

УДК 004.056.5

А. С. ШКРАДЮК, П. А. ДАНИЛОВИЧ (ЭМ-21)

Научные руководители: старшие преподаватели *В. Е. МИНИН,*
С. С. ТАТУР

ЭКОСИСТЕМА ИНСТРУМЕНТОВ КИБЕРБЕЗОПАСНОСТИ

Даётся характеристика современного ландшафта средств кибербезопасности, задействованных в обеспечении защиты веб-ориентированных систем и цифровых платформ. Систематизированы основные классы защитного инструментария: средства статического и динамического выявления дефектов безопасности, решения для событийного мониторинга, механизмы укрепления клиентской составляющей, аппарат проверки настроек и менеджмента конфиденциальных данных. Обосновывается положение, согласно которому усложнение архитектурных решений в вебе, расширение спектра угроз и внедрение технологий генеративного искусственного интеллекта настоятельно требуют от специалиста освоения обширного набора оборонительных технологий.

В профессиональной ИТ-среде последних лет фиксируется отчетливая тенденция к усилению алармистских взглядов касательно перспектив веб-разработки. Активное внедрение конструкторов с низким порогом вхождения и генеративных нейросетевых моделей послужило питательной средой для возникновения тезиса о постепенной девальвации данной профессии [5]. Между тем, предпринятый автором анализ свидетельствует об обратном: веб-разработка не утрачивает позиций, а эволюционирует в сторону большей зрелости, где доминантным критерием профессионализма становится выстраивание системы киберзащиты. Реалии таковы, что эксплуатируемые веб-продукты находятся в зоне перманентного атакующего воздействия, что диктует необходимость внедрения совокупности страховочных мер и углублённой трактовки природы возможных брешей.

Совокупность актуальных средств безопасности распадается на несколько крупных категорий, среди которых особое место занимают утилиты анализа уязвимостей. Инструменты статического типа дают возможность фиксировать несоответствия ещё на этапе работы с репозиторием, тогда как динамические анализаторы ориентированы на оценку функционирующего экземпляра приложения; гибридные же комплексы пытаются объединить достоинства обоих методов [1]. Отдельный блок мероприятий касается ревизии внешних компонентов – контроль цепочки зависимостей призван блокировать включение в проект неблагонадёжных сторонних библиотек. Комплексное задействование перечисленных средств открывает путь к своевременному подавлению межсайтовых сценариев (XSS), инъекций

SQL-кода, ошибочных параметров конфигурации и всевозможных отклонений от утверждённых политик безопасности.

Не менее существенен сегмент решений, ориентированных на клиентскую сторону веб-продуктов. В целях пресечения атак подобного рода действует политика ограничения загружаемого контента (CSP), процедуры очистки и валидации вводимых пользователем данных, анти-CSRF-защита, сверка целостности внешних ресурсов и отслеживание модификаций DOM [2]. Инженер обязан осознавать особенности сопряжения означенных механизмов с браузерными интерфейсами и оценивать их влияние на общую архитектурную схему. В условиях лавинообразного прироста инцидентов на стороне клиента практическое владение данной группой технологий становится императивом.

Серьёзную нишу в общей системе защиты занимают подсистемы отслеживания угроз и сигнальные механизмы. Платформы SIEM аккумулируют и подвергают обработке логи безопасности, IDS-IPS-системы маркируют подозрительные паттерны сетевой активности, тогда как агентные решения EDR-XDR нацелены на превентивное блокирование атак через поведенческий анализ процессов [3]. Указанные компоненты образуют фундамент для быстрой реакции на инциденты и способствуют купированию их потенциальных последствий.

К числу приоритетных задач относится и приведение практик разработки в соответствие с отраслевыми стандартами. С этой целью применяются оценочные листы OWASP ASVS, средства валидации конфигурационных файлов, утилиты для контроля учётных данных, а также инструменты аудита интерфейсов прикладного программирования. В качестве внешнего регулятора выступают нормы GDPR, положения ISO/IEC 27001 и критерии доступности WCAG 2.1, фиксирующие параметры обработки персональной информации и безбарьерности сервисов [4]. Исполнение предписаний данных документов рассматривается как безусловное требование для компаний, оперирующих массивами личных данных и предлагающих открытые онлайн-услуги.

Обобщение изложенных аспектов приводит к заключению, что инструментарий кибербезопасности сегодня выступает в роли системообразующего элемента веб-разработки. Тенденция к усложнению кодовой базы, расширение области недружественных воздействий и внедрение синтезирующих нейросетей настоятельно мотивируют инженера к углублённому постижению принципов сохранности информации. Средства выявления брешей, мониторинговые комплексы, защитные механизмы фронтенда и инструменты стандартизации конфигураций в совокупности очерчивают круг профессиональной компетентности современного разработчика. Владение названным инструментарием выступает в качестве обязательного условия эффективной деятельности в структурах цифровой экономики и определяет конкурентную значимость кадров на фоне форсированных трансформационных процессов.

СПИСОК ЛИТЕРАТУРЫ

- 1 **Флэнаган, Д.** JavaScript. Полное руководство / Д. Флэнаган. – М. : Вильямс, 2021. – URL: <https://www.oreilly.com/library/view/javascript-the-definitive/9781491952016/> (oreilly.com in Bing) (дата обращения: 20.05.2026).
- 2 **Чиннатхамби, К.** Изучаем React / К. Чиннатхамби. – СПб. : Питер, 2019. – URL: <https://www.pearson.com/en-us/subject-catalog/p/learning-react/P200000003465/9780134843575> (pearson.com in Bing) (дата обращения: 20.05.2026).
- 3 **Бернхардт, К.** WebAssembly: практическое руководство / К. Бернхардт. – СПб. : Питер, 2022. – URL: <https://www.cs.cmu.edu/~wasm/> (дата обращения: 20.05.2026).
- 4 **Гавнер, М.** Изучаем TypeScript 4 / М. Гавнер. – М. : ДМК Пресс, 2021. – URL: <https://link.springer.com/book/10.1007/978-1-4842-7180-0> (link.springer.com in Bing) (дата обращения: 20.05.2026).
- 5 Аналитический отчёт: Рынок труда в сфере IT. – М. : Хабр Карьера, 2025. – URL: <https://habr.com/ru/articles/810923/> (habr.com in Bing) (дата обращения: 20.05.2026).

Получено 17.06.2026

ISSN 2227-1155. Сборник студенческих научных работ.
Вып. 31. Гомель, 2026

УДК 004.8:004.91

Д. В. ЯКУБОВИЧ, И. С. КУХАРЕНКО (МТ-56)

Научный руководитель – канд. физ.-мат. наук *Н. В. РЯЗАНЦЕВА*

ИНТЕГРАЦИЯ ИНСТРУМЕНТОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В OBSIDIAN

Рассматривается концепция интеграции современных ИИ-агентов в систему управления знаниями Obsidian посредством протокола MCP (Model Context Protocol). Анализируются ключевые проблемы применения больших языковых моделей в долгосрочных проектах, предлагается архитектурное решение на основе структурированной базы знаний в формате Markdown. Исследуется феномен «context rot» – деградации внимания модели при переполнении контекстного окна – и обосновывается преимущество вынесения проектных знаний во внешнее хранилище. Приводятся практические рекомендации по организации базы знаний, настройке интеграции и применению подхода в командной разработке.

Большие языковые модели (LLM) стремительно проникают в повседневную практику разработчиков, исследователей и студентов. Инструменты на базе Claude, GPT и их аналогов позволяют генерировать код, анализи-