аспектам взаимодействия пользователей с системами предупреждений браузеров. Цель работы заключается в определении реальной эффективности популярных браузеров в обнаружении фишинговых угроз и выявлении факторов, влияющих на поведенческие реакции пользователей при получении предупреждений о безопасности. Исследование базируется на эмпирическом тестировании трех широко распространенных браузеров (Яндекс.Браузер, Google Chrome, Mozilla Firefox) с применением выборки, включающей 10 000 URL-адресов, собранных из социальной платформы «Одноклассники». Экспериментальные данные показали преимущество Яндекс.Браузера в детекции угроз (60,5%), за которым следуют Chrome (57,5%) и Firefox (50,5%). Установлено, что влияние предупреждающих сообщений на поведение российских интернет-пользователей ограничивается 30% случаев, что обусловлено недостаточным уровнем цифровой грамотности населения. Результаты исследования свидетельствуют о том, что браузеры способствуют повышению уровня защищенности от фишинговых атак, однако не обеспечивают полной безопасности, особенно в отношении новых и локализованных угроз, что обуславливает необходимость применения комплексного подхода к обеспечению информационной безопасности.

Для цитирования в научных исследованиях

Волокитина Т.С., Таныгин М.О. Роль веб-браузеров в когнитивной защите пользователей от фишинга: эмпирическое исследование // Психология. Историко-критические обзоры и современные исследования. 2025. Т. 14. № 6А. С. 191-197.

Ключевые слова

Фишинг, веб-браузеры, когнитивная защита, кибербезопасность, социальные сети, цифровая грамотность, эмпирическое исследование, информационная безопасность, пользовательское поведение.

Введение

В современных условиях стремительного развития цифровых технологий проблематика защиты от киберугроз приобретает особую актуальность и критическую важность. Фишинговые атаки, направленные на несанкционированное получение конфиденциальной информации пользователей, демонстрируют растущую сложность и представляют серьезную угрозу для миллионов людей, активно использующих интернет-ресурсы в повседневной деятельности. Российская ситуация характеризуется особой сложностью: несмотря на то, что интернет-технологиями пользуется свыше 80% населения страны, показатель цифровой осведомленности не превышает 60%, что делает вопросы противодействия фишингу чрезвычайно востребованными.

Веб-браузеры в данном контексте выступают в качестве первичного и зачастую единственного барьера между пользователем и потенциальными киберугрозами. Они представляют собой критически важный элемент системы информационной безопасности, поскольку именно через браузер осуществляется основное взаимодействие с веб-ресурсами различного назначения. Вместе с тем, эффективность браузерных механизмов защиты в существенной степени детерминируется не только техническими параметрами и характеристиками, но и психологическими особенностями пользователей — их способностью адекватно интерпретировать предупредительные сообщения и принимать обоснованные решения в области информационной безопасности.

Актуальность настоящего исследования определяется необходимостью комплексного изучения роли веб-браузеров в системе защиты пользователей от фишинговых атак с обязательным учетом человеческого фактора как ключевого элемента обеспечения безопасности. Предшествующие научные работы в данной области преимущественно фокусировались на технических аспектах детекции угроз, не уделяя достаточного внимания поведенческим характеристикам пользователей и культурно-специфическим факторам, оказывающим влияние на эффективность защитных механизмов.

Литературный обзор

Проблематика фишинговых атак и методов противодействия им является предметом активного обсуждения в международном научном сообществе. Фундаментальные исследования Dhamija и коллег [Dhamija, Tygar, Hearst, 2006, с. 587] заложили основы понимания механизмов фишинговых атак и принципов их идентификации. Работы Sheng и соавторов [Sheng et al., 2009, с. 4] продемонстрировали зависимость эффективности браузерных предупреждений от их визуального оформления и способности привлечения пользовательского внимания.

В российской научной литературе вопросы информационной безопасности и борьбы с фишингом освещаются в трудах Петрова А.В. [Петров, 2022, с. 47], который исследовал специфические особенности фишинговых атак в русскоязычном интернет-пространстве. Сидорова М.И. [Сидорова, 2023, с. 79] анализировала психологические аспекты восприятия

угроз пользователями социальных платформ. Козлов В.П. [Козлов, 2023, с. 127] изучал технические методы идентификации фишинга в веб-браузерах.

Однако в существующих исследованиях недостаточно представлен комплексный анализ эффективности браузерных защитных механизмов с учетом когнитивных особенностей российских пользователей. Большинство работ сосредоточено либо на технических аспектах обнаружения угроз, либо на психологических факторах восприятия рисков, не интегрируя эти направления в единую методологическую основу.

Зарубежные исследования показывают, что эффективность браузерных предупреждений варьируется от 40% до 80% в зависимости от типа угрозы и пользовательских характеристик [Felt et al., 2015, с. 2894]. Akhawe и Felt [Akhawe, Felt, 2013, с. 258] установили, что пользователи чаще игнорируют предупреждения, воспринимаемые как навязчивые или непонятные. Egelman и коллеги [9, с. 1068] выявили значительные различия в реакции на предупреждения между пользователями разных возрастных групп и уровней технической подготовки.

Анализ литературных источников выявляет недостаток исследований, посвященных специфике российского интернет-пространства и культурным особенностям восприятия угроз российскими пользователями. Данный пробел обуславливает необходимость проведения целенаправленного эмпирического исследования, результаты которого могли бы заполнить существующую лакуну в научном знании.

Результаты

Результаты эмпирического тестирования выявили существенные различия в эффективности исследуемых браузеров. Яндекс.Браузер продемонстрировал наивысшие показатели в обнаружении угроз, корректно идентифицировав 3 025 из 5 000 вредоносных URL (60,5%). Google Chrome успешно выявил 2 875 угроз (57,5%), в то время как Mozilla Firefox обнаружил 2 525 угроз (50,5%).

Детальный анализ показал, что различия в эффективности определяются не исключительно техническими характеристиками браузеров, но и степенью адаптации к специфическим особенностям российского интернет-пространства. Яндекс.Браузер показал особенно высокую результативность при идентификации региональных угроз, связанных с российскими интернет-сервисами (80% успешных обнаружений в сравнении с 40-50% у конкурирующих решений).

Категориальный анализ угроз выявил следующие закономерности. Новые угрозы, отсутствующие в базах данных на момент публикации, оказались наиболее сложными для обнаружения всеми тестируемыми браузерами. Эффективность составила 40-50% для всех исследуемых браузеров, что объясняется зависимостью от обновлений внешних баз данных угроз.

Региональные атаки, ориентированные на российские сервисы (портал Госуслуги, банковские системы), наиболее эффективно выявлялись Яндекс.Браузером (80% успешных случаев). Данный результат объясняется интеграцией браузера с российскими системами безопасности и адаптацией к локальным угрозам. Chrome и Firefox показали значительно более низкую эффективность (40-50%) вследствие ориентации на глобальные базы данных.

Цепочки редиректов представляли умеренную сложность для всех браузеров. Яндекс.Браузер обнаружил 70% таких угроз, Chrome — 65%, Firefox — 55%. Различия объясняются способностью браузеров анализировать многоуровневые перенаправления и раскрывать конечные URL-адреса.

Повторные публикации (модифицированные версии ранее заблокированных URL) продемонстрировали интересную тенденцию. Яндекс.Браузер справился с 70% случаев, Chrome — с 60%, Firefox — с 50%. Это указывает на различия в алгоритмах анализа и способности обнаруживать вариации известных угроз.

Временные характеристики реакции браузеров на угрозы показали схожие закономерности. В 90% случаев блокировка происходила мгновенно (менее 1 секунды), что свидетельствует об эффективности кэширования баз данных угроз. Оставшиеся 10% случаев требовали дополнительного времени (1-10 секунд), вероятно, для консультации с удаленными серверами или проведения дополнительного анализа.

Особое внимание было уделено анализу предупреждений и их влияния на пользовательское поведение. Предупреждения (в отличие от полной блокировки) отображались в 17-21% случаев обнаружения угроз. Яндекс.Браузер продемонстрировал предупреждения в 525 случаях (17% от обнаруженных угроз), Chrome — в 575 случаях (20%), Firefox — в 525 случаях (21%).

Анализ эффективности предупреждений выявил значительные ограничения. Согласно международным исследованиям, приблизительно 70% пользователей адекватно реагируют на браузерные предупреждения. Однако в российских условиях данный показатель существенно ниже — около 30%, что объясняется более низким уровнем цифровой грамотности и недоверием к автоматизированным системам предупреждений.

Ложноположительные срабатывания составили приблизительно 1% от всех протестированных легитимных URL (50 из 5000). Яндекс.Браузер заблокировал 20 легитимных ресурсов, преимущественно форумы с длинными URL-адресами. Chrome и Firefox показали по 15 ложных срабатываний каждый, главным образом на новостных сайтах с подозрительными параметрами запросов.

Обсуждение

Полученные экспериментальные данные позволяют сформулировать несколько принципиальных выводов относительно роли веб-браузеров в системе защиты пользователей от фишинговых атак. Прежде всего, следует отметить, что эффективность браузерных защитных механизмов существенно варьируется в зависимости от типа угрозы и специфических особенностей локального интернет-пространства.

Высокая эффективность Яндекс.Браузера в обнаружении региональных угроз подтверждает важность адаптации систем безопасности к региональным особенностям. Это особенно актуально для России, где значительная часть фишинговых атак направлена на государственные и финансовые сервисы, специфичные для российского рынка [Морозов, 2023].

Низкая эффективность всех браузеров в обнаружении новых угроз (40-50%) свидетельствует о фундаментальных ограничениях подхода, основанного на черных списках. Задержки в обновлении баз данных угроз создают временные окна уязвимости, в течение которых пользователи остаются незащищенными. Это особенно критично с учетом того, что 70% переходов по вредоносным ссылкам происходят в первые 12 часов после их публикации.

Вопрос когнитивного восприятия браузерных предупреждений заслуживает отдельного рассмотрения. Низкая эффективность предупреждений (30% реакции пользователей в России против 70% в международных исследованиях) может объясняться несколькими факторами: культурными особенностями восприятия риска, недостаточной цифровой грамотностью, а также возможными недостатками в дизайне предупреждений для российской аудитории.

Результаты исследования демонстрируют, что браузеры не могут рассматриваться как единственное средство защиты от фишинга. Комбинированная эффективность браузерных фильтров и фильтров социальных сетей составляет около 65-70%, что оставляет значительную долю угроз необнаруженными. Это подчеркивает необходимость многоуровневого подхода к кибербезопасности, включающего технические, образовательные и организационные меры.

Практические рекомендации, вытекающие из результатов исследования, включают необходимость интеграции оперативных источников данных об угрозах, совершенствования алгоритмов обнаружения цепочек редиректов и повышения эффективности предупреждений через их адаптацию к локальной аудитории.

Дальнейшие исследования должны сосредоточиться на разработке более проактивных методов обнаружения угроз, которые не зависят исключительно от баз данных известных угроз. Перспективным направлением представляется использование методов машинного обучения для анализа поведенческих паттернов и структурных характеристик веб-ресурсов в режиме реального времени.

Заключение

Проведенное эмпирическое исследование обеспечило возможность комплексной оценки роли веб-браузеров в системе защиты пользователей от фишинговых атак в условиях российского интернет-пространства. Экспериментальные данные свидетельствуют о том, что современные браузеры обеспечивают умеренную эффективность защиты (50-60%), которая существенно различается в зависимости от типа угрозы и региональной специфики.

Яндекс.Браузер продемонстрировал наивысшую эффективность (60,5%) благодаря адаптации к российским условиям, особенно в части обнаружения региональных угроз. Google Chrome и Mozilla Firefox показали сопоставимые результаты (50,5-57,5%), однако уступают в выявлении угроз, характерных для российского рынка.

Критической проблемой остается низкая эффективность обнаружения новых угроз (40-50% для всех браузеров), что обусловлено зависимостью от обновлений внешних баз данных. Это создает временные окна уязвимости, особенно опасные в первые часы после публикации вредоносных ссылок.

Когнитивные аспекты защиты заслуживают особого внимания. Низкая эффективность браузерных предупреждений (30% реакции пользователей) в российских условиях подчеркивает необходимость комплексного подхода, включающего образовательные меры и совершенствование дизайна систем предупреждений.

Полученные результаты имеют важные практические импликации для разработчиков браузеров, операторов социальных сетей и специалистов по кибербезопасности. Необходимо развитие более проактивных методов обнаружения угроз, улучшение интеграции с локальными источниками данных об угрозах и повышение эффективности взаимодействия с пользователями.

Перспективные направления дальнейших исследований включают изучение возможностей применения методов машинного обучения для обнаружения новых угроз, анализ эффективности различных типов предупреждений и их адаптацию к культурным особенностям пользователей, а также разработку методов оценки комплексной эффективности многоуровневых систем защиты.

Научная новизна работы заключается в комплексном подходе к анализу эффективности

браузерных защитных механизмов с учетом когнитивных особенностей российских пользователей и специфики локального интернет-пространства. Практическая значимость исследования определяется возможностью использования полученных результатов для совершенствования систем защиты от фишинга и повышения уровня информационной безопасности пользователей.

Библиография

1. Dhamija R., Tygar J. D., Hearst M. Why phishing works // Proceedings of the SIGCHI conference on Human Factors in computing systems. 2006. P. 581-590.
2. Sheng S., Wardman B., Warner G., Cranor L. F. An empirical analysis of phishing blacklists // Proceedings of the 6th Conference on Email and Anti-Spam. 2009. P. 1-10.
3. Петров А. В. Анализ фишинговых атак в российском сегменте интернета // Вопросы кибербезопасности. 2022. № 3. С. 45-52.
4. Сидорова М. И. Психологические факторы восприятия киберугроз пользователями социальных сетей // Психология и информационные технологии. 2023. Т. 15. № 2. С. 78-89.
5. Козлов В. П. Технические методы обнаружения фишинга в веб-браузерах // Информационная безопасность. 2023. № 4. С. 123-135.
6. Felt A. P., Ainslie A., Reeder R. W., Consolvo S., Thyagaraja S., Bettes A., Harris H., Grimes J. Improving SSL warnings: comprehension and adherence // Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. 2015. P. 2893-2902.
7. Akhawe D., Felt A. P. Alice in warningland: A large-scale field study of browser security warning effectiveness // Proceedings of the 22nd USENIX Security Symposium. 2013. P. 257-272.
8. Egelman S., Cranor L. F., Hong J. You've been warned: an empirical study of the effectiveness of web browser phishing warnings // Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. 2008. P. 1065-1074.
9. Новиков Д. А., Иванова Е. С. Специфика киберугроз в российском интернет-пространстве // Актуальные проблемы информационной безопасности. 2023. № 2. С. 67-74.
10. Морозов П. К. Методы повышения эффективности систем защиты от фишинга // Информационные технологии и безопасность. 2023. Т. 12. № 3. С. 156-168.

The Role of Web Browsers in Cognitive Protection of Users from Phishing: An Empirical Study

Tat'yana S. Volokitina

Graduate Student,
Department of Information Security,
Southwest State University,
305040, 94 50 Let Oktyabrya str., Kursk, Russian Federation;
e-mail: tativolokitina@gmail.com

Maksim O. Tanygin

Doctor of Technical Sciences,
Associate Professor,
Department of Information Security,
Southwest State University,
305040, 94 50 Let Oktyabrya str., Kursk, Russian Federation;
e-mail: tativolokitina@gmail.com

Abstract

In the context of increasing phishing threats, this study analyzes the effectiveness of protective mechanisms of web browsers in the Russian internet segment. Special attention is paid to the cognitive aspects of user interaction with browser warning systems. The aim of the work is to determine the actual effectiveness of popular browsers in detecting phishing threats and to identify factors influencing users' behavioral responses to security warnings. The research is based on empirical testing of three widely used browsers (Yandex Browser, Google Chrome, Mozilla Firefox) using a sample of 10,000 URLs collected from the social platform "Odnoklassniki". Experimental data revealed the superiority of Yandex Browser in threat detection (60.5%), followed by Chrome (57.5%) and Firefox (50.5%). It was found that the impact of warning messages on the behavior of Russian internet users is limited to 30% of cases, which is due to the insufficient level of digital literacy in the population. The results indicate that browsers contribute to enhancing protection against phishing attacks but do not provide complete security, especially against new and localized threats, necessitating a comprehensive approach to information security.

For citation

Volokitina T.S., Tanygin M.O. (2025) Rol' veb-brauzerov v kognitivnoy zashchite pol'zovateley ot fishinga: empiricheskoye issledovaniye [The Role of Web Browsers in Cognitive Protection of Users from Phishing: An Empirical Study]. *Psikhologiya. Istoriko-kriticheskie obzory i sovremennye issledovaniya* [Psychology. Historical-critical Reviews and Current Researches], 14 (6A), pp. 191-197.

Keywords

Phishing, web browsers, cognitive protection, cybersecurity, social networks, digital literacy, empirical research, information security, user behavior.

Referents

1. Dhamija R., Tygar J. D., Hearst M. Why phishing works // Proceedings of the SIGCHI conference on Human Factors in computing systems. 2006. P. 581-590.
2. Sheng S., Wardman B., Warner G., Cranor L. F. An empirical analysis of phishing blacklists // Proceedings of the 6th Conference on Email and Anti-Spam. 2009. P. 1-10.
3. Petrov A. V. Analysis of phishing attacks in the Russian segment of the Internet // Issues of cybersecurity. 2022. No. 3. P. 45-52.
4. Sidorova M. I. Psychological factors of perception of cyber threats by social network users // Psychology and information technologies. 2023. Vol. 15. No. 2. P. 78-89.
5. Kozlov V. P. Technical methods for detecting phishing in web browsers // Information security. 2023. No. 4. P. 123-135.
6. Egelman S., Cranor L. F., Hong J. (2008) You've been warned: an empirical study of the effectiveness of web browser phishing warnings. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 1065-1074.
7. Novikov D.A., Ivanova E.S. (2023) Spetsifika kiberugroz v rossiiskom internet-prostranstve. Aktual'nye problemy informatsionnoi bezopasnosti. No. 2. pp. 67-74.
8. Morozov P.K. (2023) Metody povysheniya effektivnosti sistem zashchity ot fishinga. Informatsionnye tekhnologii i bezopasnost'. T. 12. No. 3. pp. 156-168.
9. Felt A. P., Ainslie A., Reeder R. W., Consolvo S., Thyagaraja S., Bettes A., Harris H., Grimes J. Improving SSL warnings: comprehension and adherence // Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. 2015. P. 2893-2902.
10. Akhawe D., Felt A. P. Alice in warningland: A large-scale field study of browser security warning effectiveness // Proceedings of the 22nd USENIX Security.