УДК 004.457

# ОБНАРУЖЕНИЕ РУТКИТОВ НА БАЗЕ МЕХАНИЗМА IO_URING В ОПЕРАЦИОННОЙ СИСТЕМЕ LINUX

**Потапова П. А.**[1]
**Научный руководитель – канд. техн. наук, доцент Гирик А. В.**[1]
[1]Университет ИТМО
potapova.polia2002@yandex.ru

## Введение

Современные руткиты представляют серьезную угрозу информационной безопасности, поскольку скрывают вредоносную активность и препятствуют своевременному обнаружению факта компрометации. В операционной системе (ОС) Linux присутсвует интерфейс io_uring: он обеспечивает асинхронное выполнение операций ввода-вывода в обход классических системных вызовов. Ввиду этого, io_uring может быть использован руткитами с целью сокрытия своих действий. Механизмы ОС Linux, такие как eBPF, позволяют повысить наблюдаемость системы и делают возможным детектирование руткитов на базе механизма io_uring.

## Основная часть

Механизм io_uring, впервые появившийся в версии 5.1, представляет собой интерфейс ядра Linux для асинхронных операций ввода-вывода. Интерфейс io_uring работает с двумя кольцевыми буферами, которые используются программами и ядром, что приводит к минимизации количества системных вызовов и предотвращению копирования данных между пространствами пользователя и ядра [1]. Интерфейс io_uring поддерживает широкий спектр операций, в частности, работу с файлами и сетевыми соединениями, что делает его мощным инструментом, особенно если речь идет о руткитах. Большинство защитных инструментов отслеживают подозрительные системные вызовы и хуки, однако игнорируют все, что связано с интерфейсом io_uring, что создает "слепое пятно" в операционной системе.

В 2025 году появилось несколько proof-of-concept руткитов, которые исполняют несанкционированные действия благодаря интерфейсу io_uring и остаются незамеченными в системе. Так руткит Curing [2] умеет получать команды с удаленного сервера и выполнять произвольные операции, не прибегая к использованию классических системных вызовов, благодаря чему остается незамеченным большинством популярных средств защиты.

Современный механизм eBPF, являясь наследником BPF, расширяет его функционал. Сейчас eBPF используется не только для работы с сетевым стеком, но и для профилирования, наблюдаемости и безопасности [3]. Использование eBPF совместно с такими механизмами ОС Linux как LSM, kprobes или tracepoints [4] позволяет расширить возможности для мониторинга ОС, не ограничиваясь перехватом системных вызовов. Это позволяет обнаруживать совершение несанкционированных действий через интерфейс io_uring.

## Выводы

Интерфейс io_uring в ОС Linux открывает значительные возможности для ускорения ввода-вывода, однако его возможностями также пользуются руткиты с целью сокрытия своей вредоносной деятельности. Интеграция механизма eBPF с доступными в ОС Linux хуками обеспечивает повышение наблюдаемости системы, что способствует

улучшению детектирования потенциальных угроз информационной безопасности, в том числе руткитов на базе io_uring.

**Литература**


1. io_uring(7) — Linux manual page [Электронный ресурс]. – 2025. – URL: https://man7.org/linux/man-pages/man7/io_uring.7.html (дата обращения: 15.02.2026).
2. armosec/curing // GitHub : сайт. – Текст : электронный. – 2025. – URL: https://github.com/armosec/curing (дата обращения: 15.02.2026).
3. eBPF и его возможности / Хабр [Электронный ресурс]. – 2023. – URL: https://habr.com/ru/companies/timeweb/articles/733058/ (дата обращения: 15.02.2026).
4. Родионов Д.К., Кузнецов С.Д. Разработка и реализация средства тестирования на устойчивость хранимых данных для приложений, основанных на файловых системах // Труды Института системного программирования РАН. 2023. № 1 (35). С. 205–222.


Потапова П.А. (автор) Подпись

Гирик А.В. (научный руководитель) Подпись