Секція 1

СПОСОБИ ТА МЕТОДИ ЗАХИСТУ ПЕРЕДАЧІ ДАНИХ В ГЛОБАЛЬНІЙ МЕРЕЖІ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ДАНИХ

Положий А. С.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Бабешко Є. В.

Актуальність. З розвитком цифрових технологій, передача даних у мережі стала невід'ємною частиною сучасного суспільства. Швидкий обмін інформацією, який підтримують інтернет-сервіси, мобільні додатки та хмарні технології, значно спрощує комунікацію та роботу бізнесу. Однак зростання обсягу переданих даних супроводжується підвищенням ризиків витоку, перехоплення та модифікації інформації зловмисниками. За даними Cisco, у 2022 році 41% кібератак були націлені на перехоплення конфіденційних даних під час їх передачі [1]. Це підкреслює актуальність дослідження методів захисту даних у мережах.

Метою даної роботи є аналіз способів та методів захисту передачі даних у мережі, вивчення їх переваг і недоліків, а також виявлення найбільш ефективних практик у сучасних умовах.

Основні положення. Захист передавання даних у мережі забезпечується комплексом технологій та методів, спрямованих на запобігання втрати, викривленню чи несанкціонованому доступу до інформації. Одним із ключових способів є шифрування, яке гарантує конфіденційність даних навіть у разі їх перехоплення. Використання сучасних протоколів, таких як TLS або IPsec, дозволяє зберігати цілісність і захист трафіку в мережі [2].

Аутентифікація та авторизація є важливими компонентами захисту, забезпечуючи перевірку користувача перед доступом до системи або даних. Це доповнюється брандмауерами, які обмежують небажаний трафік, і системами виявлення загроз, що аналізують підозрілу активність.

Цифрові сертифікати забезпечують надійність зв’язків між користувачами та системами, а резервне копіювання є необхідним для відновлення даних у разі кібератак.

Моніторинг і аналіз трафіку дозволяють виявляти аномалії в мережі, забезпечуючи швидке реагування на можливі загрози. Інструменти моніторингу, такі як SIEM-системи, допомагають збирати, аналізувати та

відображати дані про мережеву активність, що сприяє надійному захисту мережі [3].

Висновки. Сучасні способи захисту передачі даних забезпечують багаторівневу безпеку інформації. Найефективнішим підходом є комбінування методів шифрування, автентифікації та використання інструментів моніторингу трафіку. Проте, навіть найкращі технології не гарантують абсолютного захисту без належного адміністрування та дотримання політик безпеки. Зростаюча складність атак вимагає постійного вдосконалення методів захисту, особливо у контексті розвитку квантових обчислень та технологій. Подальшим напрямком дослідження є вивчення нових методів шифрування для забезпечення захисту даних в умовах майбутнього розвитку квантових обчислень, а також дослідження нових інструментів автоматизації та вдосконалення моніторингу мережевого трафіку.

Список літератури

1. Cisco Annual Internet Report. *Cisco*. URL – https://www.cisco.com/c/dam/en_us/about/annual-report/cisco-annual-report-2022.pdf (дата звернення: 10.11.2024).
2. В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. Технології забезпечення безпеки мережевої інфраструктури. Київський університет імені Бориса Грінченка. – Київ, 2019. – 218 с.
3. А. В. Жилін, О. М. Шаповал, О. А. Успенський. Технології захисту інформації в інформаційно-телекомунікаційних системах. ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ, 2020. – 213 с.

Відомості про авторів

Положий Антон Сергійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.s.polozhyy@student.csn.khai.edu
Бабешко Євген Васильович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., доцент, e.babeshko@csn.khai.edu