DOI 10.37539/2949-1991.2026.37.2.005

**Якуба Иван Леонидович,**
студент магистратуры 2 курса гр. ИСТм-41,
ФГОБУ ВО «Поволжский государственный университет
телекоммуникаций и информатики»
Yakuba Ivan Leonidovich,
2st year master's student gr. ISTm-41,
FGOBU in «Volga State University
of Telecommunications, and Informatics»

**Коваленко Татьяна Анатольевна,** к.п.н, доцент,
ФГОБУ ВО «Поволжский государственный университет
телекоммуникаций и информатики»
Kovalenko Tatiana Anatolevna, k.p., associate,
FGOBU in «Volga State University
of Telecommunications and Informatics»

# ИСПОЛЬЗОВАНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ АЛГОРИТМОВ ДЛЯ АНАЛИЗА УЯЗВИМОСТЕЙ ЛОКАЛЬНЫХ ХРАНИЛИЩ ПАРОЛЕЙ
# USING INTELLIGENT ALGORITHMS TO ANALYZE VULNERABILITIES OF LOCAL PASSWORD STORAGES

**Аннотация.** В статье рассматривается применение методов машинного обучения и поведенческого анализа для тестирования надежности локальных менеджеров паролей. Обосновывается подход адаптации алгоритмов, используемых при анализе вредоносного ПО (Malware Analysis), для задач аудита легитимных средств защиты. Исследуются перспективы использования Deep Learning для анализа системных вызовов и дампов памяти.

**Abstract.** The article discusses the application of machine learning and behavioral analysis methods for testing the reliability of local password managers. The approach of adapting algorithms used in Malware Analysis for auditing legitimate security tools is substantiated. The prospects of using Deep Learning for analyzing system calls and memory dumps are explored.

**Ключевые слова:** Менеджер паролей, машинное обучение, поведенческий анализ, поиск уязвимостей, информационная безопасность, искусственный интеллект.

**Keywords:** Password manager, machine learning, behavioral analysis, vulnerability scanning, information security, artificial intelligence.

Сфера информационной безопасности переживает смену парадигм, где традиционные сигнатурные методы и ручной аудит кода уступают место адаптивным системам на базе искусственного интеллекта (ИИ). Локальные менеджеры паролей, являясь критически важным узлом хранения конфиденциальной информации, требуют применения передовых методик проверки надежности. Современные исследования показывают, что алгоритмы, изначально разработанные для детектирования вредоносного ПО, могут быть эффективно перепрофилированы для поиска уязвимостей в защищенных приложениях [1].

Основная проблема существующих методов аудита менеджеров паролей заключается в их статичности. В то же время, применение методов глубокого обучения (Deep Learning) позволяет анализировать динамическое поведение приложения, выявляя аномалии в работе с памятью и файловой системой [2].

Основные векторы применения интеллектуальных алгоритмов:

1. Анализ системных вызовов (System Calls Analysis): Использование нейросетей для мониторинга обращений менеджера паролей к ядру ОС, что позволяет выявить потенциальные утечки данных через побочные каналы.

2. Поведенческое профилирование (Behavioral Fingerprinting): Создание эталонных моделей работы приложения и фиксация отклонений, свидетельствующих о логических уязвимостях.

3. Гибридный анализ: Сочетание статического анализа бинарного кода и динамического наблюдения за исполнением программы в изолированной среде.

Внедрение алгоритмов машинного обучения позволяет кардинально трансформировать подход к аудиту кода, автоматизируя процесс поиска не только явных ошибок, но и скрытых «логических бомб», а также уязвимостей реализации криптографических примитивов. В отличие от статического анализа, ML-модели способны обучаться на нормальном поведении криптографических функций, выявляя микроскопические отклонения во времени выполнения операций, что часто свидетельствует о наличии уязвимостей к атакам по побочным каналам (Side-Channel Attacks).

В частности, методы Data-Driven Fingerprinting, детально описанные в работах по детектированию вредоносного ПО [3], могут быть адаптированы для верификации целостности процессов менеджера паролей. Создание динамического «цифрового отпечатка» процедуры дешифрования базы данных позволяет системе в реальном времени отслеживать, не вмешиваются ли сторонние процессы в адресное пространство приложения. Это особенно актуально для локальных хранилищ, где безопасность зависит от корректности работы программного кода и защиты оперативной памяти от скрапинга.

Отдельный вектор исследований направлен на проблему «черного ящика» в нейросетях. Особое внимание уделяется интерпретируемости моделей в приложениях с высоким уровнем риска, к которым относятся средства защиты информации. Простого вердикта о наличии уязвимости недостаточно; применение ML-моделей для аудита требует понимания причинно-следственных связей – почему алгоритм классифицировал определенную последовательность системных вызовов как опасную. Как отмечается в современной литературе [4], внедрение методов объяснимого ИИ (XAI) позволяет снизить количество ложных срабатываний и предоставляет разработчикам детальный отчет о том, какие именно паттерны поведения привели к срабатыванию детектора. Это критически важно для устранения найденных архитектурных брешей и верификации надежности исправлений.

Современные техники гибридного анализа (Hybrid Analysis), объединяющие статический разбор кода и динамический мониторинг в песочнице, демонстрируют высокую эффективность в выявлении скрытых дефектов ПО. Адаптация этих техник для менеджеров паролей позволяет выявлять небезопасное обращение с буфером обмена или остаточные следы паролей в оперативной памяти (RAM) после завершения сеанса [5].

Таким образом, интеграция подходов из области анализа вредоносного ПО в процессы тестирования средств защиты информации открывает новые возможности для повышения надежности локальных хранилищ паролей. Использование интеллектуальных алгоритмов позволяет перейти от реактивного исправления ошибок к проактивному обнаружению уязвимостей на ранних этапах.

*Список литературы:*

1. Stamp M., Alazab M., Shalaginov A. (eds.) Malware Analysis Using Artificial Intelligence and Deep Learning: Methods, Examples and Challenges. – Cham: Springer, 2021. – 650 с. DOI: 10.1007/978-3-030-62582-5.

2. Omar M. Machine Learning for Cybersecurity. – Springer, 2022. – 200 с.
3. Karbab E. M. B., Debbabi M., Derhab A., Mouheb D. Android Malware Detection using Machine Learning: Data-Driven Fingerprinting and Threat Intelligence. – Cham: Springer, 2021. – 212 с.
4. Hall P., Curtis J., Pandey P. Machine Learning for High-Risk Applications. – O'Reilly Media, 2023. – 300 с.
5. Barker D. Malware Analysis Techniques. – Independently published, 2023-2024.