УДК 004.056:621.39

ЗАХИСТ ВІД НЕСАНКЦІОНОВАНИХ ПІДКЛЮЧЕНЬ У МЕРЕЖАХ НОВОГО ПОКОЛІННЯ (NGN): КОМПЛЕКСНИЙ АРХІТЕКТУРНИЙ ПІДХІД

Махнюк Владислав,
здобувач першого (бакалаврського) рівня вищої освіти,
Приватного вищого навчального закладу
«Міжнародний економіко-гуманітарний університет
імені академіка Степана Дем'янчука» (м. Рівне, Україна)

Науковий керівник: Соловей Людмила,
старший викладач кафедри інформаційних систем та
обчислювальних методів,
Приватний вищий навчальний заклад
«Міжнародний економіко-гуманітарний університет імені
академіка Степана Дем'янчука» (м. Рівне, Україна)

Науковий керівник: Лотюк Юрій,
кандидат педагогічних наук, завідувач кафедри
інформаційних систем та обчислювальних методів
Приватного вищого навчального закладу
«Міжнародний економіко-гуманітарний університет імені
академіка Степана Дем'янчука» (м. Рівне, Україна)

Анотація. *У статті досліджено проблему захисту мереж нового покоління (NGN) від несанкціонованих підключень як одного з ключових чинників порушення конфіденційності, цілісності та доступності сервісів. Проаналізовано основні вектори атак на рівнях доступу, сигналізації, керування та передавання даних, зокрема SIP hijacking, SIP flooding, RTP injection і Toll Fraud. Запропоновано комплексний архітектурний підхід до кіберзахисту, що поєднує 802.1X/EAP-TLS, MACsec, SBC, SIPS/SRTP, VRF, IPsec, Zero Trust, UEBA та deception-механізми для проактивного виявлення й нейтралізації загроз.*

Ключові слова: *мережі нового покоління (NGN), несанкціоноване підключення, кіберзахист, протокол SIP, Zero Trust, UEBA, прикордонний контролер сеансів (SBC).*

Abstract. *The article examines the problem of protecting Next-Generation Networks (NGN) against unauthorized connections as a key factor affecting the confidentiality, integrity, and availability of services. The main attack vectors at the access, signaling, control, and data planes are analyzed, including SIP*

hijacking, SIP flooding, RTP injection, and Toll Fraud. A comprehensive architectural cybersecurity approach is proposed, combining 802.1X/EAP-TLS, MACsec, SBC, SIPS/SRTP, VRF, IPsec, Zero Trust, UEBA, and deception mechanisms for proactive threat detection and mitigation.

Keywords: *Next-Generation Networks (NGN), unauthorized access, cybersecurity, SIP protocol, Zero Trust, UEBA, Session Border Controller (SBC).*

Стрімкий розвиток телекомунікаційних технологій зумовив глобальний перехід від традиційних мереж з комутацією каналів (PSTN) до мереж нового покоління (Next-Generation Networks, NGN). Фундаментальною особливістю NGN є використання єдиного мультисервісного середовища на базі стека протоколів TCP/IP для передачі всіх видів трафіку: голосу (VoIP), відео, даних та управляючої інформації. Хоча така архітектура забезпечує високу масштабованість, гнучкість та економічну ефективність, вона успадковує всі вразливості, притаманні IP-мережам.

У класичних телекомунікаційних мережах безпека базувалася на фізичній ізоляції ліній зв'язку та закритих (пропрієтарних) протоколах. В архітектурі NGN периметр безпеки стає розмитим. Відкритість стандартів (SIP, H.323, MEGACO, RTP) та доступність інструментів для аналізу мережевого трафіку роблять інфраструктуру вразливою до широкого спектра кібератак. Найбільш критичною загрозою є несанкціоноване підключення до мережі, оскільки воно є першим етапом складної цілеспрямованої атаки (APT – Advanced Persistent Threat). Успішне підключення дозволяє зловмиснику закріпитися в системі, перехоплювати трафік, здійснювати крадіжку послуг (Toll Fraud), підміняти ідентифікатори користувачів (Spoofing) або реалізовувати атаки на відмову в обслуговуванні (DoS/DDoS).

Авторами проведено комплексний аналіз вразливостей архітектури NGN щодо несанкціонованого доступу та розроблена багаторівнева модель ешелонованого кіберзахисту, яка охоплює фізичний, канальний, мережевий та прикладний рівні еталонної моделі OSI.

Питання кібербезпеки мереж NGN регламентуються низкою міжнародних стандартів. Базові вимоги до архітектури безпеки визначені в рекомендаціях Міжнародного союзу електрозв'язку (ITU-T), зокрема у стандарті Y.2701 (Security requirements for NGN release 1). У специфікаціях консорціуму 3GPP (TS 33.210) деталізовано принципи мережевої доменної безпеки (Network Domain Security, NDS). Питання захисту протоколів управління сеансами активно досліджуються робочими групами IETF (Internet Engineering Task Force), що відображено у відповідних RFC (наприклад, RFC 3261 для SIP, RFC 3711 для SRTP). Однак, попри наявність стандартизованих механізмів, практична реалізація захисту часто є

фрагментарною. Сучасні дослідження вказують на необхідність переходу від реактивних методів захисту до проактивних, з використанням архітектури нульової довіри (Zero Trust Architecture) та систем поведінкового аналізу [1, с. 20].

З точки зору кіберзахисту, архітектуру NGN слід розглядати через призму трьох логічно розділених площин: площини передачі даних (Data Plane), площини сигналізації та управління сеансами (Control Plane) та площини адміністрування (Management Plane). Несанкціоноване підключення до будь-якої з цих площин має різні наслідки та вимагає різних підходів до нейтралізації [2, с. 121].

1.*Вектори атак на рівні доступу (Access Network):* Зловмисник може здійснити фізичне підключення до портів комутатора рівня доступу або логічне проникнення через вразливості бездротових сегментів (Wi-Fi/5G/LTE). Відсутність належної автентифікації на цьому етапі дозволяє реалізувати атаки типу MAC-spoofing, ARP-poisoning та впровадження несанкціонованих DHCP-серверів (Rogue DHCP) для перехоплення маршрутизації клієнтського трафіку (Man-in-the-Middle).

2.*Вектори атак на площину управління (Control Plane):* Оскільки протокол SIP (Session Initiation Protocol) функціонує на прикладному рівні та за замовчуванням передає дані у відкритому текстовому форматі, він є вразливим до несанкціонованих реєстрацій. Атака *SIP REGISTER Hijacking* передбачає підміну IP-адреси у повідомленнях реєстрації, що дозволяє зловмиснику перенаправляти вхідні виклики легітимного абонента на власне обладнання. Іншою загрозою є *SIP Flooding* – генерування великої кількості фальшивих запитів INVITE або REGISTER, що виснажує обчислювальні ресурси комутатора (Softswitch).

3.*Вектори атак на площину даних (Data Plane):* Якщо зловмиснику вдалося несанкціоновано підключитися до сегмента медіатрафіку, він може здійснювати *RTP Injection* (ін'єкцію підроблених аудіо- чи відеопакетів у поточну сесію) або пасивне прослуховування розмов (Eavesdropping).

4.*Крадіжка послуг (Toll Fraud):* Це фінансово найбільш руйнівний наслідок несанкціонованого підключення. Отримавши доступ до ресурсів мережі оператора (шляхом компрометації IP-PBX або підбору паролів до SIP-акаунтів), зловмисники ініціюють масові дзвінки на платні міжнародні напрямки [3, с. 45].

Фундаментом архітектури безпеки NGN є реалізація принципу ешелонованого захисту (Defense-in-Depth). Першим бар'єром має стати жорсткий контроль підключень на межі мережі.

Класичні методи, такі як статична прив'язка MAC-адрес (Port Security), не відповідають сучасним вимогам стійкості, оскільки MAC-адреса легко підробляється програмними засобами. Найефективнішим

рішенням для запобігання несанкціонованому доступу на фізичному та канальному рівнях є впровадження стандарту IEEE 802.1X [4, с. 2].

5.*Сертифікатна автентифікація:* 802.1X забезпечує контроль доступу на рівні порту. Пристрій (Суплікант) не отримує доступу до мережі NGN, поки не пройде процедуру автентифікації на сервері AAA (RADIUS або Diameter). Для максимального рівня захисту доцільно використовувати протокол розширеної автентифікації EAP-TLS (Extensible Authentication Protocol - Transport Layer Security). На відміну від методів, заснованих на паролях (PEAP чи EAP-TTLS), EAP-TLS вимагає наявності валідного криптографічного сертифіката X.509 як на сервері, так і на клієнтському пристрої. Це унеможливлює підключення стороннього обладнання (наприклад, ноутбука зловмисника, підключеного до Ethernet-розетки), навіть якщо він знає логін і пароль користувача.

6.*Захист від канальних атак (MACsec):* Після успішної автентифікації залишається ризик пасивного перехоплення трафіку на фізичному каналі (наприклад, через відгалуження кабелю). Для нівелювання цієї загрози пропонується використовувати стандарт IEEE 802.1AE (MACsec). Він забезпечує автентифікацію джерела даних, цілісність та шифрування (за алгоритмом AES-128 або AES-256) кожного кадру Ethernet на ділянці між клієнтським пристроєм і портом комутатора.

7.*Ізоляція трафіку:* Додатковим ешелоном є використання віртуальних локальних мереж (VLAN) у поєднанні з технологіями Private VLAN (PVLAN) та Access Control Lists (ACL). Кожен тип пристроїв (IP-телефони, медіашлюзи, комп'ютери користувачів) повинен розташовуватися в окремому ізольованому сегменті, що мінімізує можливості горизонтального переміщення (Lateral Movement) зловмисника у разі успішного компрометування одного з вузлів [5, с. 112; 6, с. 4].

Якщо рівень доступу захищає від несанкціонованого фізичного або канального підключення, то рівень площини управління має захищати інфраструктуру від атак прикладного рівня, зокрема на протоколи встановлення з'єднань (SIP, H.323). Центральним елементом безпеки на цьому рубежі є *Session Border Controller (SBC)* – прикордонний контролер сеансів.

SBC функціонує на межі між мережею оператора та зовнішніми мережами (або клієнтськими сегментами) і діє як спеціалізований міжмережевий екран прикладного рівня. Його архітектурна роль полягає у виконанні функцій B2BUA (Back-to-Back User Agent). Усі SIP-повідомлення від кінцевих пристроїв термінуються на зовнішньому інтерфейсі SBC, який після перевірки (Deep Packet Inspection для SIP) ініціює нове, очищене з'єднання до внутрішнього комутатора (Softswitch).

8.*Топологічне приховування (Topology Hiding):* SBC повністю замінює IP-адреси та заголовки внутрішньої мережі у SIP-пакетах на власні.

Це позбавляє зловмисника можливості отримати інформацію про внутрішню структуру мережі NGN та адреси критичних серверів.

9.*Захист від DoS/DDoS та SIP Flooding:* SBC обмежує швидкість надходження запитів (Rate Limiting) та аналізує їхню валідність. Аномальні сплески реєстрацій (REGISTER) або запитів на з'єднання (INVITE) автоматично відкидаються, зберігаючи ресурси ядра мережі.

10. *Криптографічний захист транзиту:* Для унеможливлення перехоплення сигналізації всі сесії мають встановлюватися з використанням SIPS (SIP over TLS). Шифрування медіатрафіку (голосу та відео) є критично важливим для запобігання RTP-ін'єкціям та реалізується через SRTP (Secure Real-time Transport Protocol). Обмін ключами для SRTP повинен здійснюватися захищеними методами, такими як DTLS-SRTP, що виключає передачу ключів у відкритому вигляді через SDES.

Навіть у випадку успішного обходу периметральних засобів захисту, зловмисник не повинен отримати можливість переміщуватися всередині мережі. Це досягається завдяки жорсткій логічній ізоляції площин на рівні транспортного ядра [7, с. 25].

11. *VRF та MPLS L3 VPN:* Інфраструктура NGN проектується з використанням віртуальних маршрутизаторів (VRF). Управлінський трафік (OAM – Operations, Administration, and Management), сигналізація та користувацькі дані (медіатрафік) ізолюються у різних VPN-доменах. Якщо зловмисник отримує несанкціонований доступ до сегмента медіашлюзу, він фізично не зможе маршрутизувати пакети до сегмента управління білінгом або софтсвічем.

12. *Захист довірчих доменів (IPsec):* Згідно зі стандартами 3GPP (Network Domain Security), обмін даними між ключовими вузлами інфраструктури (наприклад, між Media Gateway Controller та Media Gateway) повинен здійснюватися виключно через захищені IPsec-тунелі. Це гарантує конфіденційність та цілісність даних (через протокол ESP) та автентифікацію джерела на мережевому рівні.

Сучасний ландшафт кіберзагроз вимагає переходу від статичних правил безпеки до концепції *Zero Trust Network Access (ZTNA).* Парадигма нульової довіри стверджує: "ніколи не довіряй, завжди перевіряй". У контексті NGN це означає відмову від концепції "довіреної внутрішньої мережі". Кожен запит на встановлення сесії, незалежно від його походження (зсередини чи ззовні), підлягає автентифікації та перевірці політик доступу.

Оскільки зловмисники часто використовують викрадені легітимні облікові дані, традиційна автентифікація є недостатньою. На цьому етапі архітектура захисту посилюється інтелектуальними системами:

13. *User and Entity Behavior Analytics (UEBA):* Впровадження систем поведінкового аналізу на базі машинного навчання (Machine Learning). Ці системи аналізують телеметрію з SBC, серверів AAA та

комутаторів, формуючи базову лінію (baseline) нормальної активності кожного абонента та пристрою. Алгоритми здатні виявляти складні аномалії: наприклад, «неможливу подорож» (спроба реєстрації SIP-акаунта з України, а через 10 хвилин – з іншого континенту) або нетиповий сплеск тривалості викликів. Такі відхилення автоматично блокуються до з'ясування обставин.

14. *Технології Deception (SIP Honeypots):* Ефективним методом виявлення схованих загроз є розгортання пасток – фіктивних серверів усередині NGN, що імітують вразливі SIP-шлюзи. Легітимні користувачі ніколи до них не звертаються, тому будь-яка спроба сканування портів або підключення до такої пастки є індикатором компрометації мережі, що дозволяє миттєво ізолювати джерело атаки.

Забезпечення кіберстійкості мереж нового покоління (NGN) до несанкціонованих підключень є багатовимірною проблемою, яка не може бути вирішена шляхом впровадження окремих ізольованих засобів захисту. Відкрита природа протоколів та конвергенція сервісів вимагають впровадження комплексного архітектурного підходу [8, с. 50; 9, с. 12].

Запропонована ешелонована модель (Defense-in-Depth) мінімізує поверхню атак шляхом:

1) жорсткої сертифікатної автентифікації на фізичному та канальному рівнях (802.1X/EAP-TLS, MACsec);

2) захисту площини управління сеансами та топологічного приховування через прикордонні контролери (SBC) з обов'язковим шифруванням SIPS/SRTP;

3) логічної ізоляції сегментів ядра мережі (VRF/IPsec);

4) переходу до архітектури нульової довіри (ZTNA) з використанням систем поведінкового аналізу (UEBA) для проактивного виявлення аномалій. Тільки синергія цих механізмів здатна гарантувати цілісність, конфіденційність та доступність сервісів NGN в умовах постійної еволюції кіберзагроз.

ЛІТЕРАТУРА

1. Вілянський А. В., Позняк А. А. Організаційні аспекти впровадження моделі Zero Trust у корпоративному середовищі. Актуальні питання забезпечення кібербезпеки та захисту інформації : матеріали XI Міжнародної науково-практичної конференції, 24 квіт. 2025 р., Київ. Київ, 2025. С. 20–21. URL: https://files.znu.edu.ua/files/Bibliobooks/Inshi84/0063968.pdf (дата звернення: 15.03.2026).

2. Дудикевич В. Б., Микитин Г. В., Мурак Т. Є. Комплексна система безпеки регіональної корпоративної мережі на основі еталонної моделі OSI та моделі «глибокого захисту». CSN. 2025. Вип. 7, № 1. С. 119–131. DOI: 10.23939/csn2025.01.119.

3. Терейковський І. А., Гнатюк С. О. Захист інформації в комп'ютерних системах [Електронний ресурс]: навчальний посібник для здобувачів ступеня бакалавра за освітньою програмою «Системне програмування та спеціалізовані комп'ютерні системи» спеціальності 123 Комп'ютерна інженерія. Київ : КПІ ім. Ігоря Сікорського, 2022. 135 с. URL: https://ela.kpi.ua/bitstream/123456789/50138/1/ZI_in_CS.pdf (дата звернення: 15.03.2026).
4. Artioli P., Maci A., Magrì A. A comprehensive investigation of clustering algorithms for User and Entity Behavior Analytics. Frontiers in Big Data. 2024. Vol. 7. Article 1375818. DOI: 10.3389/fdata.2024.1375818.
5. Mohd Ramly A., Ng Z. W., Khamayseh Y., Kwan C. S. C., Amphawan A., Neo T.- K. Review and Enhancement of VoIP Security: Identifying Vulnerabilities and Proposing Integrated Solutions. Journal of Telecommunications and the Digital Economy. 2024. Vol. 12, no. 4. P. 109–136. DOI: 10.18080/jtde.v12n4.1022.
6. Morić Z., Dakić V., Regvart D. Advancing Cybersecurity with Honeypots and Deception Strategies. Informatics. 2025. Vol. 12, no. 1. Article 14. DOI: 10.3390/informatics12010014.
7. National Institute of Standards and Technology. Implementing a Zero Trust Architecture: High-Level Document. NIST Special Publication 1800-35. Gaithersburg, MD : NIST, 2025. 55 p. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-35.pdf (accessed: 15.03.2026).
8. Oracle Communications Session Border Controller Security Guide. Release S-Cz9.2.0 - for Service Provider and Enterprise. Oracle, 2023. 111 p. URL: https://docs.oracle.com/en/industries/communications/session-border-controller/9.2.0/security/security-guide.pdf (accessed: 15.03.2026).
9. Sheffer Y., Saint-Andre P., Fossati T. Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS). RFC 9325. Best Current Practice 195. November 2022. URL: https://www.rfc-editor.org/info/rfc9325 (accessed: 15.03.2026).