

ЗАСОБИ ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ ОПЕРАЦІЙНИХ СИСТЕМ З ВІДКРИТИМ КОДОМ

Цуканов Є.Є., Сорокін А.Р., Дяченко Д.О.

Харківський національний університет радіоелектроніки, Харків, Україна

Безпека операційної системи (ОС) має першочергове значення для забезпечення цілісності, конфіденційності та доступності комп'ютерних систем і даних [1].

Проведений системний аналіз представляє всебічне дослідження багатогранної сфери безпеки ОС, спрямоване на покращення розуміння, виявлення проблем і пропонування ефективних рішень.

Метою доповіді є аналіз засобів підвищення рівня безпеки операційних систем з відкритим кодом, зокрема в контексті забезпечення конфіденційності, цілісності та доступності даних.

Дослідження спрямоване на виявлення актуальних загроз та розробку практичних рекомендацій для підвищення захисту від кіберзагроз.

В роботі розглянуті методи контролю доступу, а саме:

RBAC (Role-Based Access Control) – надає можливість управління доступом на основі ролей користувачів, кожна роль має обмежений доступ до системних ресурсів, зменшуючи ризик несанкціонованих дій;

SELinux (Security-Enhanced Linux); AppArmor – механізми обмеження доступу до системних файлів та процесів на основі політик безпеки. Вони дозволяють ізолювати процеси, запобігаючи доступу до критично важливих ресурсів.

Також запропоновано використання модулів виявлення та запобігання вторгненням (IDS/IPS): Snort і Suricata – відкриті системи для моніторингу трафіку та виявлення загроз. IDS дозволяє виявляти аномальну активність, а IPS здатен блокувати підозрілі з'єднання в реальному часі; OSSEC – IDS для моніторингу системних журналів та виявлення аномалій в активності користувачів і системи [2].

Ці методи є фундаментальними для забезпечення безпеки в операційних системах з відкритим кодом і надають змогу створювати стабільні та захищені середовища для зберігання та обробки даних.

Список літератури

1. Журило, О., Ляшенко, О. (2024) «Архітектура та системи безпеки IoT на основі туманних обчислень», Сучасний стан наукових досліджень та технологій в промисловості, (1(27), с. 54–66. doi: 10.30837/ITSSI.2024.27.054.
2. Ляшенко О. С. Система виявлення вторгнень в мережі / О. С. Ляшенко, Д. О. Гольцев, К. С. Мельникова // Проблеми інформатизації : тези доповідей восьмої міжнародної науково-технічної конференції, 26-27.11.2020. – Черкаси: ЧДТУ; Х.: НТУ «ХП»; Баку: ВА ЗС АР; Бельсько-Бяла: УТІГН; ДП «ПД ПКНДІ АП», 2020, Т. 1: секції 1-3. – С. 107.