

СУЧАСНІ ПІДХОДИ ТА ІНСТРУМЕНТИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ МЕРЕЖЕВОГО ОБЛАДНАННЯ В ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

Вінницький національний технічний університет

Анотація

В роботі розглянуто сучасні підходи до забезпечення безпеки мережевого обладнання, визначено основні вразливості, які впливають на функціонування локальних мереж. Проаналізовано методи комплексного захисту обладнання, зокрема фізичного і програмного забезпечення. Також приділено увагу безпечним протоколам адміністрування, системам автентифікації та авторизації користувачів, застосуванню мережевої сегментації, системам моніторингу та важливості регулярного оновлення програмного забезпечення.

Ключові слова: Мережеве обладнання, безпека мереж, вразливості, SSH, SNMPv3, VLAN, TACACS+, RADIUS, VPN.

Abstract

The paper examines modern approaches to ensuring network equipment security, identifies key vulnerabilities affecting local networks. It analyzes comprehensive methods for protecting equipment, including physical and software security. Attention is also paid to secure administration protocols, user authentication and authorization systems, network segmentation, monitoring systems, and the importance of regular software updates.

Keywords: network equipment, network security, vulnerabilities, SSH, SNMPv3, VLAN, TACACS+, RADIUS, VPN

Основні вразливості мережевого обладнання та їх вплив на безпеку мереж

Мережеве обладнання є ключовим компонентом локальних комп'ютерних мереж, і його захищеність безпосередньо впливає на загальну стабільність та безпеку всієї мережевої інфраструктури. Основними вразливостями мережевого обладнання є несанкціонований доступ, злами через відомі уразливості прошивок і програмного забезпечення, а також атаки типу «відмова в обслуговуванні» (DoS). Ці проблеми можуть призводити до витоку конфіденційної інформації, втрати контролю над мережею і навіть повного припинення роботи інформаційних систем. Небезпека таких загроз зростає з поширенням IoT-пристроїв та збільшенням кількості підключених пристроїв до локальної мережі. Водночас, у багатьох випадках вразливості виникають через нехтування базовими правилами інформаційної безпеки, наприклад, слабкі паролі, застарілі версії програмного забезпечення або неправильні налаштування. Для зменшення цих ризиків необхідно регулярно проводити аудит безпеки мережевого обладнання, використовувати актуальні методики тестування на проникнення (penetration testing), а також своєчасно оновлювати програмне забезпечення пристроїв [2].

Комплексні методи захисту мережевого обладнання

Комплексний підхід до захисту мережевого обладнання передбачає як фізичну, так і програмну складову. Фізичний захист включає встановлення обладнання в спеціалізовані комутаційні шафи з обмеженим доступом, організацію відеоспостереження та систем контролю доступу до серверних приміщень. Це запобігає несанкціонованим фізичним втручанням, які можуть призвести до крадіжок

або пошкоджень обладнання. Програмні засоби захисту включають використання фаєрволів, систем виявлення та запобігання вторгненням (IDS/IPS), а також встановлення оновлень прошивок, які закривають виявлені уразливості. Комплексний захист передбачає також налаштування захищеного доступу до пристроїв за допомогою криптографічних протоколів. Важливим аспектом комплексного підходу є навчання персоналу правилам інформаційної безпеки, оскільки людський фактор залишається одним із найслабших місць у будь-якій системі захисту [1, 3].

Безпечні протоколи адміністрування мережевих пристроїв

Адміністрування мережевого обладнання повинно здійснюватися з використанням безпечних протоколів, таких як SSH, SNMPv3 та HTTPS. Використання незахищених протоколів (наприклад, Telnet або HTTP) суттєво збільшує ризик перехоплення трафіку та викрадення автентифікаційних даних. SSH забезпечує шифрування каналу зв'язку, що захищає інформацію про логіни, паролі та конфігурації пристроїв. SNMPv3 має вбудовані механізми шифрування та автентифікації, що робить його значно безпечнішим порівняно з попередніми версіями SNMP. HTTPS використовується для безпечного веб-інтерфейсу пристроїв, дозволяючи адміністраторам безпечно керувати пристроями через браузер. Важливо належним чином налаштовувати ці протоколи, регулярно оновлювати сертифікати і забезпечувати доступ до адміністративних інтерфейсів лише перевіреним особам [2].

Системи централізованого моніторингу та управління (SIEM, NMS)

Системи централізованого моніторингу та управління, такі як SIEM (Security Information and Event Management) і NMS (Network Management System), відіграють важливу роль у забезпеченні безпеки мережевого обладнання. SIEM-системи дозволяють централізовано збирати, аналізувати та зберігати події безпеки, що надходять з мережевих пристроїв. Це допомагає виявляти загрози на ранніх стадіях і оперативно реагувати на інциденти. NMS-системи забезпечують централізований контроль стану та продуктивності обладнання, дозволяють відстежувати стан мережевих компонентів у реальному часі, що суттєво спрощує процес адміністрування та забезпечення стабільності роботи мережі. Регулярний моніторинг дозволяє швидко реагувати на будь-які проблеми, знижуючи ризик простоїв та несанкціонованого доступу [4].

Оновлення прошивок та резервне копіювання конфігурацій мережевого обладнання

Регулярне оновлення прошивок та програмного забезпечення мережевого обладнання є важливою складовою підтримки високого рівня безпеки. Виробники обладнання регулярно випускають оновлення, що містять виправлення критичних уразливостей, виявлених під час експлуатації. Створення резервних копій конфігурацій пристроїв дозволяє оперативно відновити роботу обладнання після збоїв або кібератак. Важливо, щоб резервні копії зберігалися у захищених місцях та регулярно тестувалися на можливість відновлення. Впровадження політики регулярних оновлень та резервного копіювання дозволяє значно знизити ризики, пов'язані з уразливостями та несправностями [1].

Захищені віддалені підключення до мережевого обладнання

Віддалений доступ до мережевого обладнання є необхідним у сучасних умовах, проте він має бути ретельно захищеним. Для цього використовують VPN-технології, такі як IPsec та SSL VPN, що забезпечують шифрування каналу зв'язку. Правильна конфігурація VPN дозволяє забезпечити захищений доступ до мережевих ресурсів навіть з неперевіраних мереж, таких як загальнодоступний Wi-Fi. Крім того, додаткові заходи безпеки, такі як двофакторна автентифікація, підвищують надійність захисту. Впровадження таких рішень дозволяє зберігати високий рівень безпеки мережевого обладнання навіть у разі дистанційної роботи адміністративного персоналу [3].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Азаров, О. Д. Комп'ютерні мережі [Електронний ресурс] : навч. посіб. / О. Д. Азаров, С. М. Захарченко, О. В. Кадук, М. М. Орлова ; Вінниц. нац. техн. ун-т. – Вінниця, 2020. – Режим доступу: <http://ot.vntu.edu.ua> (дата звернення: 06.03.2025). – Назва з екрану.
2. Бурячок, В. Л. Технології забезпечення безпеки мережевої інфраструктури : підручник / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний ; Київ. ун-т ім. Бориса Грінченка. – Київ, 2019. – 218 с. – Режим доступу: <http://elibrary.kubg.edu.ua>, <http://archive.mcnid.org.ua> (дата звернення: 06.03.2025). – Назва з екрану.
3. Савицька, Л. А. Метод та засіб моніторингу безпеки в комп'ютерній мережі засобами SIEM [Електронний ресурс] / Л. А. Савицька, Т. І. Коробейнікова, О. П. Волос, М. Г. Тарновський ; Вінниц. нац. техн. ун-т, Нац. ун-т «Львів. політехніка». – Вінниця, Львів, 2023. – Режим доступу: <https://itce.com.ua> (дата звернення: 06.03.2025). – Назва з екрану.
4. Толбатов, А. В. Система аналізу налаштувань мережевого обладнання на базі технологій Cisco в контексті інформаційної безпеки [Електронний ресурс] / А. В. Толбатов ; Сум. держ. ун-т. – Суми, 2021. – Режим доступу: <https://essuir.sumdu.edu.ua> (дата звернення: 06.03.2025). – Назва з екрану.

Манченко Вадим Віталійович, студент групи 2КІ-23мс, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: vadym.manchenko@gmail.com

Науковий керівник: **Захарченко Сергій Михайлович**, кандидат технічних наук, професор, Вінницький національний технічний університет, м. Вінниця, e-mail: zachap@i.ua

Vadym Vitaliiovych Manchenko, faculty of Information Technology and Computer Engineering

Supervisor: **Serhii Mykhailovych Zakharchenko**, PhD, Professor, Vinnytsia National Technical University, Vinnytsia, Ukraine, email: zachap@i.ua