УДК 004.457

З.С. КУТЬИН

*Национальный исследовательский ядерный университет «МИФИ», Москва*

# ПРОГРАММА ДЛЯ АНАЛИЗА СВЕДЕНИЙ АВТОРИЗАЦИИ LINUX

Рассматривается проблема обеспечения информационной безопасности (ИБ) Linux-систем. В качестве решения предлагается программа для анализа сведений авторизации. Инструмент, созданный на Python, предоставляет удобный графический интерфейс для централизованного просмотра и анализа данных из лог-файлов secure/auth, wtmp и btmp. Ключевые функции включают фильтрацию по дате, поиск и сортировку, что значительно упрощает для администратора ИБ задачу выявления подозрительных попыток входа и несанкционированного доступа. Программа представляет собой готовый инструментарий для усиления защиты Linux-инфраструктур.

## Введение

Подавляющая часть информационных систем, которые являются в том числе объектами критической информационной инфраструктуры, включая серверные платформы, облачные вычисления и автоматизированные рабочие места рядовых сотрудников, построены на базе ОС Linux [1]. С ростом актуальности этой ОС растет и количество угроз ИБ. Одним из основных способов защиты является анализ сведений об авторизации пользователей. Функциональный инструмент, обрабатывающий эти данные, позволит администратору ИБ быстрее выявлять аномалии, предотвращать утечки информации и своевременно реагировать на потенциальные угрозы.

## Разработка программы анализа сведений авторизации Linux

При разработке программы использовалась парадигма объектно-ориентированного программирования, которая удовлетворяет требованиям современной разработки, а также позволяет реализовать функционал для анализа данных: подсвечивание выбранных строк, поиск по ключевым словам, сортировка [2]. В программе реализована авторизация пользователей с повышенными привилегиями (root) для доступа к сведениям авторизации без ограничений. Интерфейс программы обеспечивает вывод информации из различных лог-файлов: secure/auth (авторизация пользователей, включая удачные и неудачные попытки входа в систему, а также задействованные механизмы аутентификации.), wtmp (записи о всех сессиях входа в систему), btmp (записи о неуспешных попытках входа). Кроме того, в программе

реализован вывод всех событий авторизации по указанной дате. Интерфейс программы показан на рис. 1.

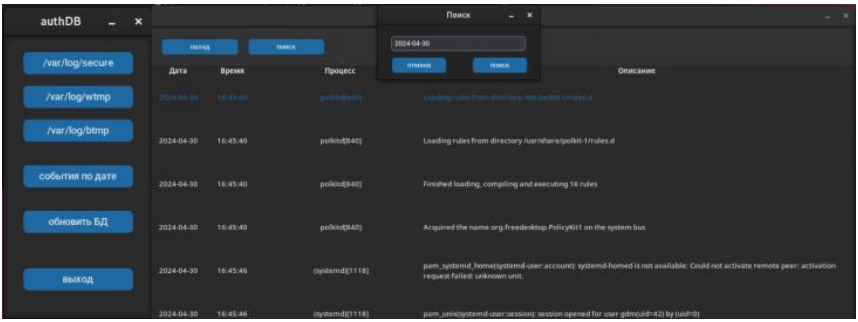


*Рис. 1. Интерфейс программы для анализа сведений авторизации Linux*

Логика и интерфейс программы разработаны с помощью языка программирования Python и совместимых с ним библиотек. Этот язык является одним из лучших вариантов для разработки качественных и полезных инструментов, в том числе в сфере ИБ [3].

## Заключение

Разработанная программа сможет повысить эффективность работы администратора ИБ благодаря широкому функционалу для анализа сведений авторизации и применения современных технологий, а значит снизить процент реализации угроз ИБ в организации. При этом использование актуального языка программирования позволит расширять функционал программы под нужды развивающегося мира технологий.

*Список литературы*

1. Зайнабидинов Рахматулло Мадаминович Обзор ядра Linux и его роль в современных информационных системах // Universum: технические науки. 2024. №3 (120). URL: https://cyberleninka.ru/article/n/obzor-yadra-linux-i-ego-rol-v-sovremennyh-informatsionnyh-sistemah (дата обращения: 23.10.2025).

2. Гулджанова Д., Мырадов Р., Довранов С. История развития объектно-ориентированного программирования // Вестник науки. 2024. №5 (74). URL: https://cyberleninka.ru/article/n/istoriya-razvitiya-obektno-orientirovannogo-programmirovaniya (дата обращения: 23.10.2025).

3. Дронов В.Ю., Дронова Г.А. Python как средство автоматизации в информационной безопасности. Контроль актуальности защиты от вредоносного кода // ОмГТУ. 2021. № 4. URL: https://cyberleninka.ru/article/n/python-kak-sredstvo-avtomatizatsii-v-informatsionnoy-bezopasnosti-kontrol-aktualnosti-zaschity-ot-vredonosnogo-koda (дата обращения: 23.10.2025).