Сініцина О.В., магістрантка
Бродський Ю.Б., к.т.н, доцент
Єфіменко А.А., к.т.н, доцент
Державний університет «Житомирська політехніка»

АНАЛІЗ НАЙПОШИРЕНІШИХ ЗАГРОЗ ДЛЯ LINUX-СИСТЕМ У 2024 РОЦІ

Операційна система Linux залишається однією з найбільш поширених платформ для серверів, хмарних інфраструктур і вбудованих систем завдяки її стабільності, безпеці та відкритому вихідному коду. Однак зростаюча популярність Linux-систем призводить до збільшення кількості кіберзагроз, спрямованих на їхню компрометацію.

Метою цього дослідження є аналіз найбільш поширених загроз для Linux-систем у 2024 році, а також вивчення ефективних методів їхньої нейтралізації. Дослідження базується на аналізі вразливостей, виявлених у 2024 році, та рекомендаціях з безпеки, спрямованих на мінімізацію ризиків для користувачів та організацій.

Згідно з дослідженням MITRE, проведеним на основі аналізу 31 770 CVE-записів, у 2024 році було виявлено критично важливі вразливості програмного забезпечення, які становлять загрозу безпеці Linux-систем. Найбільш небезпечними серед них стали помилки в архітектурі, програмному коді та механізмах реалізації. Особливу загрозу становлять вразливості нульового дня, кількість яких значно зросла порівняно з попередніми роками. Загальний збиток від хакерських атак у 2024 році досяг 2,3 мільярда доларів США, що на 40% більше, ніж у 2023 році.[1]

На основі аналізу вразливостей найбільш поширеними загрозами для Linux-систем стали:

1. **SQL Injection (CWE-89)** – виникає у випадку некоректної обробки введених користувачем даних, що дозволяє виконання довільних SQL-команд у базі даних. Це може призвести до несанкціонованого доступу, модифікації або видалення даних.
2. **Cross-Site Scripting – XSS (CWE-79)** – вразливість, що виникає через недостатню фільтрацію введених користувачем даних, що дозволяє виконання шкідливих скриптів у веб-браузерах інших користувачів. Наслідки включають компрометацію облікових записів та викрадення конфіденційної інформації.
3. **OS Command Injection (CWE-78)** – експлуатація неконтрольованого введення даних у командний інтерпретатор операційної системи, що дозволяє виконувати довільні команди на сервері та призводить до повної компрометації системи.[2]

Окрім зазначених загроз, у 2024 році було виявлено численні вразливості з високим рейтингом CVSS, серед яких варто виокремити CVE-2024-42256 з рейтингом 9,8. Ця вразливість дозволяла несанкціонований віддалений доступ до системи через виконання довільного коду. Також значну небезпеку становили вразливості ядра Linux, які призводили до пошкодження пам’яті, збоїв у роботі системи та порушення її стабільності. Для мінімізації наслідків експлуатації таких вразливостей необхідно впроваджувати методи оновлення, які не потребують перезавантаження операційної системи.[3]

Для забезпечення належного рівня безпеки Linux-інфраструктури необхідно дотримуватись таких рекомендацій:

- Регулярне впровадження останніх патчів для ядра та програмного забезпечення дозволяє закрити відомі вразливості та зменшити ризик атак.
- Застосування технологій безперервного оновлення без перезавантаження мінімізує простої та підвищує рівень безпеки.
- Контроль доступу та моніторинг активності – багаторівнева аутентифікація, обмеження привілеїв користувачів та аналіз журналів доступу сприяють ранньому виявленню підозрілих дій.
- Проведення тренінгів щодо безпечних методів роботи з Linux-системами допомагає мінімізувати ризики, пов’язані з людським фактором.

Це дослідження дозволило визначити основні загрози для Linux-систем, серед яких SQL-ін’єкції, XSS-атаки, ін’єкції команд операційної системи, а також експлуатація вразливостей з високим рейтингом CVSS. Крім того, було розглянуто ефективні методи їхньої нейтралізації, включаючи регулярне оновлення програмного забезпечення, впровадження багаторівневої аутентифікації, моніторинг активності та навчання персоналу. Дотримання запропонованих рекомендацій сприятиме підвищенню безпеки Linux-інфраструктури та мінімізації кіберзагроз у майбутньому.

Список використаних джерел:

1. Дослідження MITRE. URL: https://www.bleepingcomputer.com/news/security/mitre-shares-2024s-top-25-most-dangerous-software-weaknesses/ (дата звернення: 21.03.2025).
2. Загальний перелік вразливостей (CWE). URL: https://cwe.mitre.org/ (дата звернення: 21.03.2025).
3. Перелік вразливостей NIST. URL: https://nvd.nist.gov/vuln (дата звернення: 21.03.2025).