УДК 004.03.26+004.56

Д.В. Сазонова, асп.
П.П. Урбанович, проф., д-р техн. наук (БГТУ, г. Минск)

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ И ПРОГРАММНЫХ БИБЛИОТЕК

Криптография играет ключевую роль в обеспечении безопасности программного обеспечения, предоставляя важнейшие механизмы для гарантии конфиденциальности, целостности и подлинности данных. Наряду с криптографией, задачи защиты информации решает стеганография, которая обеспечивает скрытие самого факта передачи данных, при этом современные стеганографические методы всё чаще основываются на нейросетевых технологиях [1]. Однако правильное использование криптографических приложений представляет собой сложную задачу [2]. Повышение «криптографических сбоев» подчеркивает значимость методов обнаружения криптоуязвимостей. Это согласуется с исследованиями, которые выявили высокий уровень неправильного использования криптографических приложений [3].

Ошибки в реализации криптографических алгоритмов можно разделить на несколько категорий, каждая из которых требует особых подходов к обнаружению:

1. Уязвимости, ведущие к атакам по побочным каналам (Side-Channel Vulnerabilities). Данный класс уязвимостей возникает, когда реализация непреднамеренно раскрывает секретную информацию через физические параметры работы устройства: время выполнения, энергопотребление, электромагнитное излучение [4].

2. Уязвимости управления памятью. К этой категории относятся классические ошибки, такие как переполнение буфера, использование памяти после освобождения и двойное освобождение [2].

3. Логические ошибки и неправильное использование криптографических API. Данный класс включает в себя широкий спектр ошибок, связанных с нарушением логики работы протокола или некорректным использованием криптографических библиотек [3].

4. Проблемы генерации псевдослучайных чисел. Качество генератора псевдослучайных чисел (ГПСЧ) является критическим для стойкости многих криптосистем [5]. Перспективным направлением исследований в этой области является анализ процессов синхронизации нейросетевых структур, таких как Tree Parity Machine, которые могут служить основой для генерации случайных последовательностей и протоколов обмена ключами [6].

Традиционные подходы к поиску уязвимостей можно разделить на статические (SAST), динамические (DAST) и гибридные. Однако для обнаружения сложных ошибок в криптографических реализациях все чаще применяются методы машинного и глубокого обучения.

1. Традиционные методы статического анализа. Классические SAST-инструменты работают на основе сопоставления шаблонов и набора эвристических правил. Они эффективны для поиска простых ошибок, но имеют ряд существенных недостатков, таких как высокий уровень ложных срабатываний, ограниченная адаптируемость, неспособность к обнаружению сложных семантических ошибок [3,7].

2. Применение глубокого обучения для анализа представлений кода. Современные исследования в области применения Deep Learning для анализа кода фокусируются на способах представления исходного кода, понятного для нейронной сети, и выбора архитектуры для его обработки [7].

Код может быть представлен в различных формах:

– как текст (последовательность токенов) [2,8].

– как абстрактное синтаксическое дерево (AST) [8].

– как граф: комбинирует AST, граф потока управления (CFG) и граф зависимостей по данным (DFG). Именно такое представление позволяет эффективно выявлять сложные, контекстно-зависимые уязвимости [5, 8].

Помимо этого, архитектура нейронной сети может быть следующей:

– рекуррентные нейронные сети (RNN/LSTM) [2].

– трансформеры [2,8].

– графовые нейронные сети (GNN) [5,8].

– большие языковые модели (LLM/SLM): Современные исследования демонстрируют, что LLM, такие как GPT-4, способны не только обнаруживать, но и исправлять ошибки использования криптографических API [3,7].

На основе проведённого анализа можно сделать вывод, что применение нейронных сетей, в особенности графовых архитектур (GNN) и больших языковых моделей (LLM), открывает новые возможности для обнаружения сложных криптографических уязвимостей, которые не поддаются традиционным методам статического анализа.

В дальнейшем планируется разработка гибридного подхода к автоматизации обнаружения уязвимостей реализации в криптографическом ПО на основе комбинирования методов глубокого обучения и классического статического анализа.

ЛИТЕРАТУРА

1. Сазонова Д.В. Классификация средств стеганографического анализа на основе нейросетевых технологий / Д. В. Сазонова // Информационные технологии: материалы 89-й научно-технической конференции профессорско-преподавательского состава, научных сотрудников и аспирантов с международным участием, Минск, 3 – 18 февраля 2025 г. - Минск: БГТУ, 2025.

2. Saroo Raj, R. B. Predicting Software Vulnerabilities with Deep Learning-Driven Static Code Analysis in Security and Cryptographic Systems /R.B. Saroo Raj [et al.] // Proceedings of the 2025 IEEE Conference on Artificial Intelligence and Security. – New York : IEEE, 2025. – P. 112–125.

3. Firouzi, E. Can generative AI detect and fix real-world cryptographic misuses? / E. Firouzi [et al.] // Journal of Systems and Software. – Amsterdam: Elsevier, 2025. – Vol. 210. – Article 112234.

4. Weissbart, L. J. A. Side-Channel Analysis with Deep Learning: An Evergrowing Ally in Hardware Security Evaluation: PhD Thesis / L.J. A. Weissbart. – Delft : Delft University of Technology, 2025. – 185 p.

5. Farhad, M. HYDRA: A Hybrid Heuristic-Guided Deep Representation Architecture for Predicting Latent Zero-Day Vulnerabilities in Patched Functions / M. Farhad [et al.] // arXiv preprint server. – 2025. – arXiv:2511.06220. – URL: https://arxiv.org/abs/2511.06220 (дата обращения: 23.01.2026).

6. Сазонова Д.В. Особенности синхронизации нейронных сетей в распределённых системах / Д. В. Сазонова, П.П. Урбанович // Передовые технологии и инновации в образовании и науке для улучшения качества жизни и стимулирования устойчивого экономического роста : сб. ст. VIII Междунар. науч.-техн. конф. «Минские научные чтения – 2025», Минск, 3 – 5 декабря 2025 г. : в 3 т. – Минск : БГТУ, 2025. – Т. 1. – С. 530 – 534.

7. Bappy, A. H. Case Study: Fine-tuning Small Language Models for Accurate and Private CWE Detection in Python Code / Md. A. H. Bappy [et al.] // arXiv preprint server. – 2025. – arXiv:2504.16584. – URL: https://arxiv.org/abs/2504.16584 (дата обращения: 22.01.2026).

8. Kumar A. Deep Learning-Based Cloud Security: Innovative Attack Detection and Privacy Focused Key Management / A. Kumar [et al.] // IEEE Transactions on Computers. – 2025. – Vol. 74, No. 6. – P. 1978–1989.