*УДК 004.056.53*

***Лев Георгиевич Хомустахов,***
***студент, кафедра информатики,***
***Арктический государственный институт культуры и искусств,***
***г. Якутск, РС(Я), Россия***
***Научный руководитель:***
***Ольга Герасимовна Готовцева,***
***доцент кафедры информатики, к.п.н.,***
***Арктический государственный институт культуры и искусств,***
***г. Якутск, РС(Я), Россия***

# НАУЧНЫЙ АНАЛИЗ УЯЗВИМОСТЕЙ ВЕБ-САЙТОВ И МЕТОДЫ ОБЕСПЕЧЕНИЯ ИХ БЕЗОПАСНОСТИ

***Аннотация*:** *В статье проводится научный анализ уязвимостей веб-сайтов с целью выявления ключевых угроз информационной безопасности. Рассматриваются современные методы и технологии обеспечения защиты сайтов от несанкционированного доступа и атак. Исследование основывается на систематическом подходе к идентификации, классификации и оценке уязвимостей, а также на оценке эффективности применяемых защитных решений.*

***Ключевые слова:*** *Научный анализ, уязвимость, информационная безопасность, веб-сайт, методы защиты.*

***Lev Georgievich Khomustakhov,***
***student, Department of Computer Science,***
***Arctic State Institute of Culture and Arts,***
***Yakutsk, Sakha Republic (Yakutia), Russia***
***Scientific director:***
***Olga Gerasimovna Gotovtseva,***
***Associate Professor of the Department of Informatics, Ph.D.,***
***Arctic State Institute of Culture and Arts,***
***Yakutsk, Sakha Republic (Yakutia), Russia***

# SCIENTIFIC ANALYSIS OF WEBSITE VULNERABILITIES AND METHODS OF ENSURING THEIR SECURITY

***Annotation:*** *The article presents a scientific analysis of website vulnerabilities with the aim of identifying key information security threats. It examines modern methods and technologies for protecting sites from unauthorized access and attacks. The research is based on a systematic approach to the identification, classification, and assessment of vulnerabilities, as well as an evaluation of the effectiveness of applied protective solutions.*

***Keywords:*** *Scientific analysis, vulnerability, information security, website, protection methods.*

## Введение

В современном цифровом мире веб-сайты играют ключевую роль в функционировании бизнеса, государственного управления и коммуникации. Однако наряду с возможностями возрастают и риски, связанные с уязвимостями сайтов, которые могут привести к серьезным нарушениям в работе, утечке данных и финансовым потерям. Актуальность исследований в области анализа уязвимостей и методов обеспечения безопасности веб-

сайтов обусловлена возрастанием числа и разнообразия кибератак, что требует комплексного и системного подхода к защите.

## 1. Классификация уязвимостей веб-сайтов

Основные уязвимости веб-приложений, выделяемые сегодня включают:

- Межсайтовое исполнение сценариев (XSS), позволяющее злоумышленникам внедрять и запускать вредоносный код в браузерах пользователей;
- SQL-инъекции, которые дают возможность изменять или извлекать данные из базы данных с помощью злонамеренных SQL-запросов;
- Предсказуемость идентификаторов сессий, что ведет к перехвату и угону пользовательских сессий;
- Подмену содержимого (Content Spoofing), когда пользователю показывается фальшивый контент, но кажется, что он настоящий [1].

## 2. Методы анализа уязвимостей

Наиболее распространенными подходами к выявлению уязвимостей являются автоматизированное сканирование, ручное тестирование и проведение пентестов с использованием методов «белого», «серого» и «черного» ящика. Системный сбор и анализ структуры веб-приложения позволяют выделить потенциально уязвимые точки доступа и параметры в URL адресах, методах и входных данных [2].

## 3. Методы обеспечения безопасности

Для защиты сайтов применяются многоуровневые меры, среди которых:

- Защита с помощью SSL для шифрования трафика и предотвращения перехвата данных;
- Использование систем фильтрации трафика, таких как Cloudflare, и файрволов для блокировки подозрительных IP-адресов;

- Настройка безопасной конфигурации веб-серверов и регулярное обновление CMS и других компонентов для устранения известных уязвимостей;
- Внедрение системы многофакторной аутентификации и одноразовых паролей для защиты административных панелей;
- Мониторинг и журналирование действий для своевременного обнаружения подозрительной активности;
- Защита от DDoS-атак с помощью специализированных решений, обеспечивающих сохранение доступности сайта даже при больших нагрузках [3].

## 4. Оценка эффективности защитных решений

Современные системы защиты объединяют сигнатурные методы, анализ поведения и машинное обучение для адаптивного реагирования на угрозы и повышения устойчивости к атакам. Важным фактором является быстрое обнаружение и реагирование на инциденты, что снижает время простоя и ущерб.

1. Защита с помощью SSL оценивается по уровню шифрования и правильности настройки, что обеспечивает конфиденциальность передаваемых данных и снижает риск их перехвата. Успешная реализация гарантирует высокий уровень защиты, но требует регулярного обновления и контроля.

2. Системы фильтрации трафика и WAF оцениваются по точности настроек через показатели ложных срабатываний и пропущенных атак. Хорошо настроенный WAF существенно снижает риски, однако требует постоянного мониторинга и оптимизации [4].

3. Безопасная конфигурация и своевременное обновление ПО являются базовыми мерами, эффективность которых зависит от регулярного аудита и автоматизированного сканирования уязвимостей. Их успешное применение позволяет закрыть большинство известных уязвимостей [5].

4. Многофакторная аутентификация значительно снижает вероятность компрометации аккаунтов, но требует правильной организации процедуры для наибольшее продолжительной эффективности.

5. Мониторинг и оперативное реагирование на инциденты считаются ключевыми для сокращения времени простоя и минимизации ущерба. Использованием SIEM, IDS/IPS и систем машинного обучения обеспечивает своевременное выявление атак и позволяет быстро реагировать на угрозы [6].

6. Защита от DDoS-атак оценивается по способности систем обеспечить доступность ресурсов при высокой нагрузке, что достигается через масштабируемость и фильтрации трафика.

В ходе проведенного научного анализа уязвимостей веб-сайтов и методов обеспечения их безопасности выявлено, что комплексный и систематический подход к выявлению и классификации уязвимостей позволяет существенно снизить риски несанкционированного доступа и атак.

**Литература:**

1. Уязвимости сайтов [Электронный ресурс] // Anti-Malware.ru. URL: https://www.anti-malware.ru/threats/site-vulnerability (дата обращения: 10.11.2025).

2. Что такое анализ защищенности веб-приложений [Электронный ресурс] // DDoS-Guard.ru. URL: https://ddos-guard.ru/blog/analiz-zashchishchennosti-veb-prilozhenii (дата обращения: 10.11.2025).

3. ТОП-10 способов защиты сайтов: как обезопасить сайт от вирусов и взлома [Электронный ресурс] // Bmamonts.ru. URL: https://bmamonts.ru/blog/kak-obezopasit-sajt-ot-virusov-i-vzloma (дата обращения: 10.11.2025).

4. Безопасность веб-приложений: обзор методов и инструментов [Электронный ресурс] // Habr.com. URL:

https://habr.com/ru/companies/webmonitorx/articles/781852/ (дата обращения: 11.11.2025).

5. Оценка уязвимостей: методики, порядок проведения и средства [Электронный ресурс] // RT-Solar.ru. URL: https://rt-solar.ru/services/jsoc/blog/5682/ (дата обращения: 11.11.2025).

6. How to Detect 10 Popular Pentester Techniques [Электронный ресурс] // Ptsecurity.com. URL: https://www.ptsecurity.com/research/analytics/how-to-detect-10-popular-pentester-techniques/ (дата обращения: 11.11.2025).