https://www.sworldjournal.com/index.php/swj/article/view/swj33-01-065
DOI: 10.30888/2663-5712.2025-33-01-065

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 організації віддаленого адміністрування в інфраструктурі електронних комунікацій. Основна увага приділяється аналізу потенційних загроз та вразливостей, включаючи перехоплення трафіку, підбір паролів, соціальну інженерію та атаки на віддалені протоколи. Досліджено сучасні криптографічні засоби захисту, методи аутентифікації, багатофакторні механізми, управління ключами та рольові моделі контролю доступу. Окремо розглядаються практичні інструменти безпечного адміністрування, такі як конфігурація SSH, VPN, jump-host сервери, моніторинг доступу та захист від brute-force атак. Крім того, обговорюються перспективи розвитку безпечного віддаленого адміністрування, включаючи біометричну автентифікацію, апаратні ключі, інтеграцію з IAM/PAM та автоматизацію безпеки через DevSecOps. Основний внесок статті полягає у комплексному підході до аналізу та впровадження безпечного віддаленого доступу, що дозволяє підвищити захищеність інформаційних систем і зменшити ризики несанкціонованого доступу.*

Ключові слова: *віддалене адміністрування, безпека інформаційних систем, управління доступом, криптографічні протоколи, електронні комунікації, мережеві протоколи, телекомунікаційна інфраструктура.*

Вступ.

Сучасний розвиток телекомунікаційних систем і цифровізація більшості сфер діяльності зумовлюють стрімке зростання потреби у віддаленому доступі та адмініструванні мережевої інфраструктури. Це забезпечує гнучкість і зручність управління, проте водночас створює передумови для нових кіберзагроз: перехоплення даних, несанкціонований доступ, компрометація облікових записів та атакування критичних протоколів (SSH, RDP, VPN). Особливої ваги проблема набуває в умовах повномасштабної війни, коли інформаційна інфраструктура стає однією з ключових цілей противника, а

ризики кібердиверсій, кібершпигунства та деструктивних атак різко зростають [1]. Тому дослідження безпекових аспектів організації віддаленого адміністрування є вкрай актуальним для підвищення стійкості та захищеності інфраструктури електронних комунікацій.

Еволюція технологій віддаленого адміністрування тісно пов'язана з розвитком обчислювальних систем та глобальних мереж. У 1960–1970-х роках віддалене управління здійснювалося через термінальний доступ до мейнфреймів за допомогою протоколів на кшталт Telnet. Хоча вони забезпечували базові функції, відсутність шифрування робила такі системи вразливими до перехоплення інформації.

У 1980–1990-х роках із поширенням комп'ютерних мереж та Інтернету з'явилася потреба у більш захищених механізмах адміністрування. Тоді були розроблені технології Remote Access Service (RAS) та перші VPN-рішення, які дозволяли підключатися до корпоративних мереж через публічні канали зв'язку. Водночас виникла проблема аутентифікації користувачів та захисту від несанкціонованого доступу.

Справжнім проривом стало впровадження протоколу SSH (Secure Shell) у середині 1990-х років, який вперше поєднав шифрування трафіку, цілісність даних та надійну автентифікацію. Це дозволило значно підвищити рівень захисту при віддаленому адмініструванні серверів та мережевих пристроїв.

На початку XXI століття із розвитком широкосмугового доступу, мобільних технологій та хмарних сервісів віддалене управління стало повсюдним явищем. З одного боку, це відкрило нові можливості для адміністраторів і користувачів, а з іншого — створило додаткові вектори атак. Актуальними стали питання багатофакторної автентифікації (MFA), захисту від «людини посередині» (MITM), управління ключами та моніторингу доступу [2].

Сьогодні віддалений доступ в інфраструктурі електронних комунікацій є не лише інструментом адміністрування, а й критичним елементом безпеки, що потребує комплексного підходу з урахуванням новітніх криптографічних технологій, політик управління і стандартів кіберзахисту [3].

Метою даної статті є аналіз технологій, методів та принципів організації безпечного віддаленого доступу та адміністрування у мережах електронних комунікацій, оцінка їх впливу на безпеку інфраструктури та визначення перспектив розвитку захисних механізмів проти сучасних кіберзагроз.

Основний текст.

Віддалений доступ забезпечує користувачам і адміністраторам можливість підключення до інформаційних систем, серверів або мережевих пристроїв без необхідності фізичної присутності. Це дозволяє здійснювати моніторинг, конфігурацію, обслуговування та управління ресурсами в реальному часі, незалежно від географічного розташування.

Класифікацію віддаленого доступу можна здійснити за різними критеріями. За способом підключення він поділяється на прямий (через інтернет або локальну мережу) та опосередкований (через VPN або інші захищені шлюзи). За рівнем доступу виділяють користувацький (робота з окремими сервісами чи застосунками) та адміністративний (повний контроль над системою). За ступенем захисту розрізняють незахищений (наприклад, Telnet) та захищений (SSH, TLS, IPsec) віддалений доступ.

Віддалений доступ є критично важливим елементом сучасних систем електронних комунікацій, оскільки він забезпечує безперервність функціонування інфраструктури, швидке реагування на інциденти та зручність адміністрування розподілених мереж.

Віддалене адміністрування реалізується за допомогою різних технологій, які відрізняються рівнем захисту, зручністю та сферою застосування. До традиційних підходів належать сервіси та протоколи віддаленого підключення (RAS), віртуальні приватні мережі (VPN), а також системи графічного доступу на кшталт RDP та VNC. Вони дозволяють організувати як тунелювання мережевого трафіку, так і безпосереднє керування віддаленими станціями.

Сучасна практика адміністрування все частіше спирається на SSH (Secure Shell) як базовий інструмент безпечного доступу. Це пояснюється його комплексним підходом до захисту: протокол забезпечує конфіденційність даних

через шифрування, автентифікацію користувачів за паролями чи криптографічними ключами, а також контроль цілісності за допомогою хеш-функцій. На відміну від VPN, який переважно працює на мережевому рівні, або RDP, орієнтованого на графічний інтерфейс, SSH надає гнучкі можливості для адміністрування серверів, автоматизації завдань та інтеграції з багатофакторними системами автентифікації. Завдяки постійному розвитку алгоритмів і підтримці сучасних моделей безпеки (Ed25519, ChaCha20-Poly1305, Zero Trust) SSH став фактичним стандартом захищеного віддаленого адміністрування. Одним із способів оцінки ефективності різних методів і протоколів віддаленого доступу є їх порівняння (таблиця 1) [4].

Зіставлення різних методів і протоколів віддаленого доступу показує, що кожен з них має свої переваги та обмеження. SSH вирізняється високим рівнем безпеки та стабільністю при роботі з серверами, проте вимагає базових знань командного рядка. RDP забезпечує зручний графічний інтерфейс і легкість підключення, але менш безпечний при публічному доступі. Інші протоколи, такі як VNC або Telnet, можуть застосовуватися в специфічних умовах, враховуючи вимоги до швидкості, сумісності та захисту даних. Таким чином, вибір конкретного методу або протоколу повинен базуватися на пріоритетах безпеки, зручності та технічних особливостях середовища користувача.

Вибір SSH як основного протоколу віддаленого доступу обумовлений його високим рівнем безпеки, проте навіть цей метод не є повністю захищеним від потенційних загроз. Ключові загрози віддаленого доступу включають [5]:

- перехоплення трафіку (MITM-атаки): незважаючи на шифрування, атаки "людина посередині" можуть виникати при неправильній перевірці ключів сервера. Тому важливо контролювати аутентичні ключі та уникати підключень до невідомих серверів;

- використання слабких алгоритмів шифрування: старі версії SSH або застарілі алгоритми (наприклад, DES, RC4) можуть бути вразливими. Використання сучасних алгоритмів шифрування (AES, ChaCha20) значно знижує цей ризик;

Таблиця 1 - Порівняння методів і протоколів віддаленого доступу

Метод / Протокол	Призначення	Переваги	Недоліки	Безпека
SSH (Secure Shell)	Віддалене управління серверами (Linux, Unix)	Надійне шифрування, командний доступ, автоматизація, тунелювання	Потребує знань командного рядка, складніший для початківців	Ключі SSH, паролі, обмеження за IP, підтримка MFA
RDP (Remote Desktop Protocol)	Віддалений доступ до Windows	Графічний інтерфейс, зручність для адміністраторів і користувачів	Уразливий без додаткового захисту, високі вимоги до пропускної здатності	Використання через VPN, двофакторна автентифікація
VNC (Virtual Network Computing)	Графічний віддалений доступ	Кросплатформеність, простота використання	Менш захищений за замовчуванням, обмежений функціонал	Шифрування, використання через VPN
TeamViewer / AnyDesk	Віддалене керування ПК через інтернет	Простота використання, кросплатформеність, мобільність	Залежність від стороннього сервісу, можливі обмеження безкоштовних версій	Паролі, двофакторна автентифікація, контроль доступу
VPN	Безпечне підключення до корпоративної мережі	Шифрування всього трафіку, доступ до внутрішніх ресурсів мережі	Потребує налаштування, може знижувати швидкість доступу	Протоколи IPSec, OpenVPN, WireGuard, логування
FTP / SFTP	Передача файлів на сервер	Простота використання, підтримка більшості клієнтів	FTP без шифрування небезпечний, не рекомендується	SFTP шифрує дані, автентифікація ключами, контроль доступу
Хмарні сервіси	Зберігання та обмін файлами	Доступ з будь-якого пристрою, автоматичне резервування	Залежність від провайдера, ризик витоку даних через сторонні системи	HTTPS, двофакторна автентифікація, розмежування прав доступу
Web-доступ	Керування через веб-інтерфейси або панелі	Простий доступ через браузер, інтуїтивний інтерфейс	Обмежений функціонал порівняно з повним віддаленим доступом	HTTPS, логін/пароль, багатофакторна автентифікація

Авторська розробка

- підбір/викрадення паролів та ключів: SSH аутентифікація на основі пароля може піддаватися атакам брутфорс або словниковим підбором. Використання ключів SSH і двофакторної аутентифікації мінімізує цю загрозу;

- несанкціоноване використання облікових записів: компрометація облікового запису користувача дає доступ до сервера. Рекомендовано застосовувати політики складних паролів, обмежувати доступ за IP;

- атаки на віддалені протоколи (RDP, VNC, Telnet): навіть якщо SSH є основним протоколом, інші відкриті сервіси можуть стати точкою входу для зловмисників. Необхідно обмежувати або вимикати небезпечні протоколи на сервері;

- людський фактор (фішинг, соціальна інженерія): користувачі можуть випадково передати доступи стороннім особам. Навчання персоналу та впровадження політик безпечного використання SSH зменшує ймовірність таких інцидентів.

SSH може забезпечити високий рівень захисту від більшості загроз віддаленого доступу, проте без належної конфігурації, регулярного оновлення та дотримання правил безпеки залишаються потенційні вразливості.

Для забезпечення безпечного віддаленого доступу використовуються різноманітні криптографічні методи та протоколи [6]:

- протоколи шифрування (SSH, TLS, IPsec, WireGuard): SSH застосовується для захищеного доступу до серверів, забезпечуючи шифрування каналу передачі даних. TLS захищає веб-з'єднання, IPsec — мережевий трафік на рівні IP, а WireGuard пропонує сучасне VPN-рішення з високою швидкістю та надійним шифруванням.

- використання симетричних і асиметричних алгоритмів: Симетричне шифрування (AES, ChaCha20) дозволяє швидко захищати великі обсяги даних, тоді як асиметричне шифрування (RSA, ECC) використовується для аутентифікації та обміну ключами між сторонами. Комбінація цих методів забезпечує баланс між безпекою та продуктивністю.

- хеш-функції та HMAC для забезпечення цілісності: Хеш-функції (SHA-2,

SHA-3) гарантують, що дані не були змінені під час передачі. HMAC додає до цього криптографічний ключ, що дозволяє перевірити автентичність повідомлення та запобігти підробці.

- керування ключами (PKI, сертифікати, ротація ключів): Ефективне управління ключами забезпечує безпечну аутентифікацію та шифрування. PKI і цифрові сертифікати підтверджують достовірність користувачів і серверів, а регулярна ротація ключів мінімізує ризики їх компрометації.

Використання комплексного набору криптографічних засобів дозволяє не лише захистити віддалений доступ від перехоплення та підробки даних, але й підтримувати високий рівень довіри між користувачами та серверами.

Безпечний віддалений доступ неможливий без ефективної аутентифікації користувачів та контролю їхніх прав. Основні підходи включають [7]:

- Парольна автентифікація та її недоліки: Використання паролів є простим методом доступу, проте він вразливий до підбору, фішингу та повторного використання паролів. Складні, унікальні паролі та політики їх регулярної зміни знижують ці ризики, але повністю не усувають.

- Ключова автентифікація (RSA, Ed25519): Аутентифікація за допомогою пари ключів забезпечує надійний захист, оскільки приватний ключ зберігається на користувацькому пристрої, а сервер перевіряє відповідність відкритого ключа. Особливо ефективно в SSH-підключеннях [8].

- Багатофакторна автентифікація (MFA, TOTP, U2F): Використання декількох факторів — пароля, одноразового коду або апаратного токена — значно підвищує безпеку, ускладнюючи компрометацію облікового запису зловмисником.

- Розмежування прав доступу (рольова модель, принцип найменших привілеїв): Надання користувачам лише тих прав, які необхідні для їхніх задач, мінімізує ризики несанкціонованих дій і обмежує наслідки можливих атак.

- Zero Trust Architecture як підхід до безпеки: Модель «нульової довіри» передбачає постійну перевірку всіх користувачів і пристроїв, незалежно від їхньої позиції в мережі, що забезпечує додатковий рівень контролю доступу та

захисту від внутрішніх загроз.

Поєднання сучасних методів аутентифікації та принципів розмежування прав доступу дозволяє значно підвищити безпеку віддаленого доступу, мінімізуючи ризики компрометації облікових записів і несанкціонованого доступу до ресурсів.

Для забезпечення безпечного віддаленого доступу необхідно застосовувати конкретні інструменти та методи адміністрування:

- Конфігурація SSH (алгоритми, доступ лише по ключах, MFA): Вибір сучасних алгоритмів шифрування, заборона аутентифікації за паролем та впровадження багатофакторної автентифікації забезпечують високий рівень захисту від перехоплення та несанкціонованого доступу.

- VPN для безпечного віддаленого з'єднання: Створення захищеного каналу через VPN дозволяє шифрувати весь трафік між користувачем і сервером, обмежуючи можливості атак на мережевому рівні.

- Використання jump-host / bastion server: Проміжний сервер дозволяє централізовано контролювати доступ до внутрішніх ресурсів і зменшувати прямі підключення до критичних серверів.

- Моніторинг та аудит доступу (Syslog, SIEM): Логи підключень та події безпеки повинні постійно відслідковуватися та аналізуватися для своєчасного виявлення аномальної активності та потенційних загроз.

- Захист від brute-force (Fail2Ban, обмеження спроб входу): Автоматичне блокування IP-адрес після кількох невдалих спроб входу та встановлення обмежень на частоту підключень значно знижує ризик компрометації облікових записів.

Поєднання правильної конфігурації SSH, використання VPN, проміжних серверів, систем моніторингу та механізмів захисту від brute-force дозволяє ефективно знизити ризики та забезпечити надійний віддалений доступ до критичних ресурсів.

Сучасні тенденції розвитку віддаленого адміністрування орієнтовані на підвищення рівня безпеки та зменшення впливу людського фактора. Одним із

перспективних напрямів є використання біометричної автентифікації, що дозволяє забезпечити ідентифікацію користувача за фізіологічними ознаками, такими як відбитки пальців або розпізнавання обличчя, з мінімальною ймовірністю підробки.

Апаратні ключі (наприклад, YubiKey, FIDO2) пропонують надійний спосіб двофакторної автентифікації, забезпечуючи захист приватних ключів від компрометації та підвищуючи стійкість системи до фішингових атак.

Інтеграція віддаленого адміністрування із системами керування ідентифікацією та доступом (IAM, PAM) дозволяє централізовано контролювати права користувачів, впроваджувати політики мінімальних привілеїв та проводити аудит активності, що значно підвищує рівень контролю та безпеки.

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 процесі дослідження віддаленого адміністрування було виділено ключові аспекти забезпечення безпеки. По-перше, застосування сучасних криптографічних протоколів (SSH, TLS, IPsec) та ефективних алгоритмів шифрування дозволяє захистити дані від перехоплення і забезпечити їх цілісність. По-друге, належна організація аутентифікації та контролю доступу, включно з ключовою та багатофакторною автентифікацією, розмежуванням прав доступу та принципом найменших привілеїв, значно знижує ризик несанкціонованого доступу.

Практичні заходи, такі як правильна конфігурація SSH, використання VPN,

jump-host серверів, систем моніторингу та захист від brute-force атак, дозволяють ефективно адмініструвати серверні ресурси та зменшувати ймовірність компрометації систем.

Перспективи розвитку безпечного віддаленого адміністрування включають використання біометричної автентифікації, апаратних ключів (YubiKey, FIDO2), інтеграцію із системами IAM та PAM, а також автоматизацію та оркестрацію безпеки через DevSecOps. Ці напрями відкривають можливості для створення комплексних систем, стійких до сучасних кіберзагроз [9].

Рекомендації: Для впровадження безпечного віддаленого доступу слід поєднувати сучасні криптографічні методи, багатофакторну автентифікацію, регулярний аудит доступу та автоматизовані інструменти моніторингу.

Напрями подальших досліджень можуть включати оцінку ефективності нових методів біометричної автентифікації, інтеграцію Zero Trust моделей у корпоративну інфраструктуру та впровадження передових рішень DevSecOps для забезпечення постійної безпеки віддалених систем [10].

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. Ylonen, T., & Lonvick, C. The Secure Shell (SSH) Authentication Protocol. RFC 4252. IETF, 2006. URL: https://www.rfc-editor.org/rfc/rfc4252

6. Ylonen, T., & Lonvick, C. The Secure Shell (SSH) Transport Layer Protocol. RFC 4253. IETF, 2006. URL: https://www.rfc-editor.org/rfc/rfc4253

7. Ylonen, T., & Lonvick, C. The Secure Shell (SSH) Connection Protocol. RFC 4254. IETF, 2006. URL: https://www.rfc-editor.org/rfc/rfc4254

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

9. ISO/IEC 27033-3:2010. Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues. Geneva: ISO, 2010.

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

Abstract. *The article examines security aspects of organizing remote administration in electronic communications infrastructure. The focus is on analyzing potential threats and vulnerabilities, including traffic interception, password guessing, social engineering, and attacks on remote protocols. Modern cryptographic protection methods, authentication techniques, multi-factor mechanisms, key management, and role-based access control models are explored. Practical tools for secure administration, such as SSH configuration, VPNs, jump-host servers, access monitoring, and protection against brute-force attacks, are also discussed. Furthermore, the prospects for the development of secure remote administration are considered, including biometric authentication, hardware keys, integration with IAM/PAM systems, and security automation through DevSecOps. The main contribution of the article lies in a comprehensive approach to analyzing and implementing secure remote access, which enhances information system security and reduces the risk of unauthorized access.*

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

Стаття надіслана: 19.09.2025 р.

© Поляков О.Л., Кузьмін А.В., Івко С.О.