УДК 004.45

Б. В. Войтко
М. Р. Обертюх

СИСТЕМА АВТОМАТИЗОВАНОГО РОЗГОРТАННЯ ОПЕРАЦІЙНОЇ СИСТЕМИ LINUX ІЗ ЗАХИЩЕНОЮ КОНФІГУРАЦІЄЮ МЕРЕЖЕВОГО ДОСТУПУ

Вінницький національний технічний університет

Анотація

У роботі досліджено сучасні методи автоматизованого розгортання операційних систем Linux, засоби централізованого адміністрування та механізми захисту мережевого доступу. Основою проєкту є використання технологій PXE або Autoinstall, а також системи керування конфігурацією Ansible для автоматичного налаштування серверного середовища.

Розроблена система дозволяє автоматизувати встановлення Linux-серверів, забезпечити стандартизовану конфігурацію та мінімізувати ризик помилок адміністратора під час налаштування.

Ключові слова: Linux; автоматизоване розгортання; мережева безпека; SSH; PXE; Ansible; Kickstart; firewall; системне адміністрування.

Abstract

This paper examines modern methods for the automated deployment of Linux operating systems, centralized administration tools, and network access security mechanisms. The project is based on the use of PXE or Autoinstall technologies, as well as the Ansible configuration management system, to automatically configure the server environment.

The developed system allows for the automation of Linux server installation, ensures standardized configuration, and minimizes the risk of administrator errors during setup.

Keywords: Linux; automated deployment; network security; SSH; PXE; Ansible; Kickstart; firewall; system administration.

Вступ

Актуальність теми бакалаврської кваліфікаційної роботи обумовлена необхідністю автоматизації процесів встановлення та адміністрування операційних систем Linux у сучасних серверних середовищах. Зі збільшенням кількості серверів та мережевих пристроїв виникає потреба у швидкому, централізованому та безпечному розгортанні операційних систем без значного ручного втручання адміністратора. Особливо актуальним є забезпечення захищеного мережевого доступу до серверів, оскільки неправильне налаштування служб та мережевих параметрів може призводити до несанкціонованого доступу, витоку даних та мережевих атак.

Аналіз останніх досліджень і публікацій показав, що сучасні серверні інфраструктури активно використовують технології PXE-завантаження, Autoinstall, cloud-init та системи конфігураційного керування Ansible для автоматизації процесів встановлення та налаштування Linux-систем. Значна увага приділяється також використанню засобів мережевого захисту, таких як SSH, firewall та Fail2Ban, які дозволяють підвищити рівень інформаційної безпеки серверного середовища.

Робота пов’язана з напрямками розвитку сучасних інформаційних технологій у сфері автоматизації адміністрування комп’ютерних систем, мережевої безпеки та централізованого керування серверною інфраструктурою. Тема дослідження відповідає освітньо-професійному напряму підготовки фахівців у галузі комп’ютерної інженерії.

Результат дослідження

У ході дослідження було визначено ключові фактори, які впливають на ефективність автоматизованого розгортання операційних систем та управління серверною інфраструктурою, серед яких: швидкість введення нових вузлів в експлуатацію, абсолютна ідентичність та стандартизація конфігурацій безпеки, мінімізація ручного втручання адміністратора (парадигма Zero-Touch Provisioning) та можливість проактивного захисту системи від мережевих атак із першої секунди її

запуску[1].

Аналіз існуючих підходів до встановлення та конфігурування ОС Linux показав, що використання традиційних локальних методів (інтерактивного встановлення з фізичних носіїв) не завжди є ефективним і надійним, оскільки вони можуть призводити до виникнення низки проблем. Серед них: висока ймовірність помилок через «людський фактор», поява конфігураційного дрейфу (configuration drift) на різних серверах інфраструктури, значні часові витрати на масштабування мережі, а також наявність критичного «вікна вразливості», коли свіжовстановлена система залишається незахищеною до моменту її ручного налаштування адміністратором.

Для усунення вищенаведених недоліків було запропоновано та спроєктовано систему автоматизованого розгортання ОС Linux із захищеною конфігурацією мережевого доступу. Ця система забезпечує автоматизоване завантаження та інсталяцію Ubuntu Server по локальній мережі (під час моделювання ці процеси ініціюються через скоординовану взаємодію інфраструктурних служб), базову ініціалізацію ядра та дискового простору, а також автоматичне пост-інсталяційне налаштування політик безпеки за допомогою розроблених сценаріїв конфігураційного керування. На рисунку 1 зображено структурну схему, яка відображає основні елементи системи автоматизованого розгортання та захисту Linux.

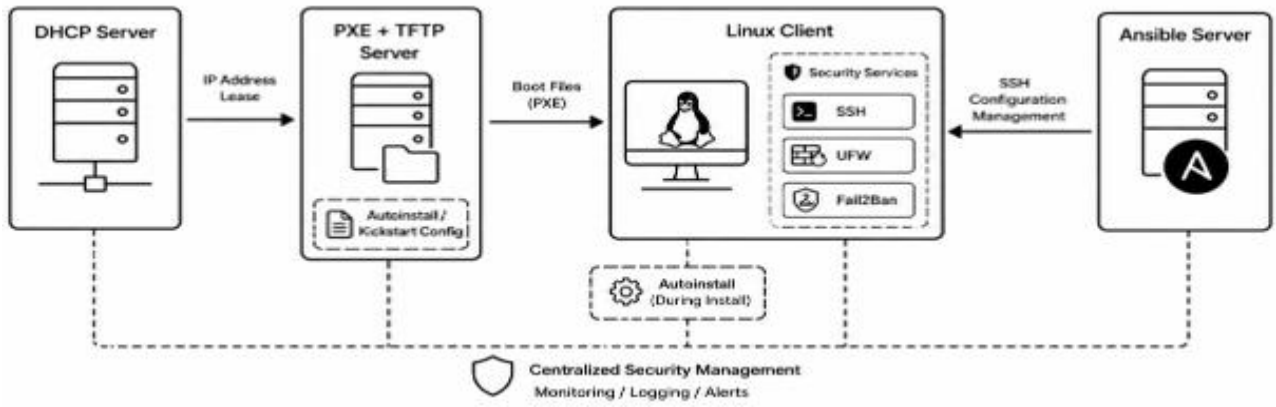

Рис. 1. Структурна схема системи автоматизованого розгортання ОС Linux

Ключовим елементом системи є наявність блоку декларативного опису інфраструктури у вигляді конфігураційних файлів формату YAML (user-data) для рушія Autoinstall та сценаріїв Ansible Playbooks. Це дозволяє адміністраторові заздалегідь чітко визначити еталонний кінцевий стан сервера, встановити схему розмітки накопичувачів, задати список необхідного програмного забезпечення та сконфігурувати параметри доступу, повністю виключивши потребу ручного введення команд під час розгортання[3].

У системі передбачено можливість інтеграції функціоналу підсистеми захищеного мережевого доступу, який забезпечує базу для автоматизованого керування брандмауером UFW та службою активного захисту Fail2Ban через захищений протокол SSH. Це дозволяє здійснювати централізований контроль безпеки вузлів, автоматично блокувати джерела brute-force атак у реальному часі та гнучко налаштовувати правила фільтрації трафіку. Усе це забезпечує повну і безпечну інтеграцію нових обчислювальних потужностей до існуючої корпоративної мережі підприємства за допомогою технології логічної сегментації VLAN[4].

Окрім того, буловедено перевірку працездатності системи за допомогою моделювання в ізольованому віртуальному середовищі на базі технологій віртуалізації. Перевірка підтвердила коректність роботи алгоритму мережевого PXE-завантаження, безпомилковість виконання сценаріїв автоматичного встановлення, а також стабільність відбиття мережевих загроз службою Fail2Ban та швидкість реакції брандмауера на критичні зміни показників активності. Усе це показує, що система повністю відповідає критеріям технічного завдання та готова до практичного використання.

Як результат, за допомогою використання поточного підходу досягається високошвидкісне автоматизоване розгортання Linux-серверів у режимі реального часу, автоматизація збору та застосування налаштувань безпеки (парадигма Infrastructure as Code) та миттєве реагування на спроби несанкціонованого доступу. Це в цілому сприяє підвищенню рівня відмовостійкості інфраструктури, оновленню та оптимізації управління адміністративними ресурсами та забезпеченню надійного й безпечного середовища для функціонування корпоративних сервісів[1].

Висновки

У результаті виконання бакалаврської кваліфікаційної роботи було розроблено систему автоматизованого розгортання операційної системи Linux із захищеною конфігурацією мережевого

доступу, яка забезпечує автоматичне встановлення операційної системи, централізоване налаштування серверів та базовий рівень мережевої безпеки. Реалізована система дозволяє значно спростити процес розгортання Linux-серверів у локальній мережі, мінімізувати ручне втручання адміністратора та зменшити кількість помилок конфігурації.

Розроблена система має перспективи подальшого розвитку. У майбутньому можливе додавання підтримки інших Linux-дистрибутивів, інтеграція із хмарними платформами, автоматизація резервного копіювання, централізований моніторинг серверів та розширення механізмів мережевого захисту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Canonical Ltd. (2025). Ubuntu Server Documentation [Електронний ресурс] — Режим доступу: https://ubuntu.com/server/docs
2. Ubuntu Community Hub. (2025). Automated Server Installation [Електронний ресурс] — Режим доступу: https://discourse.ubuntu.com/t/automated-server-installation/16612
3. Red Hat Inc. (2025). Ansible Documentation [Електронний ресурс] — Режим доступу: https://docs.ansible.com
4. Fail2Ban Community. (2025). Fail2Ban Documentation [Електронний ресурс] — Режим доступу: https://fail2ban.readthedocs.io
5. LinuxConfig.org. (2025). Ubuntu Autoinstall Guide [Електронний ресурс] — Режим доступу: https://linuxconfig.org/how-to-write-and-perform-ubuntu-unattended-installations-with-autoinstall

Войтко Богдан Віталійович – студент групи 2СП-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: voytko2017@gmail.com.

Науковий керівник: ***Обертюх Максим Романович*** – доктор філософії, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, м. Вінниця.

Voitko Bogdan Vitaliyovych – student of group 2SP-22b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: voytko2017@gmail.com.

Supervisor: ***Obertukh Maksym Romanovych***– Ph.D., Associate Professor, Department of Computer Engineering, Vinnitsa National Technical University, Vinnitsa.