3. Strelkovskaya I., Zolotukhin R. Research of low-bandwidth radionetworks QoS parameters // Information and Telecommunication Sciences, International Research Journal, Volume 11, Number 1(20), January-June 2020, DOI: https://doi.org/10.20535/2411-2976.12020.77-81.

4. Strelkovskaya I.V., Zolotukhin R.V. « Simulation modeling algorithm of low-bandwidth radio network of automated control systems» / Springer Science + Business Media, 2025 (до друку).

DOI https://doi.org/10.36059/978-966-397-491-0-40

ЗБЕРЕЖЕННЯ КОНФІДЕНЦІЙНОСТІ ШЛЯХОМ МАСКУВАННЯ ПЕРЕДАЧІ ІНФОРМАЦІЇ

Тріль Д. Д.
здобувач
Міжнародний гуманітарний університет
м. Одеса, Україна

Збереження конфіденційності інформації набуває дедалі більшої значущості в умовах сучасного цифрового світу, де технологічний прогрес рухається стрімкими темпами. Цей розвиток супроводжується зростаючою кількістю загроз, включаючи витоки даних, кібернапади та незаконні способи збору персональної інформації. Враховуючи, що сьогодні майже кожна людина активно використовує інтернет у різних сферах життя – для спілкування, професійної діяльності, здійснення фінансових операцій – питання цифрової безпеки та захисту конфіденційності стає надзвичайно актуальним для широкого загалу [1].

Одним із дієвих способів зменшення ризиків втрати конфіденційності є використання технологій маскування передачі даних. Цей підхід дає змогу приховати як сам факт передачі інформації, так і її зміст, забезпечуючи захист від можливих спроб несанкціонованого доступу з боку зловмисників. У нинішніх реаліях, коли державні організації, великі корпорації та кіберзлочинці активно аналізують численні цифрові сліди, такі методи виступають важливим інструментом для збереження персональної безпеки.

Особливе значення маскування передачі даних має для тих, чия діяльність нерідко супроводжується ризиками витоку інформації чи її неправомірного використання. Це журналісти, котрі шукають правду у чутливих темах, правозахисники, що борються за свободу та права людини, підприємці, які прагнуть захистити інтелектуальну власність, а також

звичайні користувачі, що цінують приватність своїх онлайн-дій. Однак існує проблема нестачі знань про принципи функціонування цих технологій серед широкої аудиторії. Необізнаність щодо ефективних методів маскування нерідко ускладнює процес їхнього впровадження на практиці, знижуючи рівень загального захисту інформації [1].

Збереження конфіденційності під час передачі інформації шляхом її маскування є багатогранною і пропонує ряд викликів, які потребують уважного розгляду. Перш за все, сучасні технології спостереження та аналізу трафіку дозволяють відстежувати навіть зашифровану інформацію під час її передавання. Це свідчить про те, що звичайне шифрування далеко не завжди забезпечує повноцінний захист, оскільки може бути виявлено сам факт обміну даними, що вже наражає користувачів на певний ризик. У подібних випадках методи аналізу метаданих можуть надати значну кількість інформації про характер зв'язку, навіть якщо самі дані залишаються зашифрованими.

Другою важливою складовою цієї проблеми є низька обізнаність користувачів щодо необхідності захищати власну інформацію. Багато хто недостатньо усвідомлює серйозність питання конфіденційності та уникає використання ефективних інструментів маскування через брак знань або недовіру до технологічних рішень. Це породжує ґрунт для вразливості, якою можуть скористатися зловмисники. Водночас обмеження, накладені на використання певних технічних засобів державами чи великими корпораціями, ще більше ускладнюють ситуацію [1].

У бізнес-середовищі це питання стає ще гострішим через загрози промислового шпигунства, які можуть призвести до витоку важливих комерційних даних. Втрата такої інформації нерідко тягне за собою значні фінансові втрати, а інколи – навіть втрату конкурентних переваг на ринку. Так само і в повсякденному житті витік особистих даних несе ризики, серед яких фінансові шахрайства, викрадення ідентичності чи навіть використання конфіденційної інформації для шантажу. Усвідомлення цих загроз є першим кроком до пошуку ефективних рішень і вироблення стратегій захисту інформації у сучасному цифровому світі.

Рішення проблеми конфіденційності через маскування передачі інформації можливе завдяки застосуванню передових технологій і підвищенню обізнаності користувачів. Одним із ключових підходів є використання стеганографії, яка дозволяє приховувати повідомлення в інших цифрових носіях, таких як зображення чи аудіофайли. Це робить передачу даних менш помітною, адже файли виглядають як звичайні. Популярним рішенням також є використання анонімних мереж, що забезпечують передачу інформації із приховуванням місцезнаходження відправника та отримувача [2].

VPN та проксі-сервери слугують дієвими інструментами для шифрування трафіку та приховання реальної IP-адреси користувача. Проте важливо обирати надійні сервіси, оскільки деякі з них можуть зберігати журнали активності, що створює ризики для конфіденційності. Використання шифрування кінцевої точки, яке реалізоване в месенджерах типу Signal або у секретних чатах Telegram, допомагає гарантувати, що передані дані залишаються недоступними для сторонніх осіб.

У контексті бізнесу та корпоративного середовища важливим є впровадження комплексних заходів безпеки. Це включає регулярне навчання працівників, багаторівневу аутентифікацію та застосування криптографічних рішень для захисту внутрішньої комунікації. Водночас необхідно врахувати можливі законодавчі обмеження щодо технологій маскування. Відстежування змін у нормативній базі та адаптація захисних стратегій до актуальних умов залишаються важливими складовими ефективного забезпечення конфіденційності.

Одним із ключових аспектів забезпечення конфіденційності є використання програмного забезпечення з відкритим кодом. Ці проєкти дозволяють користувачам перевіряти вихідний код на предмет вразливостей чи прихованих функцій, які можуть становити загрозу безпеці. Завдяки відкритому коду спільнота розробників може регулярно перевіряти та вдосконалювати механізми безпеки, роблячи такі системи більш надійними. Це особливо важливо для організацій, які прагнуть мати повний контроль над своїми цифровими активами [2].

Інший спосіб підвищення захисту – впровадження двофакторної або багатофакторної аутентифікації. Додаткові рівні захисту у формі одноразових паролів, біометричних даних чи апаратних ключів значно ускладнюють несанкціонований доступ до облікових записів. Такі рішення допомагають значно знизити ризики, пов’язані з крадіжками паролів або фішинг-атаками. Крім цього, регулярна зміна паролів і застосування менеджерів для їх зберігання сприяють кращому управлінню конфіденційною інформацією. Сучасні технології дозволяють генерувати складні паролі та автоматично заповнювати їх у відповідних полях, одночасно полегшуючи користування й забезпечуючи високий рівень безпеки.

Отже, збереження конфіденційності через захист передачі інформації є наріжним каменем у сучасному цифровому світі. Загрози витоку даних, кіберзлочинів та стеження вимагають від нас впровадження дієвих заходів захисту. Технології, такі як стеганографія, анонімні мережі, VPN, шифрування та корпоративні стратегії безпеки, значно знижують ризики несанкціонованого доступу до інформації. Однак для повного вирішення проблеми потрібно поєднувати технологічні інструменти з підвищенням рівня обізнаності користувачів про важливість захисту даних. Лише

комплексний підхід, що враховує як технічні рішення, так і освітні ініціативи, здатний забезпечити належний рівень конфіденційності в цифровому світі.

Література:

1. Як організації захищають дані? URL: https://corewin.ua/blog/how_do_organizations_protect_data/ (дата звернення: 14.03.2025).

2. Конфіденційна інформація URL: https://www.solix.com/uk/kb/sensitive-information/ (дата звернення: 14.03.2025).

DOI https://doi.org/10.36059/978-966-397-491-0-41

ЕЛЕКТРОННІ КОМУНІКАЦІЇ КРОКУЮТЬ У МАЙБУТНЄ

Уривський Л. О.
доктор технічних наук,
професор кафедри електронних комунікацій та Інтернету речей
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
м. Київ, Україна

Синергія інформаційно-комунікаційних технологій (ІКТ), які поєднують можливості електронних комунікацій і інформаційних ресурсних об'єктів, сьогодні все більше впливає на всі аспекти суспільства.

Ще в 1982 році академік В.М. Глушков передбачив майбутню революційну трансформацію існуючих обчислювальних засобів та технологій зв'язку та глобалізацію їх використання.

За словами В. М. Глушкова, «*... **злиття телекомунікацій** з машинною **інформатикою** (впроваджене в комп'ютерних мережах та комп'ютерних центрах з віддаленими терміналами) вже призвело до появи нового терміну «телематика «... не за горами день, коли звичайні книги, газети та журнали зникнуть. Натомість кожна людина матиме **«електронний» блокнот**, який є комбінацією плоского дисплея з мініатюрним радіопередавачем. Ввівши потрібний код на клавіатурі цього «блокнота», ви можете (з будь-якої точки нашої планети) **отримати будь-які** тексти, зображення (включаючи динамічні) з гігантських комп'ютерних баз даних, **підключених до мережі**, які замінять не тільки сучасні книги, журнали і газети, а й сучасні телевізори. ...*» [1].