МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІЖНАРОДНИЙ УНІВЕРСИТЕТ

МІЖНАРОДНА КОНФЕРЕНЦІЯ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

(ПТІКІ'2026)

Одеса, Україна, 16 липня 2026 р.

Матеріали конференції

ОДЕСА

2026

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІЖНАРОДНИЙ УНІВЕРСИТЕТ

МІЖНАРОДНА КОНФЕРЕНЦІЯ

«Передові технології в інформаційно-комунікаційній інженерії»

(ПТІКІ'2026)

Одеса, Україна, 16 липня 2026 р.

Матеріали конференції

Одеса

2026

УДК 004.9
ББК 32

Проведення заходу зареєстровано в Державній науковій установі «Український інститут науково-технічної експертизи та інформації» (Реєстраційний номер: 3326U000765 від 01-07-2026 р.).

Рецензенти:
Надія КАЗАКОВА – д.т.н., професор, завідувач кафедри інформаційних технологій Одеського національного університету ім. І.І. Мечнікова
Віктор СТРЕЛЬБИЦЬКИЙ – к.т.н., доцент, доцент кафедри підйомно-транспортні машини та інжиніринг портового технологічного обладнання Одеського національного морського університету

International Conference "Advanced Technology in Information and Communication Engineering" (ATICE'2026): Conference Proceedings. Odesa: International university, 2026, 145 p**.**
DOI: https://doi.org/10.32837/11300.33747

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2026): Матеріали конференції. Одеса: Міжнародний університет, 2026, 145 с.

У збірнику подано результати наукових досліджень, висвітлено обговорення актуальних проблем, викликів і тенденцій з інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами у різних галузях народного господарства. Матеріали охоплюють інноваційні підходи, досвід упровадження сучасних рішень і приклади успішних практик трансформації різних галузях народного господарства .

Видання призначене для науково-педагогічних працівників, здобувачів освіти, науковців і фахівців ІТ галузі.

Відповідальні за випуск:
к.т.н., доцент Пунченко Наталія,
к.т.н., доцент Розенвассер Денис.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова

КІВАЛОВ С.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.

Співголови

ГРОМОВЕНКО К.В. – д.ю.н., проф., Міжнародний університет, м. Одеса, Україна.
ЛЕФТЕРОВ В.О. – д.п.н., проф., Міжнародний університет, Одеса, Україна
СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, Одеса, Україна.
УРИВСЬКИЙ Л.О. – д.т.н., проф., НТУ України "КПІ імені Ігоря Сікорського", Київ, Україна.

Члени організаційного комітету

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ЙОНА Л.Г. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
РУСУ О.П. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
РОЗЕНВАССЕР Д.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ВАКАРЧУК А.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ПУНЧЕНКО Н.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ГРІБОВА В.В. – к.ф.-м.н., доц., Міжнародний університет, Одеса, Україна.

РЕДАКЦІЙНИЙ КОМІТЕТ

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
РОЗЕНВАССЕР Д.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ПУНЧЕНКО Н.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.

КОМІТЕТ МІЖНАРОДНИХ ЗВ'ЯЗКІВ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
ГЛОБА Л. С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ВЧЕНИЙ СЕКРЕТАР

ПУНЧЕНКО Н.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.

ТЕХНІЧНО-ПРОГРАМНИЙ КОМІТЕТ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.
ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ЗМІСТ

УДК 004.056

DOI: https://doi.org/10.32837/11300.33764

ДОСЛІДЖЕННЯ СУЧАСНОГО СТАНУ ТА ПЕРСПЕКТИВ РОЗВИТКУ ПРОТОКОЛУ SSH

Петков Євген Ігорович.
Аспірант, спеціальність 125
"Кібербезпека та захист інформації",
Міжнародний університет
yepetkov@gmail.com
Науковий керівник,
Йона Лариса Григорівна, к.т.н.,
Завідувач, доцент кафедри Комп'ютерної інженерії та інноваційних технологій
Факультету Кібербезпеки, програмної інженерії та комп'ютерних наук
Міжнародного університету
yonalarisa66@gmail.com

Анотація. *У дослідженні проаналізовано принцип функціонування протоколу SSH, сучасні криптографічні методи захисту інформації, що лежать в його основі, а також перспективи подальшого розвитку цього протоколу.*

Протокол SSH (Secure Shell) використовується для створення захищеного з'єднання між клієнтом і сервером через ненадійний (незахищений) канал зв'язку з метою виконання команд, керування мережевими пристроями та передачі файлів. Він забезпечує шифрування всіх даних, що передаються між SSH-клієнтом та SSH-сервером, гарантуючи конфіденційність, цілісність інформації та автентифікацію під час віддаленого доступу й обміну файлами.

Протокол SSH був створений Тату Ілоненом в 1995 році в Гельсінському технологічному університеті після атак на мережу університету, які показали незахищеність протоколів на кшталт Telnet або Rlogin. Перша версія SSH-1 швидко поширилася завдяки підтримці шифрованого віддаленого доступу, але через виявлені деякі архітектурні проблеми та вразливості з часом її замінив SSH-2, який отримав покращені механізми шифрування, обміну ключами та автентифікації й став сучасним стандартом SSH.

Найбільш розповсюдженим є використання протоколу SSH:

- для віддаленого підключення до серверів та передачі команд для керування системою;
- для захищеної передачі файлів за допомогою протоколів SCP (Secure File Copy), або SFTP (SSH File Transfer Protocol).

Протокол SSH забезпечує безпеку завдяки трьом основним рівням: транспортному, рівню автентифікації користувача та рівню з'єднання. Кожен із

них виконує окремі функції, які спільно формують захищений канал зв’язку між клієнтом і сервером.

Етапи встановлення SSH з’єднання зображено на рис.1

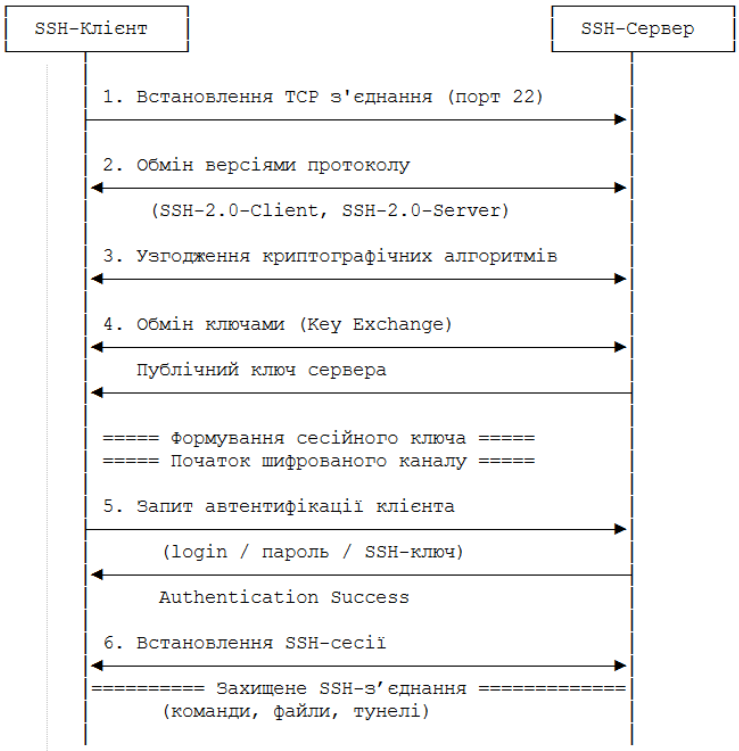

Рисунок 1 – Етапи встановлення SSH з’єднання

SSH-клієнт ініціює процес встановлення TCP-з'єднання до сервера (як правило по порту 22, але це може бути і нестандартний порт).

Далі клієнт і сервер надсилають один одному інформацію про версію SSH-протоколу (наприклад, SSH-2.0-OpenSSH). Цей етап дозволяє визначити, яку версію SSH підтримують обидві сторони та перевірити сумісність клієнта та сервера.

Після цього клієнт і сервер погоджують криптографічні алгоритми, які будуть використовуватися для захисту з’єднання: методи шифрування, алгоритми обміну ключами та механізми перевірки цілісності повідомлень. На цьому етапі сторони обирають спільно підтримувані та найбільш безпечні алгоритми. У сучасних реалізаціях SSH зазвичай застосовуються алгоритми шифрування AES, а також протоколи обміну ключами Diffie–Hellman (DH) або Elliptic Curve Diffie–Hellman (ECDH).

На наступному етапі сервер надсилає клієнту свій відкритий ключ (наприклад, RSA, DSA або інший узгоджений алгоритм). Клієнт перевіряє справжність сервера та достовірність отриманого ключа. Після підтвердження довіри клієнт і сервер за допомогою алгоритму Диффі–Хеллмана (або його

сучасних реалізацій) спільно формують сеансовий ключ, який надалі використовується для симетричного шифрування SSH-з'єднання. Після цього з'єднання вже шифрується.

На стадії автентифікації клієнт може підтвердити свою особу перед сервером декількома способами:

- Автентифікація за паролем – це найпростіший спосіб входу, що використовує ім'я користувача та пароль. Однак цей метод є менш безпечним через вразливість до підбору паролів і викрадення облікових даних.
- Автентифікація за допомогою ключів є безпечнішим методом, ніж парольна, оскільки використовує пару асиметричних ключів: приватний та публічний, які математично пов'язані друг з другом. Приватний ключ є секретним та зберігається локально тільки у SSH-клієнта. Публічний ключ є відкритим та розміщується на сервері для автентифікації цього клієнта. Їх криптографічний зв'язок дає змогу підтвердити особу користувача без передачі приватного ключа мережею, що значно зменшує ризик компрометації облікових даних. Розповсюджені тут асиметричні алгоритми: RSA, ECDSA, Ed25519, з яких Ed25519 - найсучасніший та найбезпечніший.
- Багатофакторна аутентифікація передбачає використання кількох способів підтвердження особи, наприклад SSH-ключа та одноразового пароля на основі часу. Такий підхід забезпечує підвищений рівень захисту для критично важливих систем.

Після успішної автентифікації між клієнтом і сервером створюється логічний канал, через який можна запускати shell-сесію, виконувати команди, здійснювати тунелювання портів або передавати файли за допомогою SCP чи SFTP.

Рекомендації щодо оптимального налаштування протоколу SSH:

- Використувавути інший нестандартний TCP порт (замість 22 за замовчуванням).
- Захистити доступ до SSH сервера правилами доступа на основі міжмережевого екрану.
- Використовувати автентифікацію за допомогою ключів замість автентифікації за паролем.
- Обмежити кількість невдалих спроб автентифікації (наприклад за допомогою програми «fail2ban»).

Потенційним майбутнім викликом для SSH є поява потужних квантових комп'ютерів, здатних зламати поточні алгоритми криптозахисту. Проте поточна модульна архітектура протоколу SSH дозволяє впроваджувати (додавати до

нього) нові, швидші та надійніші криптографічні алгоритми захисту в постквантовий період.

Висновки. SSH - це універсальний протокол для організації безпечного доступу до віддалених систем, передачі команд керування, а також захищеного трансферу файлів через незахищене середовище. В основі цього протоколу лежать відомі базові криптографічні алгоритми, наприклад, AES (симетричне шифрування), RSA (аутентифікація), DH (обмін ключів) та їх більш сучасні модифікації. Модульна архітектура SSH створює умови для інтеграції нових, продуктивніших і надійніших криптографічних механізмів захисту в умовах постквантових загроз.

Література

1. АНАЛІЗ ПОТОЧНОГО СТАНУ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ. Є. І. Петков. URL: https://doi.org/10.36059/978-966-397-479-8-130.
   SSH, The Secure Shell: The Definitive Guide. Daniel J. Barrett, Richard Silverman. URL: https://theswissbay.ch/pdf/Gentoomen%20Library/Operating%20Systems/Linux/SSH%20%26%20VPN/O%27Reilly%20-%20SSH%20The%20Secure%20Shell%20The%20Definitive%20Guide.pdf.
2. SSH (Secure Shell): Complete Guide to Secure Remote Access. URL: https://prehost.com/what-is-ssh/.
3. Wikipedia. Transport Layer Security. URL: https://en.wikipedia.org/wiki/Transport_Layer_Security.
4. SSH Protocol – Secure Remote Login and File Transfer. URL: https://www.ssh.com.
5. AWS: What is Secure File Transfer Protocol (SFTP)? URL: https://aws.amazon.com/what-is/sftp/.