УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ

Факультет «Інформаційно-керуючі системи та технології»

Кафедра «Транспортний зв’язок»

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломної роботи бакалавра

на тему:

ДОСЛІДЖЕННЯ МЕТОДІВ ВІДДАЛЕНОГО ДОСТУПУ ДО ОБЛАДНАННЯ ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ МЕРЕЖ

БРА 02.25.04.134.ПЗ

Виконав:
студент групи 134-ТКРТ-Д22
спеціальності 172 «Телекомунікації та радіотехніка»
Освітньої програми «Телекомунікації та радіотехніка» (роботу виконано самостійно відповідно до принципів академічної доброчесності)

Максим КУРОЧКА

Керівник:
доцент кафедри, канд. техн. наук

Ірина КОВТУН

Рецензент:
доцент кафедри АТ, канд. техн. наук, доцент

Сергій ЗМІЙ

Харків − 2025 р.

УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ

Факультет «Інформаційно-керуючі системи та технології»
Кафедра «Транспортний зв'язок»
Освітній рівень: бакалавр
Спеціальність: 172 «Телекомунікації та радіотехніка»

ЗАТВЕРДЖУЮ
В. о. завідувача кафедри, доцент

_____ С.В. Індик
(підпис)

« 07 » _____квітня____ 2025 р.

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ СТУДЕНТУ
Курочці Максиму Станіславовичу

1. Тема роботи:
«Дослідження методів віддаленого доступу до обладнання електронних комунікаційних мереж», керівник роботи: доцент кафедри, канд. техн. наук Ковтун Ірина Володимирівна, затверджені розпорядженням декана факультету інформаційно-керуючих систем та технологій від 24.02.2025 р. № 11.
2. Строк подання студентом роботи: 06.06.2025 р.
3. Вихідні дані до роботи:
− ВБН В.2.2-33-2007. Проєктування телекомунікацій;
− RFC 4251. The Secure Shell (SSH) Protocol Architecture — специфікація протоколу;
− ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): розрахунок необхідної кількості мережевого обладнання; розробка логічної структури корпоративної мережі Ethernet, визначення IP-адресації мережевих вузлів та кінцевих пристроїв; налаштування мережевого обладнання корпоративної мережі Ethernet, розробка схеми проектованої корпоративної мережі Ethernet.
5. Презентаційний матеріал: 11 слайдів.

7. Дата видачі завдання: 07.04.2025 р.

№ з/п	Назва етапів	Строк виконання етапів	**Примітка**
1	Підготовка матеріалів до оглядово-аналітичної частини дипломної роботи	21.04.2025 р	виконано
2	Розробка розділу оглядово-аналітичного характеру	12.05.2025 р	виконано
3	Розробка розділів спеціальної частини дипломної роботи з елементами моделювання	26.05.2025 р	виконано
4	Підготовка графічного матеріалу, доповіді, подання роботи на рецензію та затвердження	2.06.2025 р.	виконано

Здобувач _____ Максим КУРОЧКА
(підпис)

Керівник роботи
доцент кафедри, канд. техн. наук, _____ Ірина КОВТУН
(підпис)

Відповідальний за нормоконтроль
доцент кафедри, канд. техн. наук, доцент _____ Ірина КОВТУН
(підпис)

АНОТАЦІЯ

Актуальність роботи. У сучасних електронних комунікаційних мережах забезпечення віддаленого доступу до мережевого обладнання є ключовим аспектом адміністрування, технічної підтримки та оперативного управління. Використання протоколів Telnet і SSH дозволяє адміністраторам здійснювати керування пристроями з будь-якої точки мережі. З огляду на зростаючу потребу в захищених і надійних методах керування інфраструктурою, дослідження переваг, недоліків і особливостей впровадження даних протоколів є актуальним завданням.

Ключові слова: ВІДДАЛЕНИЙ ДОСТУП, TELNET, SSH, ШИФРУВАННЯ RSA, ЕЛЕКТРОННІ КОМУНІКАЦІЙНІ МЕРЕЖІ, УПРАВЛІННЯ ОБЛАДНАННЯМ, БЕЗПЕКА МЕРЕЖІ, КОНФІГУРАЦІЯ ОБЛАДНАННЯ, VTY, PACKET TRACER, SSH VERSION 2.

Об’єктом дослідження є процеси керування мережевим обладнанням у електронних комунікаційних мережах.

Мета роботи: дослідження методів віддаленого доступу до мережевого обладнання з використанням протоколів Telnet і SSH, а також оцінити їх ефективність і безпеку.

Структура та обсяг роботи: роботу викладено на 48 сторінках друкованого тексту, вона містить 21 рисунок, 2 таблиці, 22 джерела літератури. Робота складається зі вступу, трьох розділів, висновків, переліку умовних позначень та списку використаних джерел.

У першому розділі розглянуто теоретичні основи функціонування електронних комунікаційних мереж, поняття віддаленого доступу, а також принципи роботи протоколів Telnet і SSH.

Другий розділ присвячено практичному дослідженню методів віддаленого доступу з використанням програмного середовища Cisco Packet Tracer: описано процес налаштування, тестування, порівняння та оцінки ефективності

реалізованих рішень.

У третьому розділі проаналізовано питання безпеки при організації віддаленого доступу, наведено рекомендації щодо захисту доступу, аудиту та впровадження безпечних практик керування обладнанням.

Методи дослідження: теоретичний аналіз, математичне моделювання, емпіричне тестування.

Рекомендації щодо використання та результати впровадження. Результати роботи можуть бути використані для підготовки та налаштування інфраструктури віддаленого керування обладнанням у корпоративних мережах. Підвищення безпеки інфокомунікаційної інфраструктури.

ABSTRACT

Relevance of the work. In modern electronic communication networks, ensuring remote access to network equipment is a key aspect of administration, technical support, and operational management. The use of Telnet and SSH protocols allows administrators to manage devices from any point within the network. Given the growing need for secure and reliable infrastructure management methods, studying the advantages, disadvantages, and implementation specifics of these protocols is a relevant task.

Keywords: REMOTE ACCESS, TELNET, SSH, RSA ENCRYPTION, ELECTRONIC COMMUNICATION NETWORKS, DEVICE MANAGEMENT, NETWORK SECURITY, DEVICE CONFIGURATION, VTY, PACKET TRACER, SSH VERSION 2.

Object of the study is the process of managing network devices in electronic communication networks.

The purpose of the research: is to investigate remote access methods to network devices using Telnet and SSH protocols and to evaluate their efficiency and security.

Structure and scope of the work: the thesis is presented on 48 pages of printed text, contains 21 figures, 2 tables, and 22 literary sources. The work consists of an introduction, three chapters, conclusions, a list of abbreviations, and a list of references.

The first chapter reviews the theoretical foundations of electronic communication networks, the concept of remote access, and the principles of Telnet and SSH protocols.

The second chapter is devoted to the practical study of remote access methods using the Cisco Packet Tracer simulation environment: it describes the configuration process, testing, comparison, and evaluation of the implemented solutions' efficiency.

The third chapter analyzes security issues in organizing remote access, provides recommendations on access protection, auditing, and implementation of secure equipment management practices.

Research methods: theoretical analysis, mathematical modeling, empirical testing.

Recommendations for use and implementation results. The results of this work can be used for planning and configuring remote management infrastructure in corporate networks. It contributes to improving the security of information and communication infrastructure.

ЗМІСТ

Вступ

У сучасному світі електронні комунікаційні мережі є основою функціонування практично всіх інформаційних систем. Вони забезпечують обмін даними, доступ до ресурсів, дистанційне керування пристроями та підтримку роботи критично важливої інфраструктури. Зі зростанням масштабів мереж та кількості задіяного обладнання виникає об’єктивна потреба у впровадженні ефективних і безпечних методів віддаленого доступу до мережевих пристроїв.

Віддалене адміністрування дозволяє забезпечити оперативне налаштування, моніторинг, усунення несправностей та оновлення конфігурацій без фізичної присутності біля обладнання. Це особливо актуально в умовах територіально розподілених мереж або при роботі в критичних системах, де час реагування є вирішальним фактором. Водночас, неправильне налаштування віддаленого доступу може стати джерелом серйозних інформаційних загроз, зокрема несанкціонованого доступу, перехоплення даних або порушення конфіденційності.

Одними з найпоширеніших засобів для реалізації віддаленого доступу є протоколи Telnet і SSH. Якщо Telnet забезпечує базовий текстовий інтерфейс без захисту даних, то SSH використовує криптографічні методи для забезпечення конфіденційності та цілісності переданої інформації. Знання принципів їх роботи, особливостей налаштування та безпекових аспектів є необхідним для фахівців у сфері телекомунікацій та комп’ютерних мереж.

Актуальність дослідження полягає в необхідності забезпечення надійного та безпечного механізму віддаленого управління мережевим обладнанням з урахуванням сучасних кіберзагроз та вимог до інформаційної безпеки.

ВИСНОВКИ

У процесі виконання бакалаврської роботи було здійснено теоретичне та практичне дослідження методів віддаленого доступу до мережевого обладнання, зокрема за допомогою протоколів Telnet та SSH.

Віддалений доступ є критично важливою складовою адміністрування електронних комунікаційних мереж, адже дозволяє здійснювати конфігурацію, моніторинг та усунення несправностей без фізичної присутності біля обладнання.

У теоретичній частині було розглянуто особливості архітектури електронних комунікаційних мереж, принципи функціонування протоколів віддаленого доступу та загрози, які виникають під час їх використання.

Протокол Telnet забезпечує базову функціональність для віддаленого керування, однак має серйозні недоліки, зокрема відсутність шифрування переданих даних, що робить його вразливим до атак типу “man-in-the-middle” та перехоплення облікових даних.

Протокол SSH є значно безпечнішим рішенням завдяки використанню шифрування, автентифікації та контролю цілісності даних. Його застосування значно знижує ризики компрометації інформації під час віддаленого доступу.

У роботі також було проаналізовано потенційні загрози, пов’язані з використанням віддаленого доступу, та запропоновано комплексні заходи захисту: застосування шифрування, контроль доступу до VTY-ліній, журналювання дій, використання ACL, тайм-аутів сесій, оновлення прошивок, а також навчання персоналу.

Таким чином, результати дослідження підтверджують, що безпечне впровадження віддаленого доступу до обладнання електронних комунікаційних мереж можливе лише за умови використання захищених протоколів, таких як SSH, та дотримання сучасних вимог до інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kurose, James F., and Keith W. Ross. Computer Networking: A Top-Down Approach. 8th ed., Boston: Pearson, 2020.

2 Stallings, William. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. Boston: Pearson, 2016.

3. Tanenbaum, Andrew S., and David J. Wetherall. Computer Networks. 5th ed., Upper Saddle River: Pearson Prentice Hall, 2011.

4. Ramaswami, Rajiv, and Kumar N. Sivarajan. Optical Networks: A Practical Perspective. 3rd ed., Burlington: Morgan Kaufmann, 2010.

5. Clemm, Alexander. Network Management Fundamentals. Indianapolis: Cisco Press, 2007.

6. Cisco Systems. IP Multiservice Networking. Indianapolis: Cisco Press, 2002.

7. Subramanian, Manohar. Network Management: Principles and Practice. Boston: Addison-Wesley, 2000.

8. Minoli, Daniel. Telecommunications Technology Handbook. 2nd ed., Boston: Artech House, 2003.

9. David D. Coleman, David A. Westcott. CWNA Certified Wireless Network Administrator Study Guide Exam CWNA 107 5th Edition. SYBEX. 2018. – 1024 p.

10. Shawn M. Jackman, Matt Swartz, Marcus Burton, Thomas W. Head. CWDP Certified Wireless Design Professional Official Study Guide: Exam PW0-250. SYBEX. 2011. – 864 p.

11. Адресації в IP-мережах: Теоретичні основи та приклади розв'язання задач [Електронний ресурс]: навч. посіб. для студ. спеціальності 172 «Телекомунікації та радіотехніка» / Д. І. Могилевич, І. В. Кононова; КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2019. – 55 с.

12. Довгий С.О. Сучасні телекомунікації: мережі, технології, безпека, економіка, регулювання.[Текст] / С.О. Довгий, П.П. Воробієнко, К.Д. Гуляєв, – К.: Азимут-Україна. – 2013. – 608.

13. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.

14. Телекомунікаційні системи та мережі: навчальний посібник. [Текст] / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2017 – 384 с.

15. Bernet, D., & Vasilenko, A. Understanding and Configuring VPNs with IPsec. O'Reilly Media, 2017. – 384 p.

16. Gil, P., & Duro, R. Cryptographic Protocols in Networking: The Security of IPsec. Wiley, 2019. – 432 p.

17. Kaufman, C., & Dierks, T. IPSec: The Next Generation Internet Protocol Security. Addison-Wesley, 2002. – 528 p.

18. Raddatz, J., & Bozdag, D. An Introduction to Network Security: For Corporate Systems and Data. Springer, 2016. – 550 p.

19. Perrin, E., & Henson, R. IPSec: The Internet Protocol Security Handbook. Elsevier, 2019. – 400 p.

20. Stallings, W. Network Security Essentials: Applications and Standards. Pearson, 2017. – 288 p.

21. Easttom, C. Network Defense and Countermeasures: Principles and Practices. Pearson Education, 2020. – 640 p.

22. Rescorla, E. SSL and TLS: Designing and Building Secure Systems. Addison-Wesley Professional, 2001. – 624 p.