УДК 004.9

МЕТОДЫ И ТЕХНОЛОГИИ ДЛЯ СИСТЕМЫ ОПРЕДЕЛЕНИЯ УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ОСНОВЕ БЛОКЧЕЙНА

Наумов М.А. (ИТМО)
Научный руководитель – кандидат технических наук, доцент Иванов С.Е.
(ИТМО)

Введение. Уязвимость программного обеспечения представляет собой недостаток в системе, который может намеренно нарушить ее целостность и вызвать неполадки в работе. Своевременное обнаружение проблем, их устранение и отслеживание в общедоступном, защищенном формате имеет большое значение, поскольку это позволяет создавать безопасное программное обеспечение, в оперативном формате устранять недостатки системы и накапливать базу проблемных мест. Для создания такой надежной и многофункциональной системы по обнаружению уязвимостей требуется решение прикладных задач, связанных с угрозами безопасности программного обеспечения, а также совместной работе централизованных и децентрализованных сервисов. Изучение появления и обнаружения уязвимостей с помощью децентрализации наиболее актуально в связи со стремительным развитием информационных технологий, где люди все чаще и чаще сталкиваются с данными, которыми они владеют и всячески оперируют, а также возросшими требованиями к надежности и безопасности для различных информационных процессов [1].

Основная часть. С помощью стандартизованных методов описания и идентификации программного обеспечения решается следующий тип задач:

1) Задачи об определении проблемных частей кода и однозначном их сопоставлении с информацией в открытых базах данных угроз. Программное обеспечение существует в различных форматах, которые поддерживаются различными операционными системами: Windows, Unix/Linux, MacOS и т. д. Для каждого случая существует определенный подход в поиске уязвимостей. Однако пакеты могут иметь одинаковые названия в различных дистрибутивах, что вызывает трудности в однозначности сопоставления найденных уязвимостей с поставщиком операционной системы и корректности окончательного результата. Конвертация найденных метаданных о пакетах в CPE (стандартизованные методы описания и идентификации программного обеспечения) решает данную проблему [2].

С помощью децентрализованных методов хранения и обработки информации решаются следующие задачи:

1) Обеспечение надежного хранения найденных уязвимостей с однозначным разграничением доступа к ним [1].
2) Передача данных динамического размера в децентрализованное хранилище, где каждый блок имеет статическую длину. При добавлении данных в блокчейн используются смарт-контракты, которые отслеживают и обеспечивают выполнение описанных условий создания новых записей. Каждый блок состоит из полей, которые имеют конкретную длину в байтах, что обеспечивает быстродействие сети. Однако при сканировании программного обеспечения заранее неизвестно, сколько угроз будет найдено, а значит такие данные очень сложно записать в блок. Данную проблему решает распределенная файловая система, данные в которой хранятся на различных узлах, чье месторасположение определяется по хэшу загруженных данных, который имеет статический размер и подходит для записи в блокчейн [3].

Выводы. Проведен анализ обнаружения уязвимостей программного обеспечения, разработана методика алгоритма сканирования угроз с их добавлением в блокчейн и выполнено тестирование системы в среде разработки блокчейн кластера.

Список использованных источников:

1. Web3 [Электронный ресурс]. – URL: https://en.wikipedia.org/wiki/Web3 (дата обращение 12.10.23)
2. CPE (Common Platform Enumeration) About CPE – Archive [Электронный ресурс]. – URL: https://cpe.mitre.org/about/ (дата обращение 10.11.23)
3. IPFS: An open system to manage data without a central server [Электронный ресурс]. – URL: https://ipfs.tech/ (дата обращение 24.10.23)