https://www.proconference.org/index.php/usc/article/view/usc33-00-016
DOI: 10.30888/2709-2267.2025-33-00-016

УДК 004.056.5:004.8

SECURITY CONSIDERATIONS FOR REMOTE ADMINISTRATION IN ELECTRONIC COMMUNICATIONS INFRASTRUCTURE

БЕЗПЕКОВІ АСПЕКТИ ОРГАНІЗАЦІЇ ВІДДАЛЕНОГО АДМІНІСТРУВАННЯ В ІНФРАСТРУКТУРІ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

Poliakov O.L. / Поляков О.Л.
ORCID: 0009-0007-1447-226X
master/ магістр
Kuzmin A.V. / Кузьмін А.В.
ORCID: 0009-0007-9504-3626
master/ магістр
Ivko S.O. / Івко С.О.
ORCID: 0000-0002-8723-9035
c.t.s. / к.т.н.
Non-commissioned Officers College of Military Institute of Telecommunication and Informatization, Poltava, Zinkivska, 44, 36009
Військовий коледж сержантського складу ВІТІ, Полтава, Зінківська, 44, 36009

Анотація. *У статті розглядаються безпекові аспекти віддаленого адміністрування в інфраструктурі електронних комунікацій. Проаналізовано основні загрози (перехоплення трафіку, підбір паролів, атаки на протоколи) та сучасні засоби захисту, включаючи криптографічні механізми, багатофакторну автентифікацію й управління ключами. Окрема увага приділяється практичним інструментам безпечного адміністрування (SSH, VPN, jump-host, моніторинг доступу) та перспективам розвитку (біометрія, апаратні ключі, інтеграція з IAM/PAM, DevSecOps). Основний внесок статті полягає у комплексному підході до організації безпечного віддаленого доступу, що підвищує стійкість інформаційних систем до несанкціонованого втручання.*

Ключові слова: *віддалене адміністрування, інформаційна безпека, управління доступом, криптографічні протоколи, електронні комунікації.*

Abstract. *The article addresses security aspects of remote administration in electronic communications infrastructure. Key threats (traffic interception, password attacks, protocol vulnerabilities) and protection methods such as cryptography, multi-factor authentication, and key management are analyzed. Practical tools (SSH, VPN, jump-hosts, access monitoring) and future directions (biometrics, hardware keys, IAM/PAM integration, DevSecOps) are discussed. The main contribution of the article is a comprehensive approach to secure remote access that strengthens system resilience against unauthorized intrusion.*

Key words: *remote administration, information security, access control, cryptographic protocols, electronic communications.*

Вступ.

Сучасний розвиток телекомунікаційних систем і цифровізація діяльності зумовлюють зростання потреби у віддаленому доступі та адмініструванні мережевої інфраструктури. Це забезпечує зручність управління, але водночас створює умови для нових кіберзагроз: перехоплення даних, несанкціонований доступ, компрометація облікових записів та атаки на критичні протоколи (SSH,

RDP, VPN). Проблема особливо загострюється в умовах війни, коли інформаційна інфраструктура стає однією з головних цілей противника [1].

Еволюція віддаленого адміністрування від Telnet у 1960–1970-х роках до SSH у 1990-х відображає перехід від незахищених протоколів до комплексних механізмів шифрування та автентифікації. Подальший розвиток VPN, RAS та широкосмугового доступу на початку XXI ст. зробив віддалене управління масовим, але й відкрив нові вектори атак. Сьогодні актуальними є багатофакторна автентифікація, захист від MITM, управління ключами та моніторинг доступу [2].

Віддалений доступ нині розглядається як критичний елемент кібербезпеки, що потребує використання сучасних криптографічних технологій, політик управління та міжнародних стандартів [3].

Метою статті є аналіз методів організації безпечного віддаленого адміністрування в інфраструктурі електронних комунікацій та визначення перспектив розвитку захисних механізмів проти сучасних кіберзагроз.

Основний текст.

Віддалений доступ дозволяє користувачам і адміністраторам підключатися до систем, серверів чи мережевих пристроїв без фізичної присутності, забезпечуючи моніторинг, конфігурацію та управління ресурсами в реальному часі. Його класифікують за способом підключення (прямий, через VPN), рівнем доступу (користувацький, адміністративний) та ступенем захисту (незахищений — Telnet, захищений — SSH, TLS, IPsec).

Серед основних технологій віддаленого адміністрування — RAS, VPN, RDP, VNC та SSH. Останній став стандартом безпечного адміністрування завдяки комплексному захисту (шифрування, автентифікація, контроль цілісності), гнучким можливостям автоматизації та підтримці сучасних алгоритмів (Ed25519, ChaCha20-Poly1305, Zero Trust).

Порівняння протоколів свідчить: SSH найбільш безпечний, але вимагає знань командного рядка; RDP зручний у графічному режимі, проте менш захищений; VNC і Telnet доцільні лише у специфічних умовах. Вибір

інструменту має враховувати баланс між безпекою, зручністю та технічними вимогами середовища [4].

SSH є основним протоколом безпечного віддаленого доступу, проте залишається вразливим без належної конфігурації. Основні загрози: MITM-атаки при неправильній перевірці ключів, використання застарілих алгоритмів, підбір паролів і ключів, компрометація облікових записів, експлуатація інших відкритих сервісів (RDP, VNC, Telnet), а також людський фактор (фішинг, соціальна інженерія). Зменшити ризики дозволяють сучасні алгоритми (AES, ChaCha20), ключова автентифікація, MFA та обмеження доступу.

Захист забезпечується комплексом криптографічних засобів: SSH, TLS, IPsec, WireGuard; симетричним та асиметричним шифруванням; хеш-функціями й HMAC для контролю цілісності; PKI та ротацією ключів. Ефективна аутентифікація включає паролі (з обмеженнями), пари ключів (RSA, Ed25519), багатофакторні методи, розмежування прав за принципом найменших привілеїв і Zero Trust-підхід.

До практичних інструментів належать: безпечна конфігурація SSH (ключі, MFA), VPN для шифрування трафіку, bastion/jump-host сервери, моніторинг і аудит (Syslog, SIEM), захист від brute-force (Fail2Ban). Вони формують базу для стійкого та контрольованого адміністрування.

Серед сучасних тенденцій — біометрична автентифікація, апаратні ключі (YubiKey, FIDO2), інтеграція з IAM/PAM для централізованого управління правами та DevSecOps-підходи для автоматизації безпеки. Це сприяє зменшенню впливу людського фактора та підвищує надійність інфраструктури.

Нарешті, автоматизація та оркестрація безпеки (DevSecOps) відкриває можливості для постійного моніторингу, автоматичного виявлення загроз та швидкого реагування на інциденти, інтегруючи безпеку безпосередньо в процеси розробки та експлуатації систем.

Перспективні технології, такі як біометрична автентифікація, апаратні ключі, інтеграція з IAM/PAM та автоматизація безпеки, дозволяють створювати комплексні, стійкі до атак системи віддаленого адміністрування, здатні

ефективно захищати критичні ресурси в умовах постійно зростаючих кіберзагроз.

Висновки.

У дослідженні виокремлено ключові аспекти безпеки віддаленого адміністрування: застосування сучасних криптографічних протоколів (SSH, TLS, IPsec), багатофакторної автентифікації та принципу найменших привілеїв. Практичні заходи включають безпечну конфігурацію SSH, використання VPN і jump-host серверів, моніторинг та захист від brute-force атак.

Перспективи розвитку пов'язані з упровадженням біометрії, апаратних ключів (YubiKey, FIDO2), інтеграцією IAM/PAM і автоматизацією безпеки через DevSecOps. Це формує комплексні системи, стійкі до сучасних кіберзагроз.

Рекомендовано поєднувати криптографічні методи, MFA, аудит доступу та автоматизований моніторинг. Подальші дослідження варто зосередити на ефективності біометрії, інтеграції Zero Trust і використанні DevSecOps для постійного підвищення безпеки.

Література:

[1] ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: ISO, 2022.

[2] Лаврут О., Івко С.О., Пузиренко О.Г., Климович О.К. Застосування моделей оцінювання ризиків інформаційної безпеки в інформаційно-телекомунікаційних системах. ResearchGate. 2021. URL: https://www.researchgate.net/publication/355929195_Zastosuvanna_modelej_ocinuvanna_rizikiv_informacijnoi_bezpeki_v_informacijno-telekomunikacijnih_sistemah

[3] ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. Geneva: ISO, 2022.

[4] Ylonen, T., & Lonvick, C. The Secure Shell (SSH) Protocol Architecture. RFC 4251. IETF, 2006. URL: https://www.rfc-editor.org/rfc/rfc4251

[5] ISO/IEC 27033-1:2015. Network security — Part 1: Overview and concepts. Geneva: ISO, 2015.

[6] ISO/IEC 15408-1:2009. Evaluation Criteria for Information Technology Security — Part 1: Introduction and general model (Common Criteria). Geneva: ISO, 2009.

Стаття надіслана: 19.09.2025 р.