ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В МЕРЕЖІ NGN»

на здобуття освітнього ступеня магістра
зі спеціальності 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Віктор БОЦЕНКО
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Виконав: здобувач вищої освіти гр. ТСДМ-62
Віктор БОЦЕНКО
Ім'я, ПРІЗВИЩЕ

Керівник: Володимир РУЖИНСЬКИЙ
к.т.н. *Ім'я, ПРІЗВИЩЕ*

Рецензент: _____
Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Телекомунікацій

Кафедра ___Телекомунікаційних систем та мереж_____
Ступінь вищої освіти __магістр_____
Спеціальність ___172 Електронні комунікації та радіотехніка _____
Освітньо-професійна програма _____Телекомунікаційні системи та мережі_____

ЗАТВЕРДЖУЮ
Завідувач кафедри __ТСМ_____
_____ Віктор ЗАЇКА
«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Боценку Віктору Сергійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Захист персональних даних в мережі NGN
керівник кваліфікаційної роботи Володимир РУЖИНСЬКИЙ, к.т.н.
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» 10. 2025 р. № 467

2. Строк подання кваліфікаційної роботи «___» _____ 2025 р.

3. Вихідні дані до кваліфікаційної роботи:
   1. Захист персональних даних.
   2. NGN.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
   1. Безпека та конфіденційність у NGN.
   2. Захист VoIP мереж в концепції архітектури NGN.
   3. Проблеми захисту персональних даний в середовищі штучного інтелекту.
   4. Захист даних на серверному рівні.

5. Перелік ілюстративного матеріалу: ___презентація на ____слайдах_____

6. Дата видачі завдання «___» _____ 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір та аналіз науково-технічної літератури	15.10.2025	Викон.
2	Розробка першого розділу	22.10.2025	Викон.
3	Розробка другого розділу	02.11.2025	Викон.
4	Розробка третього розділу	12.11.2025	Викон.
5	Розробка четвертого розділу	22.11.2025	Викон.
6	Висновки, вступ, реферат	02.12.2025	Викон.
7	Розробка презентації	12.12.2025	Викон.

Здобувач вищої освіти _____ Віктор БОЦЕНКО
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Володимир РУЖИНСЬКИЙ
(підпис) *(Ім'я ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій
ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Боценко В.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)
на тему: «Захист персональних даних в мережі NGN»

Кваліфікаційна робота і рецензія додаються.

Директор ННІТ _____ Владислав КРАВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Боценко Віктор Сергійович показав гарну теоретичну та інженерну підготовку, уміння володіти новими комп'ютерними технологіями, користуватися навчальною, довідковою і науково-технічною літературою. Працюючи над завданнями, які були поставлені керівником, проявив ініціативність, сумлінність та хист до наукової роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача Боценка Віктора Сергійовича на оцінку «відмінно» та присвоїти йому кваліфікацію магістр з електронних комунікацій та радіотехніки.

Керівник кваліфікаційної роботи _____ Володимир РУЖИНСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Боценко В.С. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри телекомунікаційних систем та мереж _____ Віктор ЗАЇКА
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу
на здобуття освітнього ступеня магістра

здобувача вищої освіти Боценка Віктора Сергійовича
(прізвище, ім'я, по батькові)
на тему «Захист персональних даних в мережі NGN»

Актуальність.
Стрімкий розвиток телекомунікаційних технологій, перехід до архітектур NGN, 5G та майбутніх 6G супроводжуються зростанням обсягів даних і появою нових кіберзагроз. Інфраструктури стають гетерогенними, відкритими та високозалежними від віртуалізації, хмарних сервісів і штучного інтелекту, що підвищує ризики витоку, перехоплення та маніпуляції персональними даними. Традиційні моделі периметрового захисту вже не забезпечують належного рівня безпеки, тому виникає потреба у нових підходах, зокрема Zero Trust, посилених механізмах шифрування, захисті VoIP та адаптивних системах кібермоніторингу.
Позитивні сторони.
1. У роботі досліджено концепцію Zero Trust, яка була визначена як ключова для захисту персональних даних у мережах нового покоління.
2. У роботі особлива увага приділена питанням конфіденційності, інтеграції ШІ та постквантової криптографії.
Недоліки.
1. У роботі недостатньо уваги приділено правовим і нормативним аспектам захисту персональних даних у NGN.
2. У роботі бракує чітких посилань на стандарти 3GPP, ITU та NIST у тих місцях, де наведені технічні твердження.

Відзначені зауваження не впливають на загальну позитивну оцінку магістерської кваліфікаційної роботи

Висновок: *кваліфікаційна робота на здобуття ступеня магістра заслуговує оцінку "відмінно", а здобувач Боценко Віктор Сергійович заслуговує присвоєння кваліфікації: магістр з електронних комунікацій та радіотехніки.*

Рецензент _____ _____
науковий ступінь, вчене звання (підпис) *(Ім'я ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 76 стор., 14 рис., 1 табл., 28 джерел.

Мета роботи – розробити та обґрунтувати комплексний підхід до підвищення безпеки персональних даних і VoIP-сервісів у телекомунікаційних мережах NGN шляхом аналізу загроз, вивчення сучасних механізмів захисту та визначення оптимальних технічних і організаційних рішень.

Об’єкт дослідження – телекомунікаційні мережі наступного покоління, їх архітектура, механізми передавання даних і системи забезпечення інформаційної безпеки.

Предмет дослідження – методи, моделі та технології захисту персональних даних і VoIP-трафіку в мережах NGN, включаючи використання SBC, механізмів аутентифікації, шифрування, IDS та сучасних концепцій кіберзахисту.

Короткий зміст роботи: у роботі проаналізовано особливості захисту персональних даних у мережах NGN, які поєднують мобільні, стаціонарні, оптичні, супутникові та IoT-технології. Показано, що зі зростанням швидкості передавання даних, масштабом підключень та інтеграцією хмарних і ШІ-систем збільшується кількість кіберзагроз. Визначено основні уразливості VoIP-інфраструктури та роль SBC у приховуванні топології, фільтрації трафіку та виявленні атак. Окрема увага приділена ризикам обробки даних у ШІ та методам їх мінімізації. Доведено, що традиційні моделі безпеки не відповідають вимогам NGN, а ключовою концепцією захисту є Zero Trust, яка забезпечує багаторівневу, адаптивну та проактивну оборону.

КЛЮЧОВІ СЛОВА: NGN, ПЕРСОНАЛЬНІ ДАНІ, КІБЕРБЕЗПЕКА, 5G, 6G, VOIP, SIP, SBC, IDS, ZERO TRUST, IP-ТЕЛЕФОНІЯ, IOT, INTERNET OF EVERYTHING, ШТУЧНИЙ ІНТЕЛЕКТ, ФЕДЕРАТИВНЕ НАВЧАННЯ, КРИПТОГРАФІЯ, DDOS, ФРОД, МАРШРУТИЗАЦІЯ, СЕГМЕНТАЦІЯ МЕРЕЖІ, АУТЕНТИФІКАЦІЯ, ШИФРУВАННЯ

ABSTRACT

Text part of the master's qualification work: 76 pages, 14 figures, 1 table, 28 sources.

The purpose of the work is to develop and substantiate a comprehensive approach to improving the security of personal data and VoIP services in NGN telecommunication networks by analyzing threats, studying modern protection mechanisms and determining optimal technical and organizational solutions.

Object of the study is next-generation telecommunication networks, their architecture, data transmission mechanisms and information security systems.

Subject of the study is methods, models and technologies for protecting personal data and VoIP traffic in NGN networks, including the use of SBC, authentication mechanisms, encryption, IDS and modern concepts of cyber protection.

Summary of the work: the work analyzes the features of personal data protection in NGN networks, which combine mobile, fixed, optical, satellite and IoT technologies. It is shown that with the increase in data transfer speed, the scale of connections and the integration of cloud and AI systems, the number of cyber threats increases. The main vulnerabilities of VoIP infrastructure and the role of SBC in topology hiding, traffic filtering and attack detection are identified. Special attention is paid to the risks of data processing in AI and methods for their minimization. It is proven that traditional security models do not meet the requirements of NGN, and the key concept of protection is Zero Trust, which provides multi-level, adaptive and proactive defense.

KEYWORDS: NGN, PERSONAL DATA, CYBERSECURITY, 5G, 6G, VOIP, SIP, SBC, IDS, ZERO TRUST, IP TELEPHONY, IOT, INTERNET OF EVERYTHING, ARTIFICIAL INTELLIGENCE, FEDERATED LEARNING, CRYPTOGRAPHY, DDOS, FRAUD, ROUTING, NETWORK SEGMENTATION, AUTHENTICATION, ENCRYPTION

ЗМІСТ

ВСТУП 9
РОЗДІЛ 1 БЕЗПЕКА ТА КОНФІДЕНЦІЙНІСТЬ У NGN 11
1.1 Еволюція мереж зв'язку та загроз безпеки 11
1.2 Безпека в NGN та 6G 23
1.3 Адаптація існуючої архітектури безпеки 27
РОЗДІЛ 2 ЗАХИСТ VOIP МЕРЕЖ В КОНЦЕПЦІЇ АРХІТЕКТУРИ NGN 33
2.1 Основні конфігурації 33
2.2 Використання Intrusion Detect System 39
РОЗДІЛ 3 ПРОБЛЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИЙ В СЕРЕДОВИЩІ ШТУЧНОГО ІНТЕЛЕКТУ 45
3.1 Ризики при обробці даних ШІ 45
3.2 Обмеження та ризики обробки персональних даних у системах штучного інтелекту 48
3.3 Генеративно-змагальні мережі та федеративне навчання 51
РОЗДІЛ 4 ЗАХИСТ ДАНИХ НА СЕРВЕРНОМУ РІВНІ 58
4.1 Принцип Zero-Trust 58
4.2 Практики для внутрішнього захисту серверів та даних 63
ВИСНОВКИ 75
ПЕРЕЛІК ПОСИЛАНЬ 77
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 80

ВСТУП

Стрімкий розвиток телекомунікаційних технологій протягом останніх десятиліть призвів до глибокої трансформації способів обміну інформацією, дистанційної взаємодії та побудови цифрових сервісів. Еволюція від аналогових систем зв'язку першого покоління (1G) до високошвидкісних цифрових мереж 4G та інтелектуальних платформ 5G стала основою для появи нового етапу — концепції NGN (Next Generation Networks) та майбутніх мереж 6G. NGN розглядається як універсальна інтегрована інфраструктура, здатна забезпечити конвергенцію мобільних, фіксованих, оптичних, бездротових, супутникових, IoT- та хмарних технологій. У такій мультисередовищній екосистемі ключову роль відіграють дані — включаючи персональні, конфіденційні та службові відомості, що циркулюють між різними платформами та сервісами.

Зі зростанням обсягів цифрової інформації, кількості підключених пристроїв і складності мережевих архітектур значно збільшується кількість кіберзагроз. Сучасні атаки на мережі NGN охоплюють цілий спектр інструментів — від перехоплення сигналів та фальсифікації SIP-трафіку у VoIP-системах до DDoS-атак, фроду, маніпуляції маршрутизацією, несанкціонованого доступу, вторинної обробки персональних даних у системах штучного інтелекту. Особливу небезпеку становлять атаки, спрямовані на IP-телефонію та голосові сервіси, які залишаються критично важливими в NGN. Саме тому ключовими елементами безпеки стають Session Border Controllers (SBC), що забезпечують контроль трафіку, приховування топології, фільтрацію небезпечних запитів, запобігання фроду та виявлення атак через IDS-модулі.

У контексті NGN персональні дані піддаються багатоетапній обробці, включаючи передавання, зберігання, аналіз, агрегацію та використання для автоматизованого прийняття рішень. До цього додається інтеграція штучного інтелекту, яка стала невід'ємною частиною мереж наступного покоління: прогнозування навантажень, адаптивне керування спектром, кібермоніторинг, розпізнавання подій, оптимізація QoS. Але навчання моделей ІІ пов'язане зі

значними ризиками щодо приватності, адже використання великих масивів даних часто призводить до побічних витоків, можливості реконструкції особистості, дискримінації або створення непрозорих алгоритмів ухвалення рішень. У роботі також розглядаються такі сучасні методи зменшення ризиків, як федеративне навчання та генеративно-змагальні мережі (GAN), що дозволяють зменшити кількість реальних персональних даних, необхідних для обробки.

Усе це підкреслює, що традиційні моделі безпеки, орієнтовані на периметровий захист, більше не можуть гарантувати належного рівня захисту персональних даних у NGN. Саме тому особливої актуальності набуває концепція Zero Trust («нульової довіри»), основана на принципах постійної перевірки, мінімізації привілеїв, сегментації, контролю доступу, поведінкової аналітики та активного моніторингу. На відміну від класичних підходів, Zero Trust виходить із припущення, що загроза може існувати на будь-якому рівні — всередині чи зовні системи — а тому кожен запит повинен бути перевірений, а кожен користувач має отримувати доступ лише до мінімально необхідних ресурсів.

Актуальність теми зумовлюється необхідністю розробки надійних механізмів захисту персональних даних у складному, гетерогенному середовищі NGN, де ризики стрімко зростають, а масштаби обробки цифрової інформації набувають безпрецедентного рівня. Результати роботи дозволяють визначити оптимальні підходи до забезпечення приватності та сталого функціонування мереж наступного покоління.

1 БЕЗПЕКА ТА КОНФІДЕНЦІЙНІСТЬ У NGN

1.1 Еволюція мереж зв'язку та загроз безпеки

Таблиця 1.1

Еволюція технологій

Технології	**Швидкість**	**Функції**	**Початок розробки**	**Впровадження**
1G	до 1,9 Кбіт/с	дзвінки	1970	1984
2G	до 14,4 Кбіт/с	смс	1980	1991
3G	до 3,6 Мбіт/с	інтернет	1990	2002
4G	до 1 Гбіт/с	відеострімінг	2000	2010
5G	до 10 Гбіт/с	Ultra HD і 3D-відео, AI-додатки	2008	2018

Еволюція мереж зв’язку та розвиток їхньої безпеки

Перші покоління мобільних мереж зіштовхнулися з широким спектром проблем у сфері кіберзахисту. У міру розвитку технологій змінювався й характер загроз: від примітивних атак із перехоплення до складних багаторівневих атак, які враховували слабкі місця архітектури мережі, механізмів шифрування, процедур ідентифікації та взаємодії між обладнанням. З появою нових поколінь мобільного зв’язку рівень компетентності зловмисників зростав разом зі складністю самих мереж.

Перше покоління (1G)

Мережі першого покоління стали початком епохи мобільного зв’язку та фактично започаткували використання переносних телефонних пристроїв у масовому масштабі. Їхнє розгортання розпочалося на початку 1980-х років у США,

Японії та Європі. Основною метою таких мереж було забезпечення голосової мобільності — дати користувачам можливість здійснювати дзвінки поза межами фіксованої телефонної мережі. Стандарти 1G існували в різних варіаціях, наприклад AMPS у США, NMT у Скандинавії, TACS у Великобританії. Всі вони працювали на основі аналогової радіотехнології та використовували широкі частотні смуги для передавання голосового сигналу.

Оскільки 1G — це повністю аналогова система, будь-яка інформація передавалася у вигляді звичайних радіохвиль без будь-яких засобів цифрової обробки. Це означало, що всі розмови передавалися "відкритим текстом", тобто в чистому вигляді, без шифрування та захисту. Тому будь-хто, хто мав простий радіоприймач, сканер частот або навіть деякі телевізійні адаптери, міг випадково або навмисно перехоплювати мобільні дзвінки. На той час це вважалося суттєвою проблемою, але її наслідки стали очевиднішими у міру того, як користувачі почали обговорювати по телефону конфіденційну інформацію — особисту, фінансову, ділову.

Уразливості 1G були пов’язані не лише з відсутністю шифрування. Мережа не використовувала жодних методів аутентифікації — ні користувача, ні обладнання. Тому підробка сигналу або видавання себе за іншу мобільну станцію було досить простим завданням. Зловмисники могли клонувати ідентифікатори телефонів, здійснювати дзвінки за рахунок інших абонентів або просто підміняти трафік. Такі схеми шахрайства стали настільки поширеними, що оператори втрачали мільйони доларів, а користувачі часто ставали жертвами нелегальних списань.

Ще однією серйозною проблемою 1G була її низька стійкість до перешкод та можливість легкого втручання в ефір. Наприклад, зловмисник міг навмисно створити радіоперешкоди, блокувати зв’язок або навіть підмінювати голосовий сигнал, вводячи в оману абонентів. Через це мережі 1G часто стикалися з перешкодами, нестабільністю сигналу та низьким захистом каналів.

Усе це призводило до того, що мережі першого покоління були практично нездатними забезпечити базові принципи інформаційної безпеки:

- Конфіденційність — відсутня через відкритий характер передавання даних.
- Цілісність — порушувалася можливістю модифікації сигналу.
- Доступність — могла бути порушена шляхом простих радіоперешкод.
- Аутентичність — не забезпечувалася взагалі.

Таким чином, мережі 1G хоч і стали важливим технологічним проривом, але були абсолютно незахищеними. Користувачі постійно перебували під загрозою перехоплення розмов, крадіжки особистої інформації, підміни дзвінків або підключення до мережі сторонніх осіб. Саме критичні недоліки безпеки 1G стали однією з головних причин переходу до цифрових мереж другого покоління.

Друге покоління (2G)

Запровадження другого покоління мобільного зв’язку стало революційним етапом у розвитку телекомунікацій. Саме 2G перетворило мобільний телефон на більш надійний та масовий засіб комунікації. На відміну від аналогових систем 1G, мережі 2G вперше використовували цифрову обробку сигналів, що суттєво покращило якість зв’язку, знизило рівень шумів і дозволило впровадити базові механізми безпеки.

Стандарт GSM (Global System for Mobile Communications) став домінуючою технологією 2G, поширившись у більш ніж 150 країнах. Він підтримував не лише голосові дзвінки, а й короткі текстові повідомлення SMS, які стали надзвичайно популярними та фактично створили новий формат комунікації.

Однією з ключових переваг 2G була поява цифрових методів модуляції, таких як TDMA, які забезпечували стабільніший зв’язок, вищу пропускну здатність і можливість одночасного обслуговування більшої кількості абонентів на одній частоті.

Покращення безпеки в 2G

Порівняно з практично незахищеними мережами 1G, друге покоління вперше запровадило комплекс заходів захисту, які стали новим стандартом для галузі. До найважливіших нововведень належать:

1. Аутентифікація абонента методом «запит–відповідь»

Мережа надсилала виклик (challenge), а SIM-карта відповідала згенерованим кодом, створеним на основі унікального ключа. Це дозволяло перевіряти, що абонент є легітимним користувачем.

2. Шифрування каналу зв’язку

Передавання голосових даних і SMS відбувалося в зашифрованому вигляді, що суттєво зменшувало ризик перехоплення. Алгоритми A5/1 та пізніші модифікації забезпечували захист від простого прослуховування.

3. Використання SIM-карти як носія криптографічних ключів

SIM-карта стала інтелектуальним модулем безпеки, який:

- зберігав секретні ключі,
- відповідав за створення криптографічних кодів,
- забезпечував аутентифікацію абонента.

Це відокремлювало особистість користувача від пристрою та підвищувало захист.

4. Тимчасовий ідентифікатор TMSI

Замість передачі постійного ідентифікатора IMSI мережа використовувала тимчасовий номер TMSI. Це запобігало можливості стеження за абонентом через його унікальний ідентифікатор.

Усі ці рішення значно підвищили конфіденційність і створили основу для формування сучасних систем захисту мобільного зв’язку.

Уразливості та слабкі місця 2G

Попри значні покращення, система безпеки 2G мала серйозний структурний недолік — односторонню аутентифікацію. Тобто телефон підтверджував свою особу перед мережею, але не мав засобів перевірити, чи справжня перед ним базова станція.

Це призвело до появи одного з найнебезпечніших типів атак — фальшивих базових станцій, або IMSI-catcher. Такі пристрої:

- видавали себе за справжню базову станцію оператора,
- змушували телефони підключатися до себе,

- могли знімати шифрування або примушувати телефон працювати в незахищеному режимі,
- перехоплювали SMS, дзвінки та службову інформацію.

Крім того, зловмисники могли:

- стежити за переміщенням абонентів через перехоплення службових повідомлень,
- підмінювати або фальсифікувати дані,
- втручатися в сигнальний трафік,
- виконувати атаки повторного відтворення.

Вразливості алгоритмів шифрування A5/1 і A5/2 також поступово були розкриті дослідниками. У деяких регіонах використовували ще слабші варіанти шифрування або взагалі вимикали його, що створювало додаткові ризики.

Усе це робило 2G набагато безпечнішою за 1G, але все ще недостатньо стійкою до сучасних типів атак.

Третє покоління (3G)

Поява мереж третього покоління на початку 2000-х років стала черговим етапом у розвитку мобільних комунікацій. Ці мережі вперше запропонували користувачам повноцінний мобільний доступ до інтернету, перетворивши мобільний телефон із засобу голосового зв’язку на мультимедійний пристрій. Завдяки швидкості передачі даних до 2 Мбіт/с користувачі отримали можливість переглядати веб-сторінки, користуватися онлайн-сервісами, дивитися відео та здійснювати потокову трансляцію — те, що раніше було доступним лише на домашніх комп’ютерах.

3G стала відповіддю на зростаючі потреби мобільних користувачів у швидкості, стабільності та безпеці. Її впровадження базувалося на нових радіотехнологіях (наприклад, WCDMA та CDMA2000), які дозволили суттєво збільшити пропускну здатність і кількість одночасних підключень.

Удосконалення механізмів безпеки в 3G

Хоча мережі 3G частково спиралися на напрацювання 2G, у сфері безпеки вони зробили великий якісний стрибок. Ключові нововведення значно зменшили ризики перехоплення, підміни сигналу та несанкціонованого доступу.

1. Двостороння аутентифікація

На відміну від 2G, де лише телефон перевірявся мережею, у 3G з'явилася взаємна аутентифікація. Це означало, що:

- абонент перевіряє мережу,
- мережа перевіряє абонента.

Завдяки цьому фальшиві базові станції, що залишалися проблемою у 2G, ставали набагато менш ефективними.

2. Протокол AKA (Authentication and Key Agreement)

AKA став одним із найважливіших нововведень. Він забезпечує:

- підтвердження особи абонента,
- автоматичне узгодження криптографічних ключів,
- захист від атак повторного відтворення,
- підвищену стійкість до підміни сигналів.

Цей протокол значно підвищив загальну безпеку мережі та забезпечив основу для майбутніх поколінь зв'язку.

3. Посилений захист IP-трафіку

Оскільки 3G поступово переходила на IP-орієнтовані мережеві структури, особливу увагу було приділено захисту інтернет-трафіку. Запроваджено:

- нові методи шифрування,
- захист службових каналів,
- удосконалення протоколів передачі даних,
- ізоляцію службових та користувацьких потоків.

Захист IP-трафіку став ключовим компонентом у запобіганні зламу мобільних пристроїв через інтернет.

Комплексна система безпеки від 3GPP

Організація 3GPP (3rd Generation Partnership Project) розробила детальну й багаторівневу модель захисту, яка охоплює всі компоненти мережі:

- радіоінтерфейс,
- транспортну мережу,
- інфраструктуру оператора,
- сигнальні системи,
- мобільні пристрої.

Це була перша по-справжньому системна спроба створити стандартизовану архітектуру безпеки для всієї мережі мобільного зв’язку.

Уразливості та загрози для мереж 3G

Попри значні покращення, мережі третього покоління не стали повністю невразливими. Із переходом на більш складну інфраструктуру з’явилися нові типи атак.

1. Атаки на IP-протоколи

Оскільки значна частина трафіку передавалася через IP, мережі 3G успадкували вразливості, притаманні інтернету:

- сканування портів,
- атаки на протоколи маршрутизації,
- спроби обходу міжмережевих екранів,
- експлуатацію вразливостей у транспортних протоколах.

Зловмисники могли намагатися впливати на роботу мережевих вузлів або втручатися в сигнальний трафік.

2. Атаки на канали між пристроями та домашніми мережами

Ці канали зазвичай були частково захищені, однак їх складність робила їх привабливою ціллю. Наприклад:

- можлива підміна пакетів,
- спроби перехоплення службових даних,
- втручання в канали тунелювання.

3. Несанкціонований доступ до послуг

Хоча більшість механізмів доступу була покращена, злочинці все ще могли намагатися:

- обходити платіжні системи,

- отримувати доступ до незаконних послуг,
- використовувати SIM-карти для шахрайських операцій.

4. DDoS-атаки

Мережі 3G були здатні передавати значно більше даних, що робило їх уразливими до розподілених атак відмови в обслуговуванні (DDoS). Особливо небезпечними були атаки на:

- базові станції,
- шлюзи обміну пакетами,
- DNS-сервери операторів.

Категорії загроз радіоінтерфейсу

Усі загрози, пов’язані з радіочастотними каналами, умовно поділялися на чотири основні категорії:

1. Порушення цілісності — зміна або модифікація даних під час передачі.
2. Порушення доступності (DoS/DDoS) — блокування каналів або перевантаження мережі.
3. Порушення конфіденційності — спроби перехоплення, декодування або аналізу трафіку.
4. Порушення функціональності — вплив на роботу мережевих сервісів або обходження механізмів аутентифікації.

Ці виклики вимагали постійного удосконалення протоколів і підштовхнули появу нових стандартів, які згодом лягли в основу технологій 4G.

Четверте покоління (4G)

Мережі четвертого покоління, масове впровадження яких розпочалося у 2009 році, стали справжнім проривом у сфері мобільних комунікацій. На відміну від попередніх поколінь, що мали гібридну архітектуру, 4G базується на повністю пакетній передачі даних, використовуючи технології LTE (Long Term Evolution) та OFDMA. Це забезпечило можливість досягати швидкості завантаження до 1 Гбіт/с і передачі до 500 Мбіт/с, перетворивши мобільний інтернет із допоміжного інструмента на рівноцінний аналог домашніх широкосмугових мереж. Саме 4G дало змогу користуватися високоякісним HD-відеострімінгом,

відеоконференціями, онлайн-іграми, хмарними сервісами та інтерактивними мультимедійними платформами, що вимагали низької затримки та стабільної пропускної здатності.

Однак радикальний перехід до повністю IP-орієнтованої архітектури, яка замінила традиційні комутаційні рішення, створив і новий спектр кіберзагроз. Оскільки вся передача даних — як користувацьких, так і службових — здійснюється поверх IP-протоколів, мережі 4G стали вразливими до загроз, властивих інтернет-середовищу. Це означає, що багато класичних атак, характерних для локальних або глобальних комп'ютерних мереж, тепер стали можливими й у мобільних системах.

Однією з ключових загроз є несанкціонований доступ до мережевих ресурсів. Зловмисники можуть намагатися проникнути в мережеві вузли, використовуючи вразливості в інфраструктурі операторів, слабкі механізми автентифікації або неправильно налаштовані елементи мережі. В умовах повної IP-орієнтації та централізації основних служб оператори повинні забезпечити ретельний контроль доступу, інакше компрометація одного вузла може створити серйозні системні наслідки.

Не менш небезпечним є перехоплення трафіку та підслуховування. Хоча 4G використовує сучасні механізми шифрування, складні атаки на сигнальні протоколи, слабини у реалізаціях або неправильна конфігурація обладнання можуть дозволити зловмисникам отримати доступ до конфіденційних даних. Додатковою загрозою є можливість аналізу метаданих, які часто залишаються незашифрованими й можуть розкривати інформацію про переміщення або профіль користувача.

Ще однією групою небезпек є модифікація даних і втручання в мережеві процеси. Оскільки LTE використовує продумані механізми маршрутизації та передачі пакетів, атака на один із вузлів або каналів може призвести до зміни вмісту пакетів, перенаправлення трафіку або штучного створення затримок. Такі втручання часто застосовуються для організації MitM-атак, коли зловмисник стає посередником між користувачем та мережею.

Атаки на протоколи керування є однією з найсерйозніших загроз. Протоколи рівнів керування та сигналізації, зокрема RRC та NAS, керують підключеннями, аутентифікацією, переходом між базовими станціями та іншими критичними процесами. Якщо атакувати ці протоколи, можна спричинити перебої в роботі мережі, створити перевантаження, ініціювати хибні переходи між сотами або навіть зірвати зв’язок користувачів.

Додаткову небезпеку становлять вразливості на рівні MAC, які дозволяють проводити атаки повторного відтворення, запис і повторну передачу трафіку або вплив на розподіл ресурсів. У результаті це може спричинити зниження якості зв’язку, втрату пакетів чи порушення стабільності всієї базової станції. Також існує ризик перехоплення службових повідомлень, що, хоча й не дає доступу до вмісту даних, але може використовуватися для подальших атак.

Загалом, підвищена взаємодія між користувацькими пристроями, програмами, додатками та хмарними сервісами значно розширила поверхню атаки. Мережі стали більш відкритими, адже сучасні смартфони взаємодіють з величезною кількістю сторонніх сервісів і серверів. Це створює більше точок входу для кіберзлочинців і вимагає від операторів і розробників постійного моніторингу, оновлення систем безпеки та впровадження сучасних технічних і організаційних засобів захисту.

Таким чином, 4G, незважаючи на свої величезні можливості та технологічні переваги, принесло з собою нові виклики у сфері безпеки. Відкритість архітектури, залежність від IP-протоколів і велика кількість взаємодій у мережі роблять її потенційною мішенню для широкого спектра атак. Саме ці проблеми стали однією з причин необхідності переходу до більш захищених і гнучких систем п’ятого покоління — 5G.

П’яте покоління (5G)

Технологія 5G стала одним із наймасштабніших проривів у розвитку мобільних мереж і визначила новий рівень можливостей для цифрових систем. На відміну від попередніх поколінь, 5G створювалася не лише для підвищення швидкості передачі даних, а й для забезпечення стабільності, гнучкості та

масштабованості, потрібної для сучасних цифрових екосистем — від побутових інтернет-пристроїв до промислових роботизованих комплексів та автономного транспорту.

Однією з головних переваг 5G є надвисока швидкість передачі даних, яка може досягати **10 Гбіт/с**. Такий рівень швидкодії став можливим завдяки застосуванню міліметрових хвиль у діапазоні від 30 до 300 ГГц. Ці частоти дозволяють передавати інформацію на надзвичайно великих швидкостях, хоча й мають менший радіус покриття. Щоб компенсувати цю особливість, 5G використовує розвинуті масиви антен MIMO з підтримкою формування променя (beamforming). Це дає змогу направляти сигнал точно в бік користувача, зменшуючи втрати та значно підвищуючи ефективність використання спектра.

Ще однією унікальною характеристикою п’ятого покоління є можливість **масового підключення пристроїв**. На одній базовій станції можуть працювати тисячі сенсорів, контролерів, побутових і промислових пристроїв, що є критично важливим для розвитку Інтернету речей (IoT), розумних міст, автономних транспортних мереж і виробничих систем Industry 4.0. Завдяки низькій затримці — менше однієї мілісекунди — 5G дозволяє передавати дані майже в реальному часі, що відкриває шлях до нових сфер застосування: дистанційної хірургії, роботизованих фабрик та обчислень на межі мережі.

Антени у мережах 5G менші за розміром, ніж у 4G, але набагато складніші з точки зору конструкції. Вони здатні формувати десятки незалежних променів, кожен із яких може працювати з окремим користувачем або групою пристроїв. Це дозволяє одній базовій станції обслуговувати значно більше абонентів без втрати якості сигналу. Крім того, використання щільнішої мережі малих сот (small cells) підвищує пропускну здатність та знижує навантаження на основні базові станції.

Однак разом із перевагами 5G принесла і новий набір загроз, що пов’язані, зокрема, зі складністю архітектури та широким застосуванням віртуалізації. Однією з найсерйозніших проблем є **атаки типу DoS та ресурсні атаки**, що використовують надвисоку пропускну здатність мережі. Якщо зловмисник створює

штучне навантаження на базову станцію або ядро мережі, це може призвести до перевантаження, відмови в обслуговуванні та недоступності ключових сервісів.

Важливою технологічною складовою 5G є використання **NFV (Network Function Virtualization)** — віртуалізація мережевих функцій, що раніше виконувались фізичним обладнанням. Віртуалізовані елементи можуть переміщуватися між різними серверами або датацентрами для оптимізації ресурсів. Проте така мобільність створює ризики витоку даних, порушення цілісності інформації та атак під час міграції сервісів. Якщо віртуальна функція потрапляє у ненадійне середовище, зловмисники можуть отримати доступ до конфіденційних ключів або даних абонентів.

Ще однією загрозою є **ризик розкриття особистої інформації**. Архітектура 5G передбачає взаємодію великої кількості компонентів — датчиків, пристроїв, сервісів і міжмережевих платформ. Значна частина трафіку передається між різними рівнями мережі, хмарними середовищами та сторонніми сервісами. Якщо механізми захисту налаштовані неналежним чином або використовуються слабкі протоколи, приватна інформація користувача може бути розкрита через метадані, некоректні конфігурації API чи атаки на оркестратори мережевих функцій.

Крім того, розподілена й децентралізована структура мережі збільшує площу атаки: окремі вузли, віртуальні компоненти або крайові обчислювальні модулі можуть стати точкою входу для зловмисників. Додаткові ризики виникають через інтеграцію величезної кількості сторонніх пристроїв, не всі з яких мають достатню апаратну або програмну безпеку.

У результаті мережі 5G, хоча й значно випереджають попередні покоління за швидкістю, масштабованістю та гнучкістю, залишаються складною екосистемою, у якій безпека стає не просто технічною вимогою, а критичним фактором стабільності всієї інфраструктури. Саме тому оператори, виробники обладнання та міжнародні стандартизуючі органи активно працюють над створенням посилених механізмів шифрування, аутентифікації та захисту віртуальних компонентів, щоб забезпечити надійну роботу 5G у майбутньому.

1.2 Безпека в NGN та 6G

Мережі шостого покоління, які нині перебувають на стадії концептуального проєктування, розглядаються як наступний великий стрибок у розвитку мобільних технологій та цифрових інфраструктур. 6G має стати логічним продовженням 5G, але зі значно ширшими можливостями, орієнтованими не лише на підвищення швидкості чи зменшення затримки, а на створення нової цифрової екосистеми, де інтелектуальні системи, автономні машини, дані та люди будуть об’єднані в єдину взаємодіючу мережу.

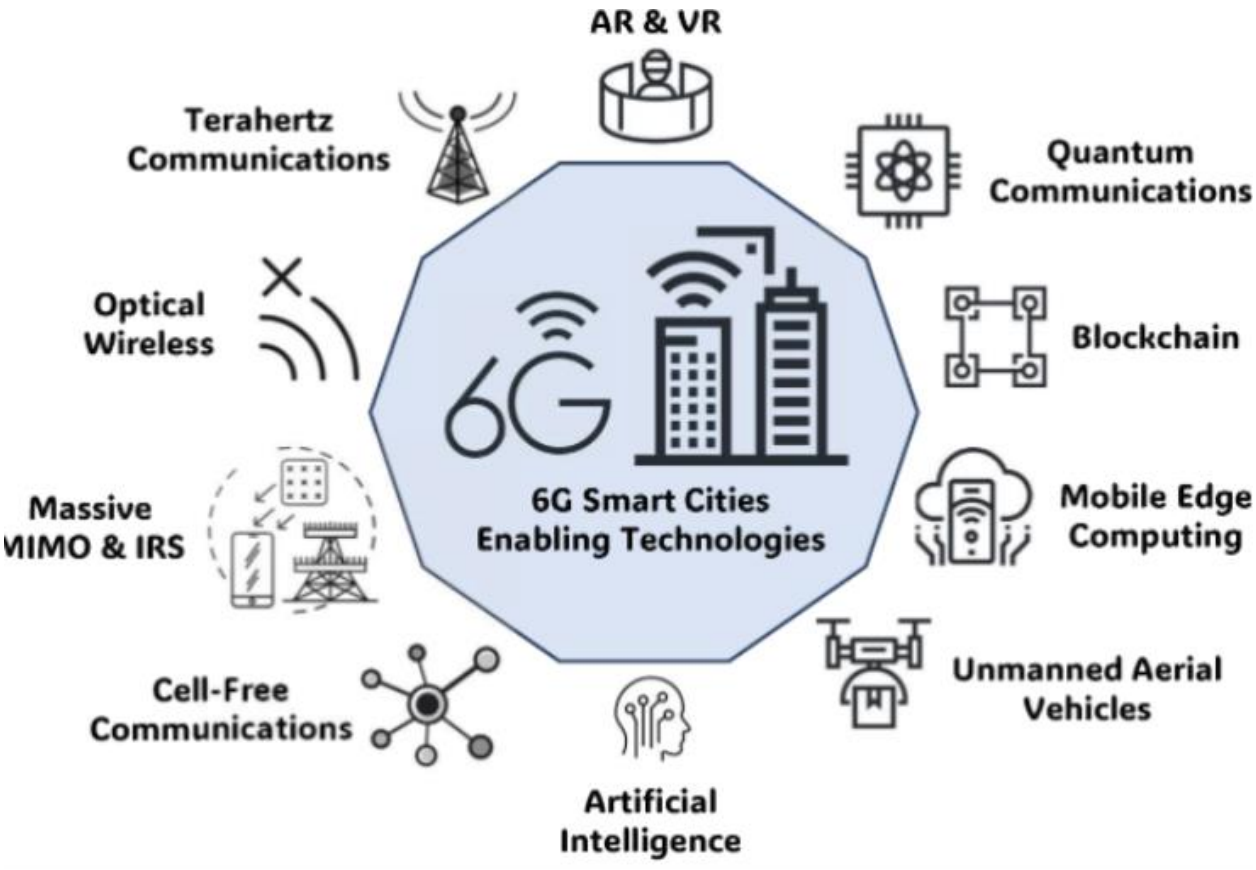


Рис. 1.1 Основні технологічні компоненти 6G: терагерцова комунікація, штучний інтелект, безосередкові мережі, мобільні периферійні обчислення, квантові комунікації, блокчейн, БПЛА, масивні MIMO та інші інновації для розумних міст

Очікується, що технологія 6G забезпечить швидкості передачі даних від 1 Тбіт/с і вище, що суттєво перевершує навіть найкращі показники мереж 5G. Досягнення таких швидкостей стане можливим завдяки використанню терагерцового спектра, покращених масивів антен, нових схем управління

спектром і гібридних методів модуляції. Це відкриє двері до надшвидких інтернет-з’єднань із практично миттєвою реакцією, що є критично важливим для автономного транспорту, високоточних промислових роботів, дистанційної хірургії, систем цифрового близнюка й інших сфер, де навіть мілісекундна затримка є надто великою.

Однією з ключових особливостей архітектури 6G стане повна відкритість і гнучкість мережевої інфраструктури. Швидке зростання кількості хмарних систем, програмного забезпечення з відкритим вихідним кодом та інструментів автоматизації приведе до появи нової концепції під назвою NaaS — Network as a Service. У межах цього підходу користувачі отримають можливість самостійно налаштовувати мережу під свої потреби. Наприклад, вони зможуть визначати бажаний рівень шифрування, обирати параметри безпеки, регулювати якість обслуговування, управляти географічним розташуванням ресурсів і навіть змінювати архітектуру на рівні віртуальних функцій. Такий рівень персоналізації стане можливим завдяки інтелектуальній автоматизації й використанню програмно визначених мереж.

6G майже напевно означатиме перехід від інтернету речей (IoT) до значно ширшої концепції — інтернету всього (IoE). У такій моделі учасниками мережі будуть не лише класичні пристрої — смартфони, комп’ютери, сенсори, побутова техніка, — а й дані, бізнес-процеси, хмарні сервіси, автономні системи, математичні моделі та навіть цифрові двійники реальних об'єктів. Це створить абсолютно новий рівень інтегрованості між цифровим і фізичним просторами, відкриваючи можливості для реалістичної доповненої та віртуальної реальності, тактильного інтернету, хмарної роботизації та повністю автоматизованих систем керування.

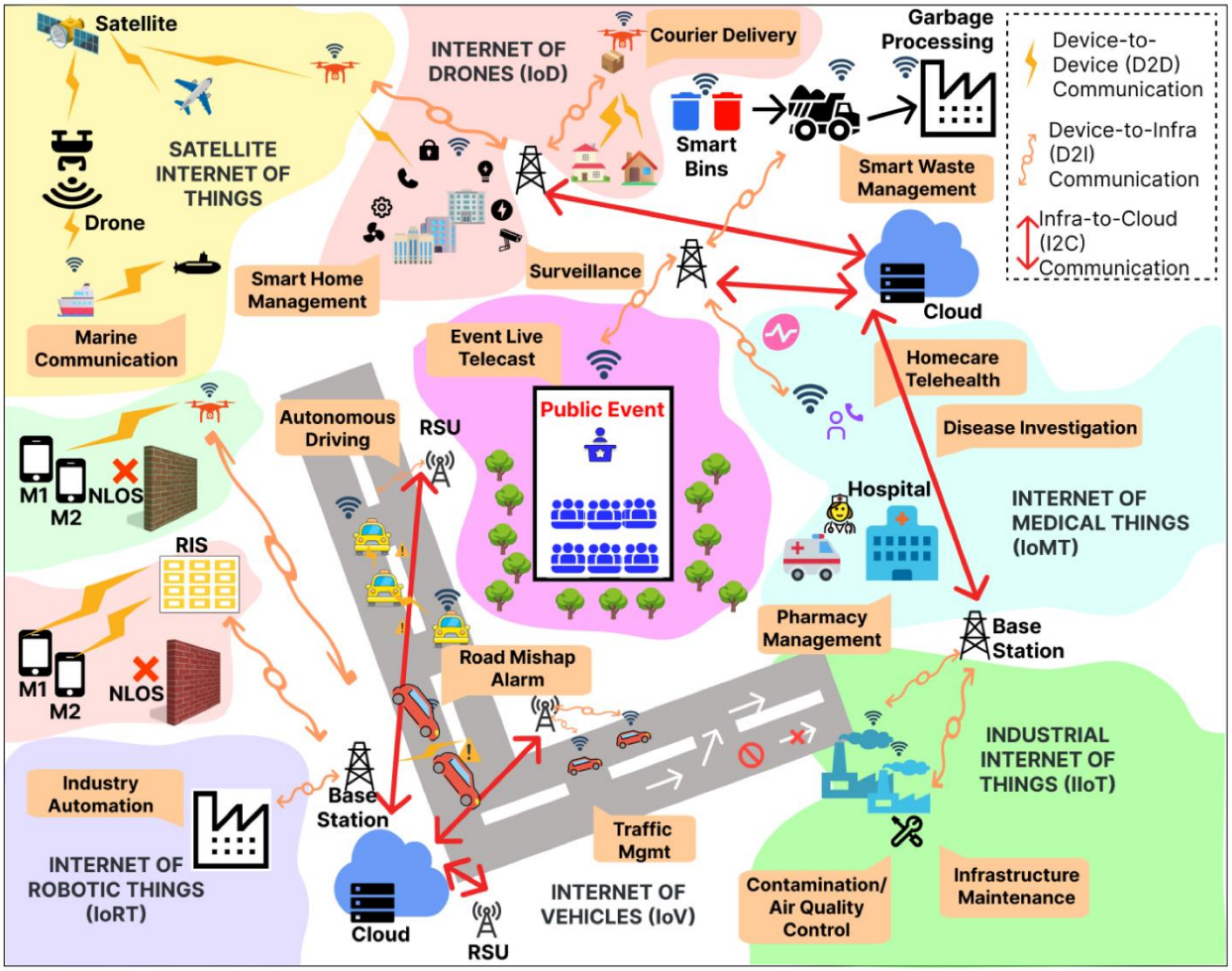


Рис. 1.2 Концептуальна модель 6G, що демонструє взаємодію транспортних, медичних, промислових, роботизованих та супутникових систем через багаторівневу інфраструктуру Інтернету всього (IoE)

Ще однією фундаментальною особливістю 6G стане те, що це може бути перша мобільна мережа, побудована навколо штучного інтелекту (ШІ). Якщо у 5G основна ідея полягала у створенні «мережі підключених речей», то у 6G головним баченням стане «мережа підключеного інтелекту». Очікується, що штучний інтелект і машинне навчання стануть центральними механізмами, які контролюватимуть більшість мережевих операцій. ШІ зможе самостійно оптимізувати маршрути даних, перерозподіляти ресурси, прогнозувати навантаження, визначати потенційні аномалії чи загрози, забезпечувати персоналізовану якість обслуговування та моментально адаптувати мережу до нових умов. Також можливе використання квантової передачі даних, квантових сенсорів та квантового шифрування на базових рівнях інфраструктури.

Попри свої переваги, шосте покоління мобільного зв’язку не уникне викликів у сфері безпеки. Оскільки 6G успадковуватиме частину технологічної бази від 5G — Multi-access Edge Computing, Software-defined Networking, Network Functions Virtualization, slicing — відповідні вразливості теж залишаться актуальними. Особливо небезпечними будуть атаки на SDN-контролери, які керують усією логікою маршрутизації, а також атаки на віртуальні машини, менеджери гіпервізорів і модулі розподілу віртуальних мережевих функцій. MEC, як уразливий компонент, залишиться чутливим до фізичного доступу та DDoS-атак, адже розміщується на периферії мережі — ближче до користувачів і потенційних зловмисників.

Варто враховувати, що в екосистемі 6G значно зросте кількість пристроїв із обмеженими ресурсами — розумні годинники, датчики, мініатюрні камери, VR-окуляри, трекери та інші гаджети. Такі девайси часто не мають достатньої обчислювальної потужності для застосування складних шифрувальних алгоритмів. У моделі IoE саме вони можуть стати найпривабливішою ціллю для зловмисників, адже їхнє компрометування дозволить отримати доступ до великих масивів даних або створити вразливі точки в мережі.

Архітектура безпеки 6G, за попередніми оцінками, буде побудована на концепції повної автоматизації та мінімального втручання людини. Технологія ZSM (Zero-touch Service Management) має забезпечити швидке розгортання сервісів, зниження експлуатаційних витрат і мінімізацію людських помилок. Водночас це створює складні виклики: у мережі, де майже всі процеси контролюються автоматично, захист конфіденційності та забезпечення безпеки даних стають надзвичайно складним завданням.

Через відкритість архітектури 6G поступово зникатиме різниця між внутрішньою та зовнішньою частинами мережі. Це означає, що традиційні засоби безпеки — міжмережеві екрани, VPN або брандмауери — більше не зможуть забезпечити достатній рівень захисту. Мережа стане настільки розподіленою, що класична модель периметру перестане працювати. Саме тому фундаментальною основою системи кіберзахисту 6G має стати парадигма нульової довіри (Zero Trust,

ZT). Її головна ідея — припустити, що зловмисник потенційно присутній у будь-якій частині мережі. Жодний компонент, жодна взаємодія не повинні вважатися безпечними за замовчуванням — перевірка має бути постійною, глибокою та автоматизованою.

На основі цієї концепції формується архітектура нульової довіри (Zero Trust Architecture, ZTA) — складна система правил, протоколів, взаємодій і контрольних механізмів, яка покликана забезпечити максимальний рівень контролю над доступом, автентифікацією, переміщенням даних і поведінкою мережевих об'єктів. У 6G ZTA стане обов’язковим фундаментом, який визначатиме всю логіку роботи безпеки — від користувацького рівня до хмарних компонентів і квантових комунікацій.

Таким чином, 6G, попри свою відкритість і надзвичайну технологічність, потребуватиме ще більш серйозного підходу до безпеки, ніж будь-яке попереднє покоління мобільних мереж. Імовірно, саме кібербезпека стане тим фактором, який визначатиме, наскільки успішним і надійним буде нове покоління глобальної комунікації.

1.3 Адаптація існуючої архітектури безпеки

Із розвитком мереж шостого покоління стає очевидним, що механізми безпеки, які застосовувалися в 3G, 4G та навіть 5G, вже не здатні забезпечити необхідний рівень захисту. Технологічне середовище стрімко ускладнюється, а кількість взаємодіючих компонентів зростає геометрично. Якщо попередні покоління мобільного зв’язку зосереджувалися насамперед на швидкості передачі, якості голосового зв’язку та оптимізації використання спектра, то 6G розглядається як глобальна інтегрована інфраструктура, що працюватиме в абсолютно різних умовах і середовищах. Йдеться про наземний, повітряний, космічний і навіть підводний сегменти, кожен з яких має свої власні ризики, фізичні обмеження та специфічні загрози.

Оскільки 6G прагне об’єднати уніфіковану інтелектуальну комунікаційну платформу, вона повинна адаптуватися до систем супутникового зв’язку, оптичних каналів, мобільних дронів, підводних сенсорів та автономних транспортних комплексів. Це означає, що традиційні підходи до кіберзахисту, які працювали в межах суто наземних мереж, більше не можуть вважатися достатніми. Для такого масштабного середовища необхідно створювати нові криптографічні алгоритми, модифіковані протоколи аутентифікації та механізми захисту, які враховуватимуть особливості кожного типу середовища, його фізичні властивості та потенційні вектори атак. Наприклад, космічні системи можуть страждати від радіаційних впливів та перешкод, тоді як підводне середовище значно ускладнює передачу сигналів через акустичні та гідродинамічні ефекти.

Експерти прогнозують, що безпека 6G базуватиметься на багаторівневій архітектурі, яка матиме ієрархічну структуру. Передбачається наявність фізичного рівня, рівня з’єднання, мережевого, транспортного та прикладного рівнів, кожен з яких виконуватиме свої функції шифрування, контролю доступу, перевірки автентичності та моніторингу. Таке розділення дозволяє створити глибоко ешелоновану систему захисту, де компрометація одного шару не руйнує всієї інфраструктури.

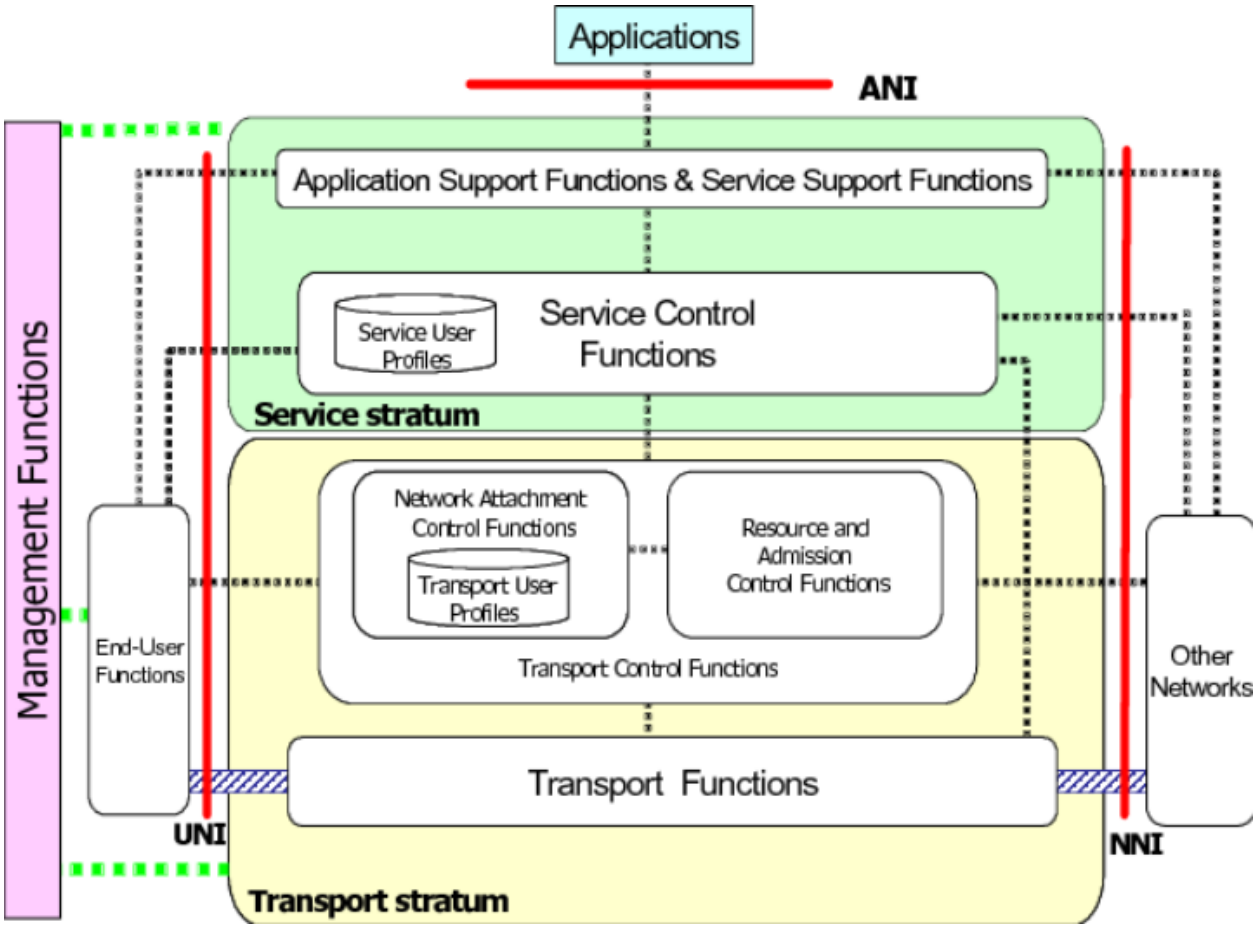


Рис. 1.3 Ієрархічна модель NGN/6G, що відображає розподіл функцій між транспортним, сервісним та прикладним рівнями та їхню взаємодію в інтелектуальній мережевій інфраструктурі

Ситуація ускладнюється ще й тим, що у 6G все частіше згадують про інтеграцію таких технологій, як роботизовані системи, автономні транспортні засоби, безпілотні літальні апарати, промислові сенсори, цифрові двійники та штучний інтелект. Кожен із цих сегментів не лише збільшує обсяг даних, що передаються мережею, але й створює нові потенційні точки входу для зловмисників. У такій складній екосистемі будь-який компонент, навіть найменший сенсор або IoT-пристрій, може стати джерелом загрози.

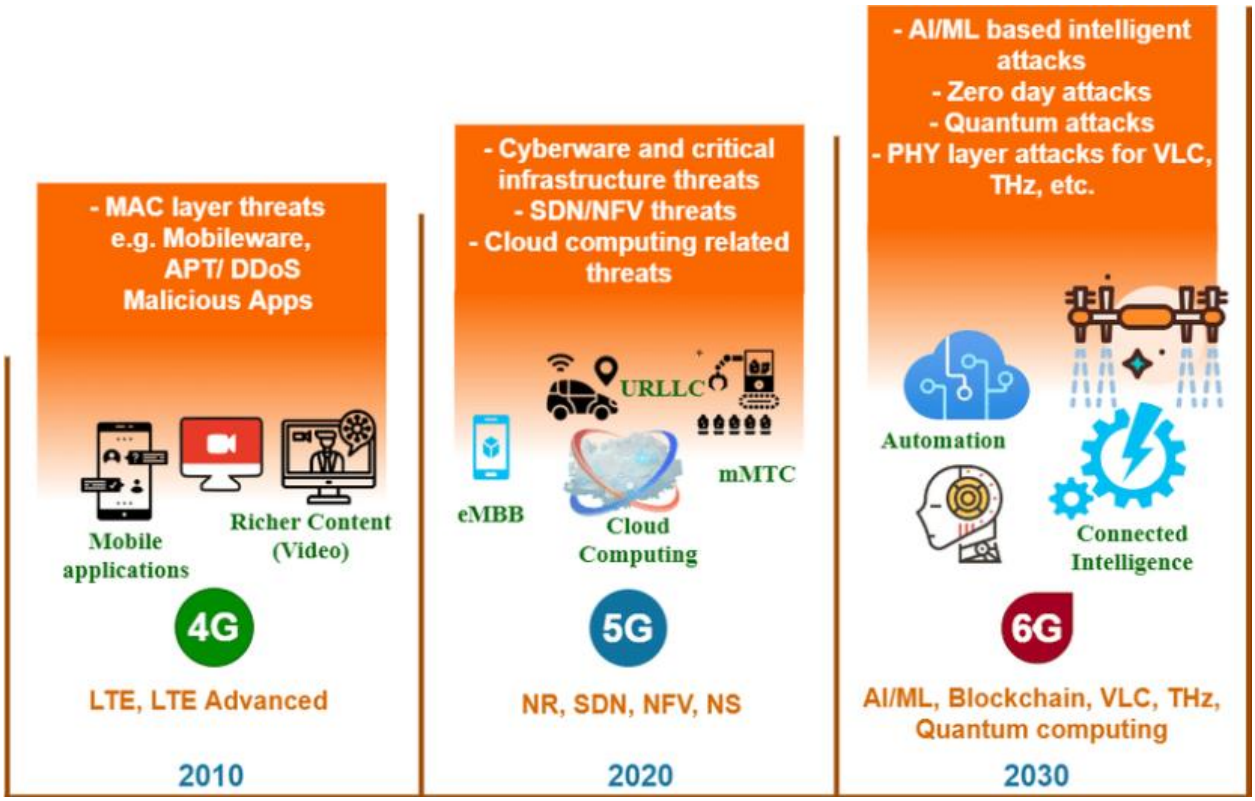


Рис. 1.4 Еволюція загроз для систем мобільного зв'язку від 4G до 6G, що демонструє ускладнення інфраструктури та появу нових класів атак у міру розвитку технологій

Ключові вимоги до ахисту мереж 6G

1. Використання високобезпечних систем віртуалізації

Оскільки 6G значною мірою покладатиметься на віртуалізовані мережеві функції та хмарні обчислення, важливу роль відіграватимуть високобезпечні системи віртуалізації. Платформи такого типу, включно з гіпервізорами (VMware ESXi, Hyper-V, KVM) та контейнерними інструментами (Docker, Kubernetes), забезпечують можливість створення відокремлених середовищ, у яких розміщуються мережеві функції, сервіси та користувацькі застосунки.

Кожен гіпервізор повинен мати можливість:

- виявляти приховане шкідливе ПЗ (руткіти, стелс-модулі),
- забезпечувати повну ізоляцію між окремими віртуальними мережами,
- контролювати доступ до апаратних ресурсів,
- гарантувати цілісність даних і роботу хмарних систем навіть у разі локальних атак.

У середовищі NFV компрометація одного елемента може вплинути на роботу цілої мережі, тому безпека віртуалізації є фундаментальною.

2. Управління уразливостями відкритого програмного забезпечення

У 6G очікується значне зростання використання рішень із відкритим кодом, оскільки сама архітектура буде більш гнучкою, динамічною та схильною до автоматизованого оновлення компонентів. Використання open source сприяє швидкому розвитку технологій, але водночас створює ризики, пов’язані з:

- недоліками безпеки у відкритому коді,
- неконтрольованими залежностями,
- можливістю компрометації через «ланцюжок постачання» (supply chain attack),
- потребою в безперервному моніторингу та виправленні вразливостей.

Управління відкритим ПЗ має включати моніторинг репозиторіїв, перевірку пакунків на наявність підписів, аналіз версій, швидке оновлення та, у разі необхідності, видалення компонентів.

3. Захист даних при використанні штучного інтелекту

ШІ стане центральним елементом 6G, відповідаючи за оптимізацію мережі, моніторинг аномалій, адаптивне керування спектром, прогнозування навантаження та розподіл ресурсів. Проте сам ШІ теж може стати мішенню для атак. Безпека моделей має гарантуватися через:

- цифрові підписи для перевірки справжності та цілісності моделей,
- захист процесу їх оновлення,
- запобігання атакам на систему навчання,
- захист від ін’єкції шкідливих даних.

Якщо зловмисник зможе змінити поведінку моделі ШІ, він отримає контроль над великими сегментами мережі.

4. Захист конфіденційності користувачів

У 6G обсяг персональної інформації, що передаватиметься мережею, різко збільшиться. Це стосується даних із сенсорів, медичних пристроїв, транспортних модулів, систем доповненої реальності, хмарного геймінгу та інших сервісів.

Для захисту конфіденційності потрібні:

- ізольовані довірені середовища виконання,
- анонімізація та мінімізація персональних даних,
- контроль доступу до API,
- обмеження обсягу даних, що можуть стати публічними.

Конфіденційність у середовищі IoE стане одним із найважливіших викликів.

5. Постквантова криптографія

З розвитком квантових комп'ютерів з'являється загроза для алгоритмів асиметричного шифрування, які використовуються сьогодні. RSA, ECC та інші криптосистеми можуть бути зламані новими квантовими методами.

Мережам 6G потрібно:

- перейти на постквантові алгоритми,
- адаптувати протоколи обміну ключами,
- гарантувати стійкість криптографії у довгостроковій перспективі.

Лише так можна забезпечити захист даних, що циркулюватимуть у критично важливих сервісах.

Узагальнюючи, варто підкреслити, що мережі 6G будуть формуватися як частина концепції NGN — Next Generation Networks, тобто мереж наступного покоління, які мають забезпечити повну гнучкість, адаптивність, інтелектуальність та безшовну взаємодію між різними технологічними доменами. NGN-архітектура передбачає інтеграцію мобільних, супутникових, оптичних, підводних і наземних систем у єдиний інтелектуальний простір. Саме тому безпека в NGN і 6G повинна бути не локальною та реактивною, а глибоко вбудованою, адаптивною та такою, що постійно самооновлюється.

Мережі шостого покоління стануть ядром глобальної NGN-інфраструктури, тому питання постквантової криптографії, довірених середовищ виконання, нульової довіри, захисту штучного інтелекту, аудиту відкритого ПЗ та безпечної віртуалізації вже зараз визначають фундамент цієї нової ери зв'язку. Успіх 6G та NGN залежатиме від того, наскільки ефективно буде вибудувана система кіберзахисту, здатна протистояти складним багаторівневим загрозам майбутнього.

2 ЗАХИСТ VOIP МЕРЕЖ В КОНЦЕПЦІЇ АРХІТЕКТУРИ NGN

2.1 Основні конфігурації

SBC та безпека: основні режими, принципи захисту та рекомендації

Перш ніж розглядати особливості захисту SBC (Session Border Controller), важливо зрозуміти, у яких типових конфігураціях він може працювати. Найчастіше виділяють два основні режими використання:

1. SIP Trunking — найпоширеніший варіант застосування SBC, коли він використовується для підключення до SIP-оператора через IP-мережу. У цьому випадку SBC виступає в ролі «межового шлюзу» між корпоративною телефонною інфраструктурою та зовнішнім середовищем оператора зв'язку.

2. Режим Registration — використання SBC для підключення віддалених користувачів до IP-АТС (наприклад, Asterisk) через інтернет. У цьому варіанті SBC виступає захисною точкою для реєстрацій користувачів, що підключаються з будь-якого місця світу.

Ці два режими істотно різняться з точки зору кібербезпеки. У випадку SIP Trunk підприємство зазвичай знає, з яких адрес надходитимуть виклики — зовнішній SIP-сервер оператора заздалегідь відомий (хоча є винятки, про які скажемо нижче). Натомість у режимі Registration абсолютно невідомо, звідки користувач може спробувати здійснити реєстрацію або виклик, що створює додаткові ризики. Усі подальші рекомендації та приклади базуються саме на цих двох сценаріях роботи SBC.

Базові підходи до забезпечення безпеки SBC

Захист SBC слід починати з найпростіших, але критично важливих речей, які формують основу всієї безпекової політики.

1. Ізоляція інтерфейсу керування SBC

Перший і найважливіший крок — розділити інтерфейс керування пристроєм та інтерфейси сигналізації.

У SBC AudioCodes інтерфейс для керування позначається роллю OAMP (Operations, Administration and Management). Він обов’язково повинен:

- бути доступним лише з внутрішньої мережі,
- розташовуватися в окремій підмережі, що не перетинається з VoIP-сегментом,
- бути ізольованим від зовнішніх маршрутів.

У великих корпоративних мережах атаки можуть походити навіть із внутрішнього середовища, тому виділення керувального інтерфейсу — принципове питання.

2. Використання нестандартних SIP-портів

Бажано уникати стандартного порту 5060, оскільки саме його в першу чергу сканують зловмисники.

У корпоративних мережах ця рекомендація особливо актуальна: на відміну від телеком-операторів, внутрішні SIP-адреси та порти ніде не публікуються, що ускладнює можливість їхнього виявлення.

Типова схема атаки виглядає так:

1. Зловмисник надсилає SIP-повідомлення одночасно на сотні чи тисячі адрес.
2. Він очікує на будь-яку відповідь.
3. Якщо відповідь отримано — починається проєктування конкретної атаки: перебір паролів, тестування реєстрацій, спроби обходу ACL тощо.

Використання нестандартного порту значно знижує ймовірність того, що SBC буде виявлений при масовому скануванні.

У SBC AudioCodes порти для SIP налаштовуються в таблиці SIP Interface Table, і зовнішній порт може відрізнятися від внутрішнього. Також не варто активувати протоколи (UDP/TCP/TLS), які не використовуються — для невикористовуваних портів значення слід встановлювати в «0».

3. Використання Firewall 3-го рівня для SIP Trunk

У випадку SIP-транку бажано максимально обмежити доступ до SBC так, щоб SIP-повідомлення та RTP-трафік могли надходити лише з конкретних IP-адрес

оператора. Це налаштовується в меню: Configuration → VoIP → Security → Firewall Settings

Однак є нюанси:

DNS-доступ

SIP-транк часто налаштовується не на IP, а на доменне ім’я оператора. Отже, якщо заблокувати доступ до DNS-серверів, SBC не зможе розв’язати доменне ім’я, що призведе до повної зупинки викликів.

Множинні IP-адреси оператора

Великі оператори використовують:

- кластерні рішення з десятками вузлів;
- динамічні пули IP-адрес, що змінюються з часом.

Тому жорстка фільтрація IP може призвести до ситуації, коли:

- частина викликів працюватиме, а частина — ні;
- або SIP-транк повністю перестане працювати після зміни IP-адрес.

Отже, Firewall бажано використовувати, але робити це потрібно обережно, з урахуванням динамічності адресації.

4. Call Admission Control — контроль викликів

Це один із найважливіших механізмів захисту SBC, який дозволяє:

- обмежувати кількість одночасних сесій,
- фільтрувати надмірні SIP-повідомлення,
- контролювати навантаження на канали.

Обмеження кількості одночасних сесій

- Для SIP Trunk: кількість одночасних викликів не повинна перевищувати кількість каналів, придбаних в оператора.
  Хоч оператор і повинен блокувати надлишок, але краще додатково контролювати це на своєму боці.
- Для Registration: суворе обмеження до 1–2 викликів на користувача.
  Два виклики інколи потрібні для переадресації, але саме механізм переадресації часто використовується хакерами для обхідних атак.

Обмеження приросту трафіку

У великих VoIP-інфраструктурах важко оперативно визначити раптовий сплеск трафіку.

Тому необхідно налаштувати:

- кількість сесій у секунду для SIP Trunk;
- кількість реєстрацій у секунду для режиму Registration.

Це особливо важливо при атаках на підбір паролів: зловмисник надсилає десятки чи сотні SIP REGISTER щосекунди. Обмеження на рівні SBC фактично унеможливлює такі атаки.

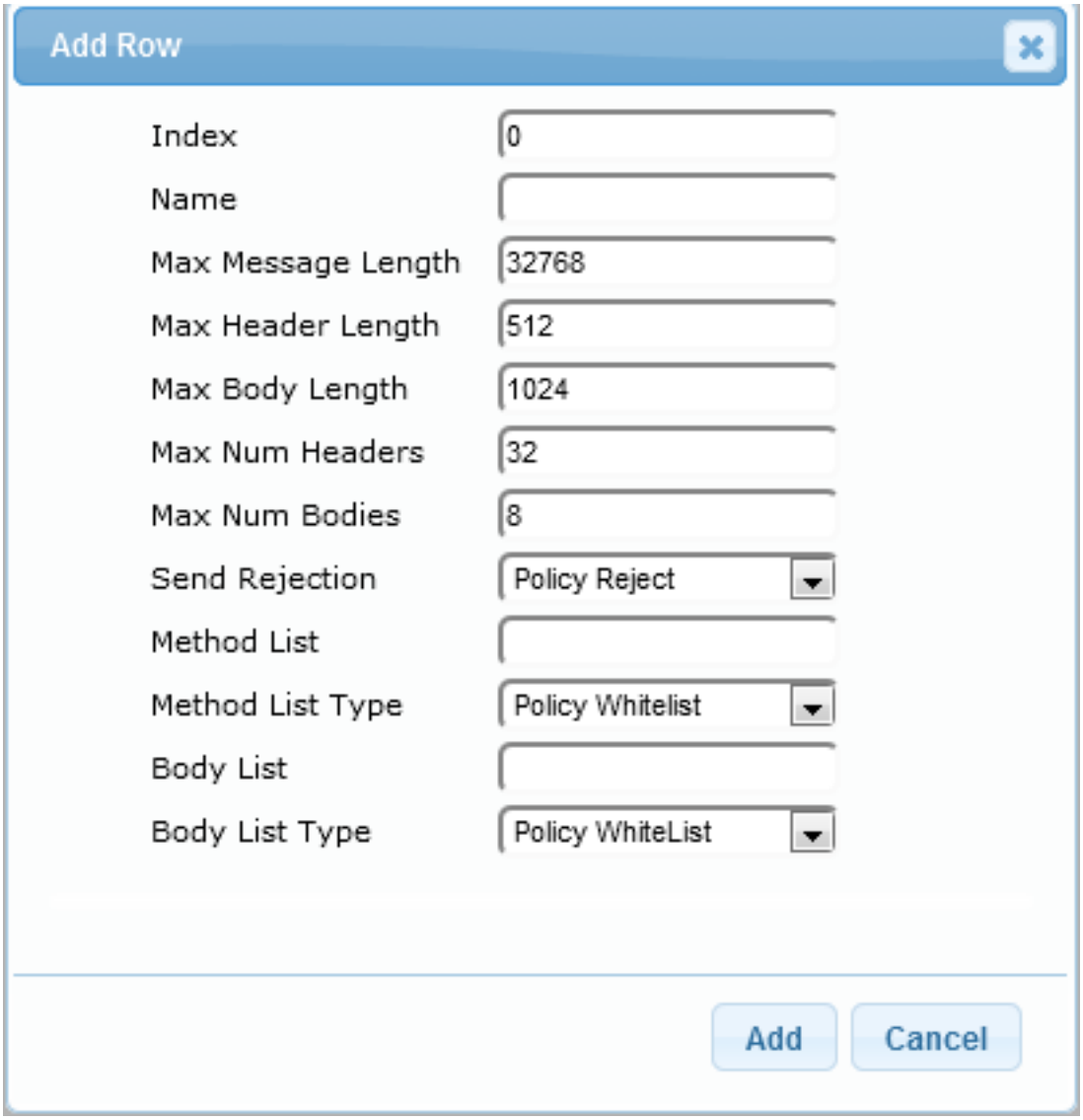


Рис. 2.1 Налаштування політик контролю SIP-повідомлень у SBC: обмеження розміру заголовків, тіла повідомлення, кількості заголовків і методів, а також визначення правил обробки небажаних або некоректних SIP-запитів

Одним із ключових завдань SBC є повне маскування внутрішньої топології мережі замовника. Йдеться не лише про приховування реальних IP-адрес, а й про захист будь-якої інформації, яка може непрямо розкрити структуру або особливості корпоративної інфраструктури. Деякі IP-АТС можуть додавати у SIP-повідомлення власні службові поля, у яких міститься конфіденційна інформація: внутрішні адреси, опис логічних модулів, версії програмного забезпечення тощо. Саме такі дані найчастіше використовують зловмисники для побудови карти мережі та подальшої атаки.

Якоїсь «чарівної галочки» для автоматичного приховування топології в SBC не існує. Єдиний справді ефективний спосіб — це детальний аналіз SIP-повідомлень і подальша їх трансформація за допомогою SIP Manipulation Rules. Такі правила дозволяють:

- видаляти небажані заголовки,
- модифікувати критичні поля,
- замінювати внутрішні адреси на публічні,
- нормалізувати формат повідомлень перед передачею назовні.

Таким чином SBC виступає своєрідним «фільтром», який не допускає витоку будь-якої інформації про внутрішню побудову мережі та захищає IP-АТС від розвідки та первинного збору даних з боку зловмисника.

Важливо пам’ятати, що атака може бути ініційована не лише ззовні, а й з внутрішньої мережі компанії. Через це контроль вихідних дзвінків є не менш важливим, ніж фільтрація вхідних. Першочерговим завданням є уникнення універсальних планів маршрутизації. Маршрути мають бути максимально конкретними й дозволяти виклики лише у визначені напрямки.

Однак не менш вагомим елементом безпеки є перевірка номера абонента, що здійснює вихідний виклик. Ефективним підходом є дозвіл викликів лише з внутрішніх службових номерів. Якщо виклик надходить із номера, який не відповідає внутрішній нумерації, SBC повинен відхилити запит.

AudioCodes SBC пропонує кілька механізмів такої перевірки:

- створення правил кваліфікації для вхідних номерів;

- обмеження маршрутів через префікси дозволених внутрішніх номерів;
- використання LDAP-каталогу для звірки номера з базою співробітників.

LDAP-перевірка особливо корисна для корпоративних середовищ, де кожен номер повинен відповідати конкретному користувачу або групі. Це дозволяє:

- перевіряти, чи існує номер у структурі організації;
- застосовувати політики доступу залежно від ролі користувача.

Наприклад, співробітник, який працює з європейськими партнерами, може мати дозвіл на дзвінки до ЄС, тоді як іншим такі напрямки будуть заблоковані. Цей метод ідеально підходить для компаній, де:

- АТС не підтримує розширені політики маршрутизації,
- використовується кілька АТС, але потрібне уніфіковане керування правами доступу,
- необхідно централізувати контроль вихідних дзвінків.

Додатково корисно впровадити окремі обмеження для користувачів, які підключаються через публічні мережі. Для таких абонентів доцільно дозволити лише внутрішні або місцеві виклики, повністю блокуючи дорогі або міжнародні напрямки.

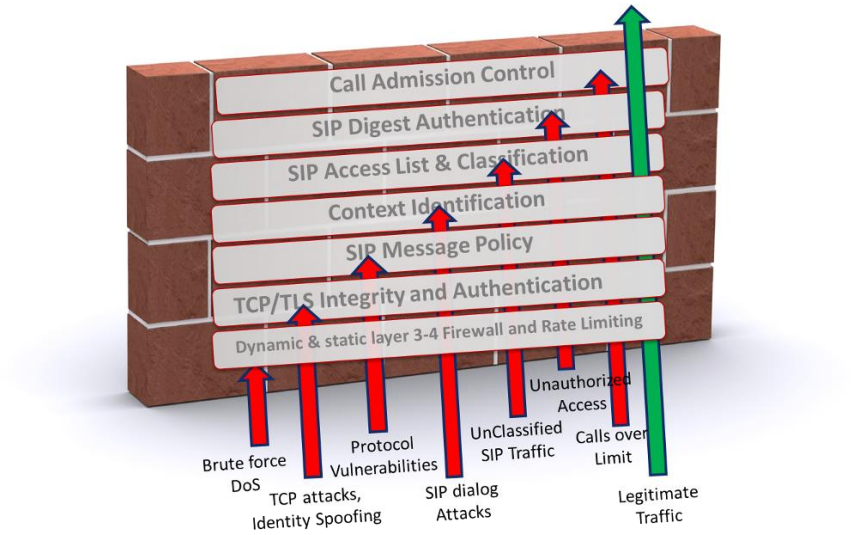


Рис. 2.2 Багаторівнева система захисту SIP-інфраструктури: послідовні механізми безпеки SBC (Firewall, TLS-аутентифікація, політики SIP-повідомлень, ACL, SIP Digest, Call Admission Control), які блокують різні типи атак — від brute force і DoS до несанкціонованого доступу та некласифікованого SIP-трафіку

2.2 Використання Intrusion Detect System

Усі описані раніше механізми безпеки SBC формують базовий рівень захисту інфраструктури IP-телефонії та покликані запобігати найпоширенішим загрозам — таким як крадіжка VoIP-трафіку, несанкціоновані виклики, фальсифікація повідомлень та маніпулювання маршрутами. Ці налаштування є першим рубежем оборони: вони закривають найвразливіші місця усієї системи й забезпечують фундамент, на якому вибудовується вся подальша система кіберзахисту. Однак сучасне VoIP-середовище дедалі частіше стикається з набагато складнішими видами атак — зокрема DoS та DDoS, метою яких є повне порушення доступності сервісу. У цих умовах традиційних засобів контролю вже недостатньо, і тому SBC застосовує спеціалізований механізм — IDS (Intrusion Detection System).

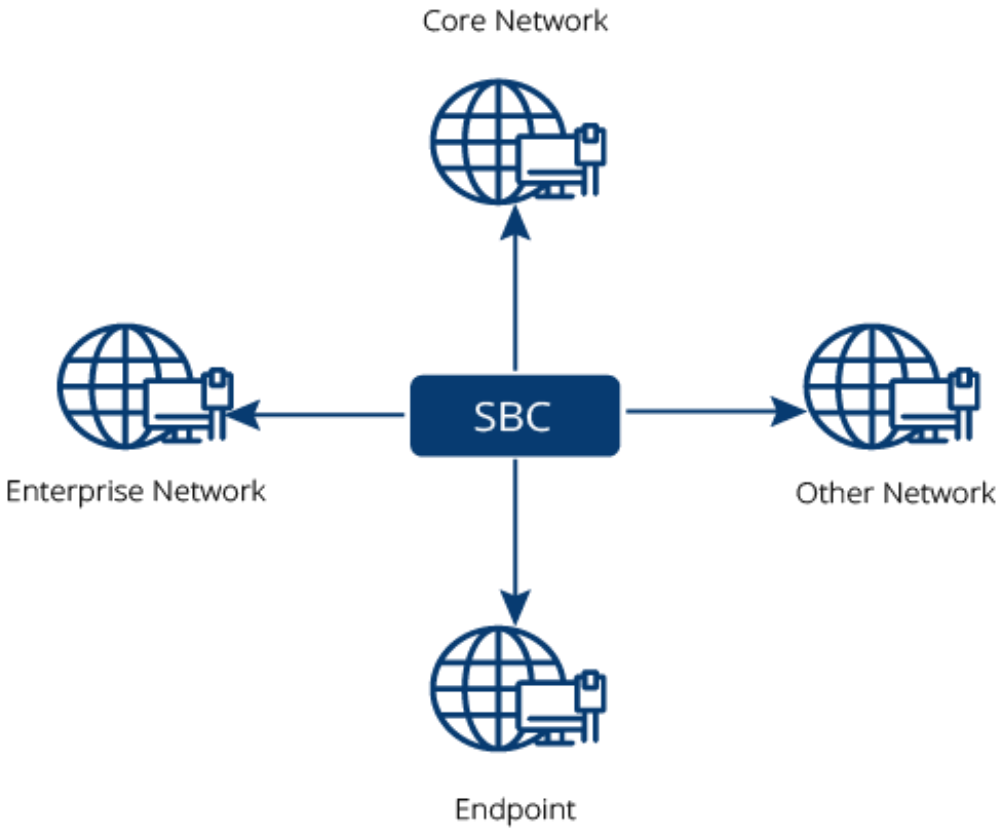


Рис. 2.3 Модель роботи SBC як центрального захисного вузла, що забезпечує контроль трафіку між корпоративною мережею, ядром оператора, зовнішніми мережами та кінцевими пристроями

Система IDS на AudioCodes Mediant виконує поглиблений аналіз SIP- та транспортного трафіку, виявляє підозрілу активність за заданими ознаками та вмикає відповідні механізми реагування. На відміну від базових політик, IDS орієнтована на поведінкову аналітику: вона оцінює не лише окремі SIP-пакети, а й взаємозв'язки між ними, часові інтервали, статичні та динамічні характеристики підозрілого трафіку.

Можливі реакції IDS:

1. **Надсилання SNMP Trap**

   Система повідомляє сервер моніторингу про подію, позначаючи її рівнем серйозності: *Minor*, *Major* або *Critical*. Це дозволяє централізованим засобам моніторингу швидко розуміти, наскільки небезпечна зафіксована активність.

2. **Тимчасове блокування IP-адреси або напряму**

   SBC може автоматично заблокувати доступ із джерела атаки на визначений проміжок часу — від кількох секунд до десятків хвилин.

3. **Журналювання інциденту з подальшим аудитом**

   Усі дані про подію можуть бути збережені у журналі, що дозволяє у майбутньому виконати аналіз, розслідування або створити нові політики захисту.

Пороги спрацювання та типи дій налаштовуються в таблиці IDS Rule Table, де адміністратор визначає, який тип трафіку вважати аномальним і що з ним робити.

Типи подій, які IDS здатна розпізнавати

Перший крок — визначення типу повідомлень або аномалій, на які система повинна реагувати. SBC дозволяє виявляти кілька ключових категорій.

1. Connection abuse

Цей тип подій пов'язаний із порушеннями під час встановлення TLS-з'єднання.

До нього відносяться:

- невдалі TLS-рукостискання;
- спроби використання підроблених або недійсних сертифікатів;

- порушення в обміні ключами;
- підозрілі відхилення у шифруванні.

Такі події можуть свідчити про спробу перехоплення трафіку або тестування вразливостей TLS-каналу.

2. Malformed message

До цієї категорії входять SIP-повідомлення, які мають некоректний формат. SBC перевіряє:

- відповідність структури SIP-стандарту;
- максимальну довжину повідомлення;
- коректність заголовків;
- відповідність правилам SIP Message Policy.

Більшість утиліт для сканування мережі формують саме такі спотворені повідомлення, тому цей тип подій є прямим індикатором розвідки або тестування мережі.

3. Authentication failure

Це помилки під час реєстрації або авторизації SIP-користувачів. Причинами можуть бути:

- неправильні паролі;
- спроби brute-force;
- невідповідність Digest-аутентифікації;
- виклики без коректної автентифікації.

Такий тип подій — один із головних індикаторів спроби підібрати пароль або отримати несанкціонований доступ.

4. Dialog establish failure

Виникає при помилках установлення SIP-діалогу. Це можуть бути:

- некоректні маршрути;
- відсутність необхідних заголовків;
- неправильне формування транзакцій;
- спроби створення фіктивного діалогу.

Цей тип подій є ознакою як технічних збоїв, так і навмисного втручання в SIP-логіку.

5. Abnormal flow

Охоплює нетипову SIP-активність:

- відповіді на неіснуючі запити;
- повідомлення без контексту сесії;
- запити від користувачів, яких немає в системі;
- хаотичні діалоги.

Це свідчить про некваліфікований або шкідливий трафік, а іноді — про інструменти для підбору інформації про систему.

Налаштування порогів, часових вікон і дій при атаці

Для кожного типу подій адміністратор налаштовує часові інтервали спостереження, порогові значення та відповідні дії. Наприклад:

Якщо з однієї IP-адреси надходить більше ніж 2 невдалі реєстрації за 5 секунд, SBC:

- фіксує подію як *brute-force*;
- надсилає SNMP-повідомлення;
- автоматично блокує адресу на вказаний час.

Такий підхід суттєво ускладнює підбір паролів, оскільки кожна нова спроба вимагає створення нового джерела атаки.

Водночас надто суворі обмеження можуть спричинити блокування легітимних користувачів, особливо якщо вони підключаються з нестабільних мереж. Тому баланс між безпекою та функціональністю є критично важливим.

Індивідуальність кожної інсталяції і потреба адаптації політик

Жодні дві VoIP-інфраструктури не є ідентичними.

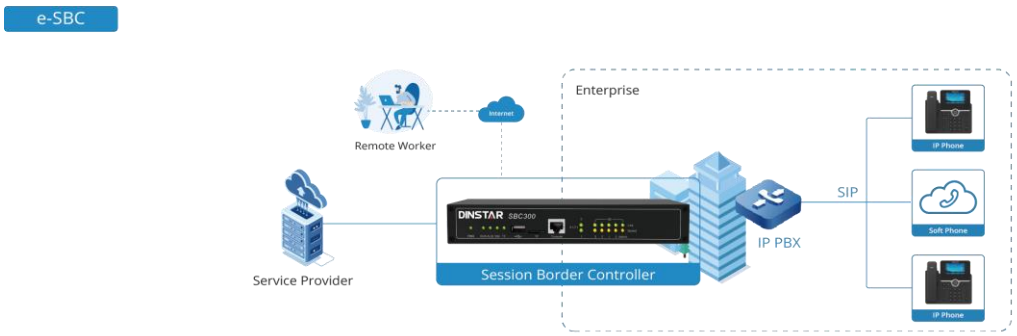


Рис. 2.4 Приклад інтеграції SBC у корпоративну VoIP-інфраструктуру: взаємодія з IP-АТС, SIP-провайдером, віддаленими співробітниками та внутрішніми VoIP-клієнтами. SBC виступає єдиною точкою захисту та контролю всіх VoIP-підключень

Вони відрізняються за:

- топологією;
- операторами;
- типами клієнтських пристроїв;
- схемами маршрутизації;
- вимогами бізнесу.

Саме тому не існує універсальної схеми безпеки. Кожен випадок потребує:

1. аналізу бізнес-процесів;
2. оцінки потенційних ризиків;
3. адаптації політик безпеки;
4. тестування впливу на функціональність;
5. постійного моніторингу та оптимізації.

SBC надає максимальний набір інструментів, але саме адміністратор вирішує, які комбінації політик забезпечать оптимальний баланс між захистом і стабільністю.

Висновки щодо ролі SBC у безпеці VoIP

Обсяг VoIP-трафіку у світі невпинно зростає, а разом із ним збільшується й кількість атак. Операторам важко контролювати величезні обсяги трафіку, тому

значна частина відповідальності за безпеку переходить до самих компаній. У цих умовах SBC стає ключовою ланкою захисту.

Його роль включає:

1. забезпечення безпечного підключення до SIP-операторів;
2. фільтрацію небажаного та шкідливого трафіку;
3. захист IP-АТС від brute-force та DDoS;
4. приховування топології корпоративної мережі;
5. контроль і обмеження VoIP-сесій;
6. уніфікацію політик безпеки;
7. централізацію роботи з VoIP-підключеннями;
8. запобігання телефонному фроду.

Особливо важливою є роль SBC у випадку підключення SIP-телефонів або софтфонів через публічний інтернет — саме такі точки найчастіше використовуються для зломів.

Також варто відзначити, що сучасні SBC доступні не лише операторам або великим підприємствам. На ринку представлені бюджетні моделі, які підтримують від 5 одночасних сесій і при цьому не поступаються старшим моделям у функціональності. Це робить SBC доступним рішенням для будь-якого бізнесу — від малих компаній до великих корпорацій.

3 ПРОБЛЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИЙ В СЕРЕДОВИЩІ ШТУЧНОГО ІНТЕЛЕКТУ

3.1 Ризики при обробці даних ШІ

Сучасні системи штучного інтелекту функціонують на основі двох ключових етапів — етапу навчання та етапу використання (інференсу). Саме ці два процеси визначають можливості, точність, адаптивність і потенційні ризики ШІ-рішень.

1. Етап навчання: як формується інтелект моделі

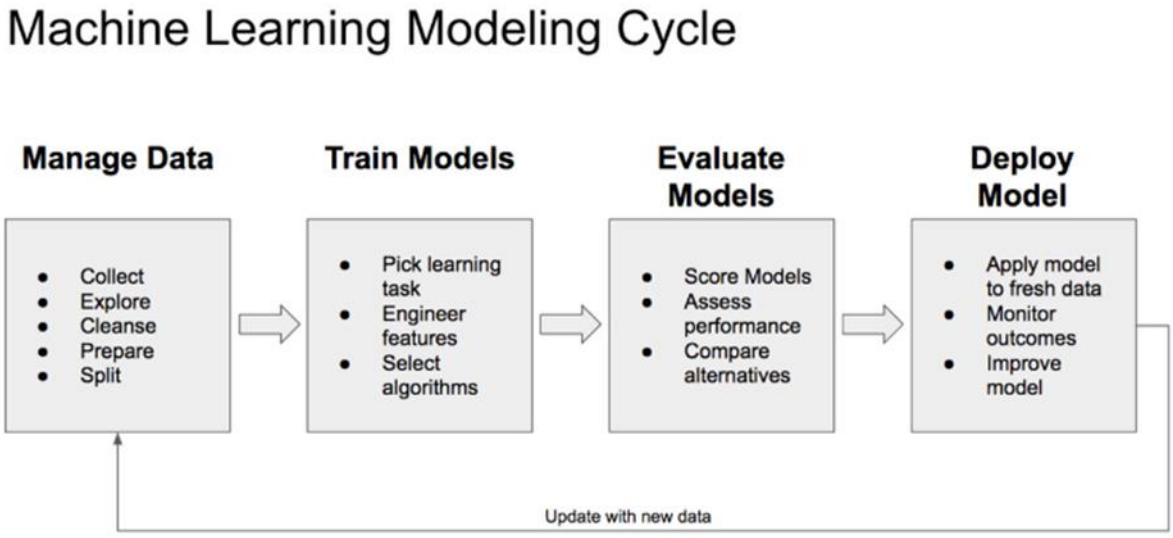


Рис. 3.1 Процес навчання моделі ШІ

Під час навчання штучного інтелекту алгоритми опрацьовують великі масиви даних, щоб виявити закономірності, структури, взаємозв'язки та повторювані патерни. Ідеться про дані абсолютно різного типу:

- мільйони зображень або відеоматеріалів;
- масиви текстів і документів;
- аудіозаписи, мовні команди;
- телеметричні дані, логи, статистичні масиви.

На цьому етапі нейронні мережі фактично навчаються розуміти світ, формуючи внутрішні моделі об'єктів, подій та мовних структур. Наприклад, модель для комп'ютерного зору вчиться розпізнавати обличчя, дороги, транспорт або

медичні аномалії на знімках. Мовна модель — структуру речень, смислові зв'язки, терміни й поняття.

Завдяки цьому формується так званий *"штучний досвід"*, який і визначає подальшу поведінку ШІ.

2. Етап використання: застосування навченого інтелекту

Після завершення навчання модель переходить у стадію практичного використання. На цьому етапі від неї вимагається:

- правильно класифікувати об'єкти;
- генерувати текст;
- відповідати на запити;
- аналізувати інформацію в реальному часі.

ШІ повинен ефективно використовувати знання, здобуті раніше, без повторного доступу до тих самих величезних масивів даних. Власне тут і проявляється реальна користь моделі: від чат-ботів і голосових помічників до медичних систем підтримки діагностики.

3. Ключова роль даних у роботі ШІ

Цілком очевидно, що обидва етапи — і навчання, і використання — абсолютно неможливі без великих обсягів даних. Дані є фундаментом усієї системи:

- без якісних та різноманітних даних модель не навчиться працювати коректно;
- без правильно підібраних наборів даних ШІ буде помилятися;
- без масивних структурованих колекцій інформації неможливо досягти високої точності.

Сучасні нейронні мережі буквально *"живляться"* інформацією. Для їхнього навчання створюються так звані data-pipelines — комплекси автоматизованих систем, які збирають, очищають, структурують та зберігають терабайти й петабайти даних.

Ці процеси часто називають *«пилососами даних»*, адже для якісного навчання потрібні величезні масиви зображень, текстів, аудіо й метаданих, які ШІ поглинає у неймовірних кількостях.

4. Проблема: персональні дані в контексті ШІ

Саме на цьому етапі виникає найбільше запитань, пов'язаних із конфіденційністю та захистом персональних даних. Великі набори інформації майже завжди включають:

- фотографії людей;
- імена, контактні дані, адреси;
- приватні документи;
- медичну або фінансову інформацію;
- телеметрію та поведінкові патерни користувачів.

Це створює низку суттєвих ризиків:

- неконтрольований збір даних, коли користувач навіть не знає, що інформацію використали;
- ризик витоку великих наборів даних, які зберігаються централізовано;
- потрапляння приватної інформації в модель, звідки її потім можна відтворити;
- використання даних без згоди, що порушує законодавство GDPR, Закон про персональні дані України та ін.;
- можливість зворотного аналізу моделей з метою відновлення вихідних даних.

Таким чином, робота ШІ неминуче пов’язана з величезними масивами інформації, а отже — з високими вимогами до безпеки, етичності та законності її використання.

Штучний інтелект відкриває масштабні можливості, але водночас потребує зваженого та відповідального підходу. Дані, на яких він працює, — це не просто інформація. Часто це реальні люди, їхні особисті історії, фото, записи, дії та взаємодія з цифровим світом.

Тому кожен етап — від збору інформації до розробки й розгортання моделі — повинен супроводжуватися:

- чіткими правилами безпеки;
- дотриманням етичних стандартів;
- використанням технологій захисту даних;

- прозорими методами обробки та зберігання інформації.

Лише так можна мінімізувати ризики та зробити використання штучного інтелекту безпечним і відповідальним.

3.2 Обмеження та ризики обробки персональних даних у системах штучного інтелекту

З розвитком штучного інтелекту та машинного навчання постає питання про те, наскільки сучасні алгоритми здатні безпечно та коректно працювати з персональними даними користувачів. Оскільки будь-яка модель, яка намагається імітувати людську поведінку, розпізнавати об’єкти або аналізувати інформацію, потребує великих обсягів даних, питання конфіденційності та законності їхньої обробки стає ключовим. Якщо раніше більшість компаній працювали зі структурованими базами даних — клієнтськими реєстрами, CRM-системами, HR-платформами, фінансовими кабінетами — де кожен користувач прямо надавав згоду на обробку своїх даних, то з появою складних ШІ-систем цей процес став набагато менш прозорим. Дані тепер використовуються не лише в тій формі, у якій вони були зібрані, але й у вигляді похідних характеристик, вторинних ознак та поведінкових профілів, що робить контроль за ними значно складнішим.

У класичній моделі захисту персональних даних закон вимагає, щоб суб’єкт даних був чітко проінформований, для чого, ким і як довго обробляються його дані. Це є фундаментальним принципом, закріпленим і в українському законодавстві, і в GDPR, і в інших міжнародних актах. Проте у випадку штучного інтелекту стає дедалі важче не лише пояснити, як саме модель використовує дані, але й визначити межі тієї інформації, яку система фактично може вивести на основі аналізу. Стає можливим так зване «непряме відновлення інформації» — коли ШІ здатний реконструювати риси, характеристики чи навіть особисті дані людини, які формально не були йому надані.

Одним із найважливіших викликів є принцип цільового використання даних. За законом, суб’єкт має знати, які саме цілі переслідує оператор. Однак у випадку

ШІ цілі використання даних можуть змінюватися вже після тренування моделі. Наприклад, дані соціальних мереж можуть бути використані не лише для формування стрічки новин, але й для створення поведінкових профілів, прогнозування покупок, оцінки психологічних особливостей чи емоційного стану. Все це відбувається поза прямим контролем людини, яка ці дані створила, і часто навіть поза контролем компанії, яка їх збирає. Під час машинного навчання алгоритм може створювати нові зв’язки, які не були передбачені під час збору даних. Це породжує проблему «розширеного профілювання» — коли ШІ здатний формувати додаткові відомості про людину, які вона ніколи не розкривала.

Особливо гостро постає проблема обробки зображень. Фотографії — це один із найбільш чутливих видів персональних даних, оскільки вони містять біометричну інформацію. Згідно з законом, біометричні дані не можуть оброблятися без прямої згоди суб’єкта. Але сучасні моделі розпізнавання облич здатні ідентифікувати людину навіть за незначними фрагментами зображення. Більш того, алгоритми можуть навчитися визначати стать, вік, емоційний стан, етнічну приналежність та навіть потенційні ризики для здоров’я. Таким чином, навіть звичайна фотографія може стати джерелом глибокого аналізу, на який людина не давала згоди. Виходить парадокс: формально фотографія не є персональними даними, якщо не дозволяє однозначно ідентифікувати особу. Але ШІ робить таке ідентифікування можливим, навіть якщо людина цього не підозрювала.

Окремим великим блоком ризиків є можливість витоку даних або несанкціонованого доступу до великих тренувальних масивів. У багатьох випадках ШІ тренується на даних, зібраних з відкритих джерел — форумів, соціальних мереж, блогів, новинарних сайтів. Користувачі не усвідомлюють, що їхні коментарі, фото, публікації та інші дії в мережі можуть перетворитися на елементи тренувального датасету. Крім того, великі корпорації іноді передають дані між підрозділами або дочірніми компаніями, що створює ризики перехресного доступу. Коли тренувальні дані об'єднуються, контроль за джерелами інформації стає майже неможливим.

Однією з найбільших загроз є той факт, що штучний інтелект перетворився на реальну систему масового аналізу інформації. Якщо раніше для того, щоб обробити мільйони фото або текстів, були потрібні великі ресурси та людська праця, то тепер це може зробити один алгоритм за кілька годин. Це створює ризик масового стеження, яке є технічно можливим навіть за мінімальних затрат. Держава, приватні компанії, банки або страхові установи можуть отримувати доступ до надзвичайно детальних поведінкових портретів людей, а отже — впливати на них, прогнозувати дії, маніпулювати рішеннями або відмовляти в послугах.

Ще одним аспектом, що викликає значні побоювання, є те, що сучасні моделі штучного інтелекту фактично є «чорними скриньками». Навіть самі розробники часто не можуть чітко пояснити, за якою логікою модель прийшла до певного рішення. Це означає відсутність прозорості у випадках, коли ШІ використовується для критично важливих рішень — медичних, фінансових, юридичних. Якщо модель відмовляє людині у кредиті, ставить некоректний медичний пріоритет або визнає її поведінку підозрілою, важливо знати, на основі яких даних і яким механізмом було прийняте таке рішення. Проте в багатьох випадках розробники не можуть цього пояснити навіть у принципі — бо алгоритм створює власні внутрішні правила самостійно під час навчання.

Ще складнішою є проблема дискримінації. ШІ може ненавмисно підсилювати упередження, що містяться у тренувальних даних. Якщо більшість даних представляє певну групу людей, алгоритм може навчитися вважати її «нормою», тоді як інші групи будуть вважатися відхиленням. Це вже призвело до відомих скандалів: алгоритми визначення кредитного рейтингу, які занижували оцінку жінкам; системи підбору кадрів, які знижували пріоритет резюме людей певної етнічності; медичні моделі, які гірше прогнозували ризики для людей з темним кольором шкіри, бо були треновані переважно на даних білих пацієнтів. Проблема дискримінації стає дедалі більш актуальною, адже ШІ часто використовується для автоматизованого прийняття рішень без участі людини.

Незважаючи на ці ризики, повністю відмовитися від штучного інтелекту неможливо — він уже став необхідною частиною сучасної цифрової економіки. Тому основне завдання — навчитися правильно керувати ризиками. Одним із ключових принципів є мінімізація даних: необхідно використовувати лише той обсяг персональної інформації, який дійсно потрібен для вирішення конкретної задачі. Якщо ідентифікація не є обов'язковою — дані повинні бути анонімізовані, псевдонімізовані або агреговані. Обмеження доступу до даних, використання криптографічних протоколів, системи контролю доступу та моніторингу — усе це має бути стандартною практикою.

Важливим елементом захисту є прозорість. Компанії повинні чесно пояснювати користувачам, навіщо збирають дані, у які процеси вони будуть залучені, і яку роль у цьому відіграє штучний інтелект. Людина повинна мати можливість зрозуміти і, при необхідності, відмовитися від обробки деяких категорій даних. Прозорість також означає необхідність розкриття того, коли рішення приймає саме ШІ, а не людина. Це дає можливість суб'єкту даних оскаржити рішення, якщо він вважає його помилковим або дискримінаційним.

Таким чином, обробка персональних даних у системах ШІ — це не лише технічне завдання, а й складна етична, юридична та соціальна проблема. Необхідно створити механізми, що гарантують безпеку, конфіденційність і справедливість. Світ стоїть на межі формування нових стандартів захисту інформації, які повинні відображати реалії епохи штучного інтелекту. Лише комплексний підхід — від законодавства до технічних інструментів — здатен забезпечити баланс між розвитком технологій та правами людини.

3.3 Генеративно-змагальні мережі та федеративне навчання

Генеративно-змагальні мережі як інструмент зменшення потреби в персональних даних у системах машинного навчання

Одним із перспективних підходів, що може бути використаний у задачах машинного навчання для зменшення обсягу персональних даних, є застосування

генеративно-змагальних мереж (GAN, Generative Adversarial Networks). Цей клас моделей за останні роки став одним із найдинамічніше розвинених напрямів у сфері штучного інтелекту, оскільки дозволяє створювати нові дані, максимально наближені до реальних.

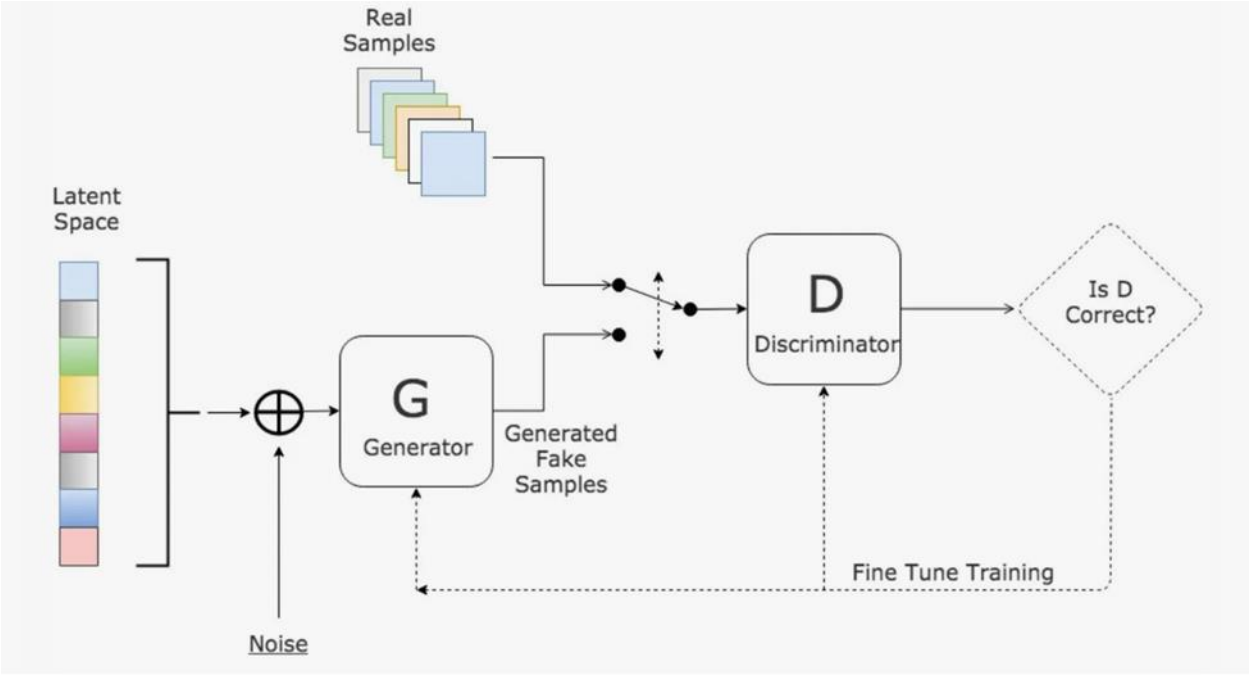


Рис. 3.2 Generative Adversarial Networks

У сучасній екосистемі машинного навчання спостерігається чітка тенденція — пошук методів, які дають змогу досягати високої точності моделей, використовуючи менші обсяги вихідних навчальних даних. Це особливо важливо в умовах посилення вимог щодо конфіденційності, захисту персональної інформації та мінімізації ризиків витоку даних. У цьому контексті GAN відкривають можливість частково замінити або доповнити реальні дані штучно створеними, зберігаючи при цьому статистичні характеристики та структуру вихідного набору.

Сутність методу полягає в тому, що він використовує вихідні (згенеровані) дані для створення нових вхідних даних. Інакше кажучи, модель вчиться на прикладах із реального датасету та поступово формує здатність будувати синтетичні елементи, які відтворюють необхідні ознаки та закономірності. Таким чином, базовий набір даних виступає радше орієнтиром для створення нового контенту, а не єдиним джерелом інформації.

Механізм GAN складається з двох взаємодіючих нейронних мереж — генератора та дискримінатора, які працюють у режимі змагання. Генератор намагається створювати дані, максимально подібні до реальних: зображення, сигнали, текстові фрагменти або інші структуровані об’єкти. Дискримінатор, у свою чергу, «оцінює» ці дані та визначає, чи є вони справжніми, чи згенерованими штучно. У процесі навчання обидві моделі одночасно вдосконалюються: генератор «вчиться обманювати» дискримінатор, а дискримінатор — ставати більш точним у виявленні підробок.

Така взаємодія створює ефект динамічної еволюції. З кожною ітерацією генератор отримує зворотний зв’язок, який дозволяє йому створювати дедалі реалістичніші дані. В кінцевому результаті може утворитися синтетичний набір даних, настільки схожий на реальний, що його важко або неможливо відрізнити. Саме тому GAN широко використовуються в задачах створення фотографій, відео, реконструкції зображень, покращення якості даних, симуляції фізичних процесів та моделювання поведінки.

Попри значні переваги, GAN не позбавлені недоліків. Головна проблема полягає в тому, що для того, щоб генератор і дискримінатор працювали справді ефективно, їм усе одно потрібен достатньо великий початковий набір даних для навчання. Мережа повинна побачити велику кількість прикладів, щоб зрозуміти закономірності та структури, характерні для реальної інформації. Тому GAN не повністю вирішують проблему надлишкового збору даних, але можуть істотно зменшити обсяг персональних даних, необхідних для подальшого функціонування системи.

І все ж головна перевага GAN полягає саме у можливості зниження тиску на використання персональних даних. Якщо алгоритм здатний створити синтетичні зображення або текстові записи, які зберігають статистичні властивості реальних даних, але не містять персональної ідентифікаційної інформації, це дозволяє будувати моделі, не порушуючи приватності та не обробляючи дані конкретних людей. Наприклад, замість реальних фотографій співробітників можна

використовувати синтетичні зображення, які не відтворюють особу, але дозволяють тестувати і тренувати алгоритми розпізнавання.

Крім того, генеративно-змагальні мережі є важливим кроком у напряму розвитку так званих «privacy-preserving AI» — систем, що зберігають конфіденційність. У поєднанні з іншими технологіями, такими як диференційна приватність, гомоморфне шифрування або федеративне навчання, GAN можуть формувати основу для більш безпечних і етичних інтелектуальних систем, де приватність користувачів стає ключовим принципом, а не побічним фактором.

Таким чином, генеративно-змагальні мережі є не лише потужним інструментом сучасного машинного навчання, а й важливим механізмом зменшення необхідності в обробці великих обсягів персональних даних. Попри те, що вони не усувають повністю потребу у вихідних даних, GAN дозволяють суттєво оптимізувати баланс між ефективністю моделі та рівнем захисту приватності, що є критично важливим у сучасних умовах інформаційної безпеки і правового регулювання цифрових технологій.

Федеративне навчання: принципи, можливості та обмеження в контексті захисту персональних даних

Федеративне навчання є одним із найперспективніших підходів до створення систем штучного інтелекту, орієнтованих на збереження приватності користувачів. На відміну від традиційних методів машинного навчання, які передбачають централізований збір великих масивів даних у єдине сховище, федеративне навчання дозволяє моделям удосконалюватися без необхідності переміщувати персональні дані за межі пристрою або локальної системи, де вони були створені.

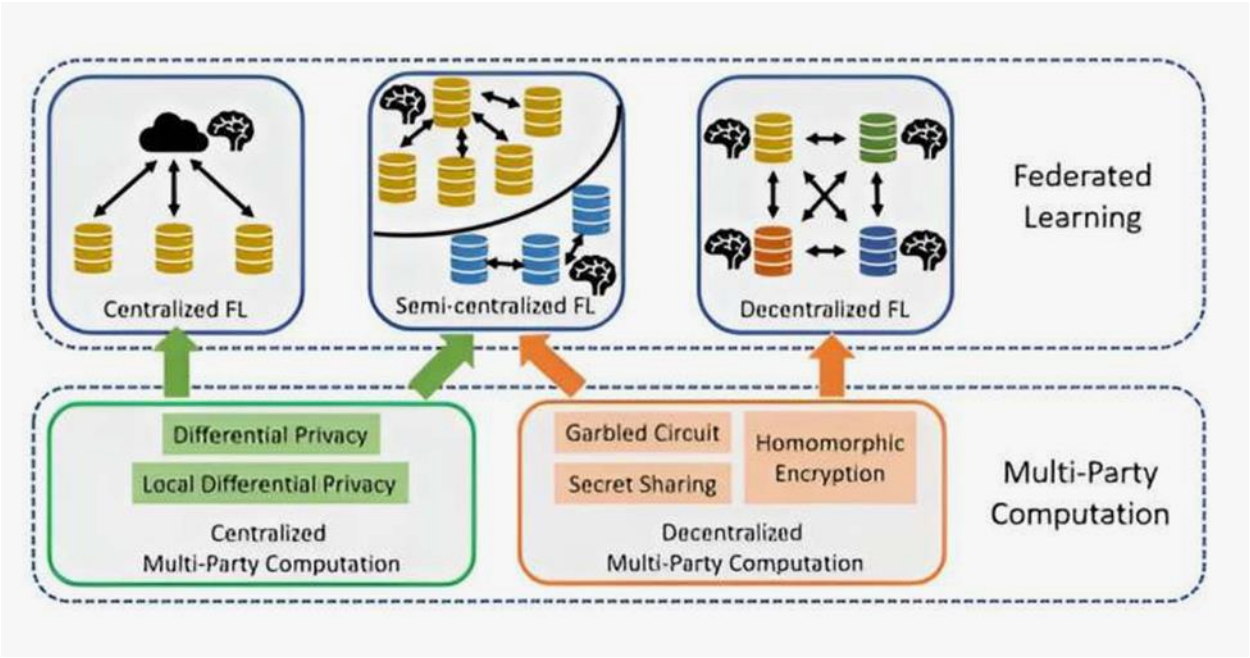


Рис. 3.3 Принцип федеративного навчання

Основна ідея полягає в тому, що дані ніколи не покидають первинне джерело. Вони не передаються до центрального серверу, не копіюються у хмару і не стають частиною спільної бази даних. Замість цього процес відбувається інакше: модель штучного інтелекту «приходить» до користувача, навчається безпосередньо на його локальних даних, а потім повертається до центрального сервера у вигляді математичних оновлень — змін ваг і параметрів. Таким чином, у систему надходить не персональна інформація, а лише статистичні характеристики, які допомагають покращувати глобальну модель.

Цей підхід має величезне значення в умовах зростання кількості регуляцій щодо захисту персональних даних, оскільки дозволяє використовувати чутливу інформацію — медичні записи, дані поведінки, історію пошуку, фото чи голосові зразки — без ризику витоку або неправомірного доступу. Федеративне навчання дає можливість створювати високоточні алгоритми, зберігаючи при цьому конфіденційність, оскільки персональні дані залишаються виключно у власника, а в процесі навчання передаються лише анонімізовані параметри.

Технічно федеративне навчання передбачає наявність великої кількості вузлів — смартфонів, IoT-пристроїв, корпоративних робочих станцій — на яких розміщуються локальні копії моделі. Кожен вузол виконує цикл навчання, після

чого результати локального обчислення передаються централізованому агрегатору. Аггрегатор об’єднує ці локальні оновлення в одну спільну глобальну модель, яка стає точнішою після кожної ітерації. Такий цикл може повторюватися тисячі разів, забезпечуючи поступове покращення якості алгоритму без створення централізованої бази персональних даних.

Попри значні переваги, федеративне навчання не є ідеальним і має власні обмеження. Моделі, що тренуються на локальних пристроях, часто стикаються з проблемами, які відсутні в централізованих системах. Наприклад, локальні дані можуть бути неповними, несбалансованими або надто різнорідними, що ускладнює навчання. Пристрої користувачів можуть мати різну обчислювальну потужність, різну якість даних, різні структури інформації. У деяких випадках локальні набори даних можуть бути настільки обмеженими, що модель отримує недостатньо інформації для повноцінного навчання. Це робить процес більш фрагментованим та потребує складних алгоритмів корекції, які дозволяють узгоджувати результати з різних джерел.

Крім того, локальне навчання вимагає значних ресурсів пристрою: процесорного часу, оперативної пам’яті, енергії. Наприклад, смартфон, на якому виконується цикл федеративного навчання, може швидше розряджатися, нагріватися або виконувати завдання повільніше. Це накладає обмеження на частоту навчання та обсяг моделей, які можна запускати на кожному вузлі.

Ще одним важливим викликом є безпека локальних оновлень. Хоча персональні дані не передаються назовні, можливість маніпулювання параметрами моделі або втручання в процес генерації оновлень не виключена. Зловмисник може спробувати підмінити локальні зміни або ввести шкідливі патерни в глобальну модель. Тому федеративне навчання передбачає додаткові механізми захисту: криптографічні протоколи, методи верифікації підписів, контроль достовірності оновлень та алгоритми агрегування, здатні виявляти аномальні поведінкові патерни.

Попри всі ці складнощі, федеративне навчання відкриває нові горизонти для створення безпечних систем штучного інтелекту, які поважають конфіденційність

користувачів. Воно особливо корисне у сферах із підвищеними вимогами до захисту персональних даних — медицині, банківській справі, телекомунікаціях, промислових системах. Технологія забезпечує унікальний баланс між точністю моделі та приватністю, дозволяючи досягати високих результатів там, де централізовані методи були б небезпечними або навіть незаконними.

Таким чином, федеративне навчання є важливим кроком у розвитку етичного штучного інтелекту. Воно надає можливість працювати з конфіденційними даними, не порушуючи приватності, та створювати алгоритми, здатні адаптуватися до реальних умов, залишаючись при цьому безпечними для користувачів. Хоча моделі, навчені таким способом, можуть мати певні технічні обмеження, сам принцип децентралізації є ключем до майбутнього, де штучний інтелект буде розвиватися без шкоди для особистої інформації.

4 ЗАХИСТ ДАНИХ НА СЕРВЕРНОМУ РІВНІ

4.1 Принцип Zero-Trust

Модель Zero Trust: концепція, принципи та практичні аспекти впровадження

У сучасних умовах цифрової трансформації, коли корпоративні мережі стрімко ускладнюються, а кількість кіберзагроз зростає в геометричній прогресії, виникає потреба у новому підході до організації безпеки. Однією з найбільш ефективних та широко обговорюваних концепцій останнього десятиліття стала модель Zero Trust, або «нульової довіри». Її головний принцип максимально простий та жорсткий: не довіряй нікому і нічому за замовчуванням — перевіряй кожного і завжди.

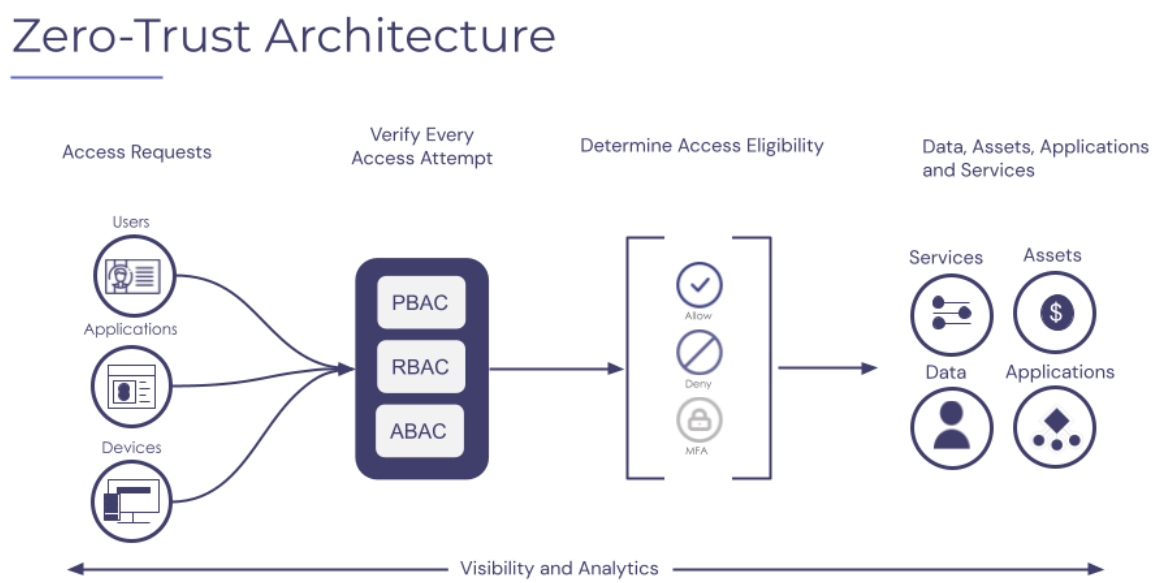


Рис. 4.1 Архітектура Zero-Trust

На відміну від традиційних моделей, де ключовим елементом вважався периметр корпоративної мережі, а внутрішні системи — «зоною довіри», Zero Trust повністю нівелює будь-які припущення щодо безпеки внутрішніх ресурсів. Вона виходить з того, що мережа вже скомпрометована або може бути скомпрометована

в будь-який момент, тому кожен запит на доступ має перевірятися незалежно від того, звідки він надходить — ззовні чи зсередини організації.

Таким чином, Zero Trust руйнує класичний принцип «trusted inside / untrusted outside» і впроваджує нову парадигму — “always verify, never trust”.

Аудит та інвентаризація активів — перший і найважливіший етап Zero Trust

Початок впровадження Zero Trust — це ґрунтовний аудит усієї IT-інфраструктури. Без розуміння того, які саме ресурси потребують захисту, модель неможливо впровадити повноцінно. Під ресурсами маються на увазі не лише фізичні сервери, а й:

- бази даних та інформаційні сховища;
- файли, архіви, резервні копії;
- хмарні сервіси та SaaS-додатки;
- бізнес-додатки, API та мікросервіси;
- мережеве обладнання;
- цифрові робочі місця співробітників;
- критичні компоненти бізнес-процесів.

Особливої уваги заслуговують дані, оскільки саме вони є найціннішим активом і найчастіше стають мішенню для атак. Правильна класифікація даних визначає, які саме політики безпеки повинні застосовуватися до того чи іншого ресурсу.

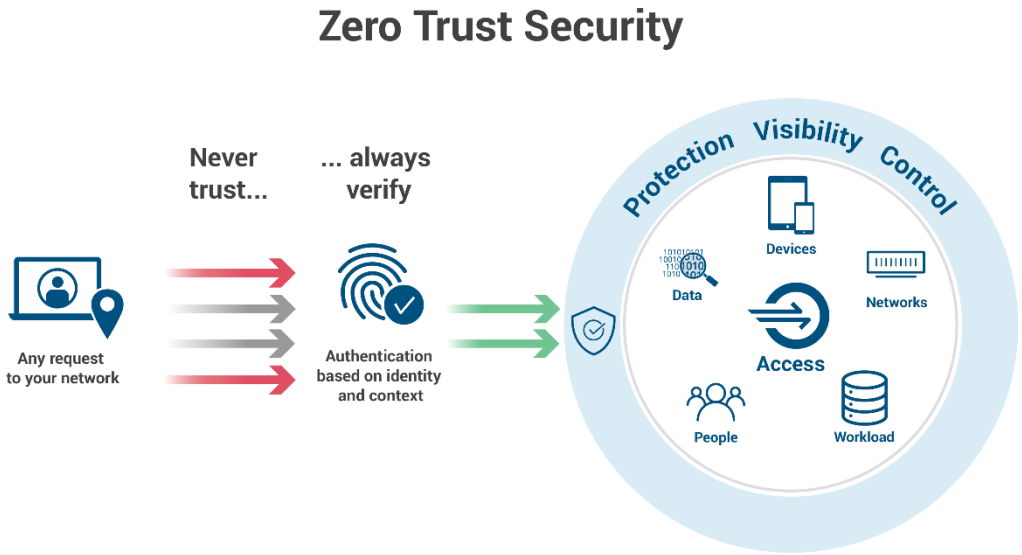


Рис. 4.2 Ключові компоненти моделі Zero Trust: ідентифікація, мінімальні привілеї, сегментація мережі, постійний моніторинг

Для якісної інвентаризації потрібно:

— визначити власників кожного активу;

— з’ясувати, яку бізнес-функцію він виконує;

— оцінити критичність активу для бізнесу;

— визначити, яким чином доступ до нього повинен бути контрольований.

Ідея полягає в тому, що інфраструктура не може вважатися безпечною, якщо компанія не має чіткого розуміння того, що саме слід захищати.

Перегляд політик доступу та принцип мінімальних привілеїв

Zero Trust передбачає жорстке регулювання доступу. Користувачі отримують лише ті права, які необхідні їм для виконання робочих обов’язків — не більше, не менше. Це називається принципом мінімальних привілеїв (Least Privilege).

Його практична реалізація включає:

- впровадження RBAC (керування доступом на основі ролей),
- обмеження дій відповідно до реальних функцій співробітника;
- регулярний перегляд прав доступу;
- автоматичне відкликання прав у разі зміни ролі або звільнення співробітника;
- суворий контроль над адміністративними обліковими записами.

Zero Trust передбачає, що будь-який доступ повинен бути підтверджений через IAM (Identity and Access Management), а всі критичні операції — захищені через MFA (Multi-Factor Authentication). Багатофакторна аутентифікація є обов'язковою не лише для керівників або адміністративних користувачів, а для всіх, хто отримує доступ до конфіденційних даних або працює поза периметром компанії.

Сегментація мережі як ключ до обмеження поширення атак

У моделі Zero Trust необхідно створювати розподілену та багаторівневу мережеву архітектуру. Мета сегментації — не допустити, щоб компрометація однієї ділянки інфраструктури автоматично відкривала шлях до інших ресурсів.

Правильно побудована сегментація передбачає:

— розділення корпоративної мережі на ізольовані сегменти;

— окремий доступ для гостьових, IoT, BYOD-пристроїв;

— використання мікросегментації для критичних сервісів;

— застосування політик «deny by default», що блокують будь-який неавторизований трафік.

Сегментація є фундаментом Zero Trust, адже вона зупиняє горизонтальне переміщення загроз — one of the key attack vectors у сучасних інцидентах.

Моніторинг і безперервна верифікація дій користувачів та пристроїв

Zero Trust виходить із того, що навіть користувачі з валідними обліковими даними можуть бути скомпрометовані. Тому перевірка не завершується після успішного входу — вона триває постійно протягом усієї роботи користувача.

Щоб це забезпечити, впроваджуються:

SIEM-системи — централізований збір логів, кореляція подій, аналіз поведінки в реальному часі.

SOC — оперативний центр кіберзахисту, що аналізує інциденти 24/7.

EDR/XDR — інструменти глибокого захисту кінцевих точок.

UEBA — аналітика поведінки користувачів і пристроїв, що використовує ШІ для виявлення аномалій.

SOAR — автоматизація реагування на інциденти, прискорення ухвалення рішень та мінімізація людського фактора.

Разом ці інструменти створюють екосистему безперервного моніторингу, без якого Zero Trust неможливий у принципі.

Контроль пристроїв та підхід «довіра через перевірку»

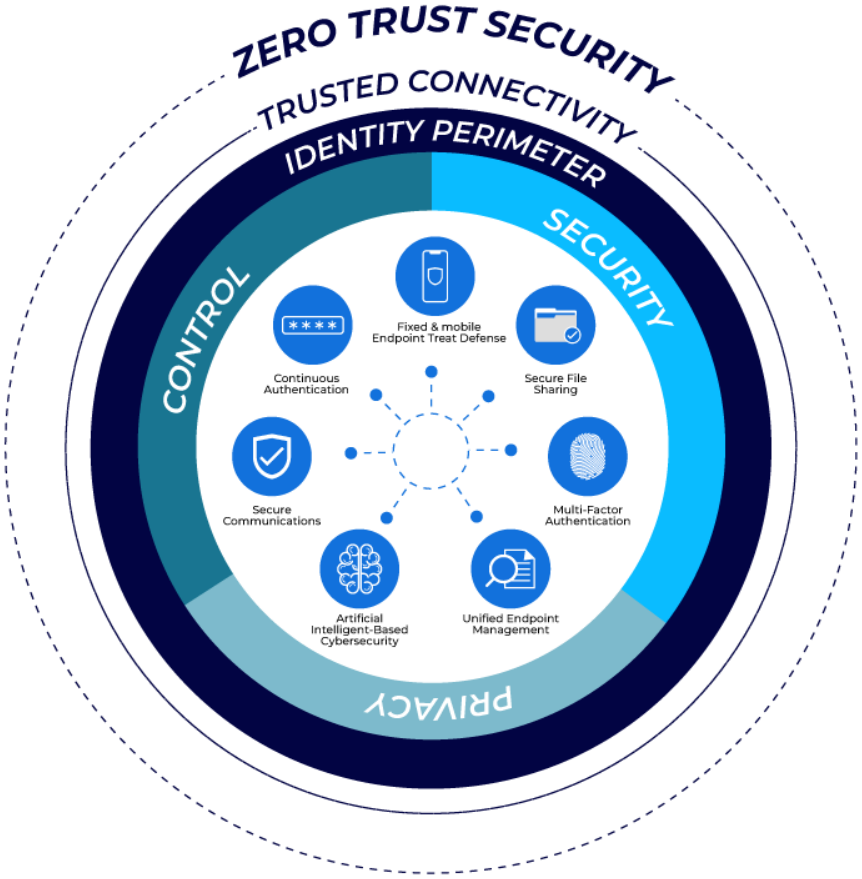


Рис. 4.3 Концепт доступу по Zero Trust: користувач або пристрій запитує доступ — перевірка контексту, статусу, політики — і лише потім дозвіл або блокування

У Zero Trust будь-який пристрій — навіть корпоративний ноутбук — розглядається як потенційна загроза. Перш ніж надати доступ до мережі, система повинна переконатися, що пристрій відповідає вимогам безпеки.

Для цього використовують:

MDM/EMM — керування мобільними пристроями, встановлення політик безпеки, контроль шифрування.

BYOD-політики — правила роботи співробітників із власних ноутбуків або смартфонів.

NAC-рішення — перевірка стану пристрою перед підключенням до мережі (оновлення, антивірус, шифрування диску).

Сегментацію доступу BYOD — поміщення особистих пристроїв у окремі, обмежені мережеві зони.

Це дозволяє уникнути ситуацій, коли заражений або незахищений пристрій стає точкою входу для зловмисника.

Модель Zero Trust — це не окремий інструмент і не продукт, а комплексна стратегія, яка охоплює всі рівні корпоративної безпеки. Її сила — у тотальній перевірці, постійному контролі та відсутності будь-яких довірчих зон.

Zero Trust будується на:

— глибокому розумінні власних активів;

— жорсткому контролі доступу;

— багаторівневому моніторингу;

— сегментації;

— перевірці кожного пристрою;

— мінімальних привілеях;

— автоматизації реагування на загрози.

Це робить модель однією з найефективніших стратегій протидії сучасним атакам, у яких зловмисники все частіше націлюються не на периметр, а на внутрішні елементи інфраструктури.

4.2 Практики для внутрішнього захисту серверів та даних

Сучасні кіберзагрози вже давно виходять за межі зовнішніх атак. Одним із найнебезпечніших сценаріїв стає внутрішній порушник — людина, яка має легальний доступ до системи, або зловмисник, що отримав контроль над її обліковими даними. Саме тому компанії впроваджують додаткові механізми контролю, моніторингу та обмеження привілеїв. Нижче наведено комплекс із

десяти дієвих підходів, які значно підвищують рівень внутрішньої безпеки корпоративної інфраструктури.

1. Створення «пасток» для моніторингу активності співробітників

Суть:

Одним із найдієвіших способів виявлення несанкціонованих дій усередині компанії є створення спеціальних «пасток» — фіктивних файлів або директорій, що імітують цінні корпоративні дані. Це можуть бути файли з такими назвами, що привертають увагу: *«Звіт_фінанси_2024.xlsx»*, *«паролі.txt»*, *«зарплати_топ_менеджменту.docx»*, *«контракти_конфіденційно.pdf»*.

Будь-яка особа, яка свідомо або випадково відкриє подібний файл, автоматично викликає підозру, адже нормальний співробітник зазвичай не має потреби переглядати документи з такими «гучними» назвами. Такий прийом працює за принципом honeypot — тобто спеціально залишеної «приманки», завдяки якій можна виявити спроби доступу, що виходять за рамки службової необхідності.

Розширена практика впровадження пасток:

Для того щоб такий підхід був ефективним, важливо не просто створити фіктивні файли, а й забезпечити постійний моніторинг будь-яких дій із ними. У Linux для цього використовують інструменти на кшталт **auditd**, **inotify**, а також інтеграцію з корпоративними системами моніторингу, включно з SIEM.

Моніторинг дозволяє автоматично:

- фіксувати факт відкриття або спроби відкриття фіктивного файлу;
- визначати користувача та час доступу;
- відстежувати вироблені подальші дії — копіювання, друк, пересилання;
- визначати, чи була дія одноразовою випадковістю, чи має ознаки систематичної цікавості до конфіденційних даних.

Переваги для виявлення внутрішніх загроз:

1. **Виявлення надмірної цікавості співробітників.**

   Навіть якщо особа не має зловмисних намірів, але регулярно намагається переглядати чутливі файли, це сигнал для служби безпеки.

2. **Виявлення компрометованих акаунтів.**

Якщо доступ здійснює користувач, який зазвичай не працює з такими типами інформації, це може означати, що його облікові дані були викрадені.

3. **Виявлення зловмисника, що проник у мережу.**

   Зловмисники, отримавши доступ до внутрішньої мережі компанії, часто одразу починають перегляд конфіденційних файлів. Саме фальшиві документи з «гучними» назвами найчастіше стають їх першими спробами доступу.

4. **Раннє реагування.**

   Система може автоматично сповіщати IT-безпеку, SOC чи відповідальних адміністраторів, що дозволяє зупинити загрозу ще до того, як вона переросте в інцидент.

Поглиблені методи інтеграції пасток:

- Створення цілих фіктивних папок або навіть псевдокористувацьких директорій.
- Впровадження прихованих метаданих, які також реагують на відкриття.
- Налаштування пасток під конкретні відділи (фінанси, HR, закупівлі).
- Використання різних пасток для різних ролей, щоб визначати специфічні сценарії доступу.
- Застосування пасток як частини загальної стратегії insider threat detection.

Перевага підходу:

Такі пастки працюють непомітно, не впливають на роботу співробітників і водночас дають змогу виявляти аномальну поведінку, яку неможливо відстежити стандартними методами. Це один із найефективніших інструментів протидії внутрішнім загрозам, оскільки він дозволяє не лише фіксувати вже скоєні дії, а й попереджати потенційні інциденти, коли співробітник або порушник лише починає проявляти інтерес до заборонених областей системи.

2. Поділ журналів для контролю дій із підвищеними привілеями

Суть:

Одним із найважливіших елементів захисту корпоративної інфраструктури є чітке та системне розмежування журналів подій. У більшості великих організацій

за добу генеруються мільйони подій: це можуть бути звичайні входи користувачів, виконання базових програм, системні повідомлення, робота сервісів та інші рутинні дії. На цьому фоні дії із підвищеними привілеями — використання команд *sudo*, *su*, зміна системних конфігурацій, запуск скриптів від root або domain admin — можуть легко загубитися.

Щоб цього не допустити, журнали подій потрібно поділяти на дві категорії: звичайні логи та логи привілейованих операцій. Це дозволяє не лише пришвидшити аналіз інцидентів, а й значно спростити роботу аналітикам SOC та адміністраторам безпеки.

Розширена практика впровадження поділу журналів

Для того щоб система моніторингу була ефективною, важливо грамотно структурувати журнали дій таким чином, щоб події, потенційно небезпечні для компанії, зберігалися окремо. До таких подій належать:

- виконання команд із підвищеними правами (*sudo*, *su*, psexec, runas тощо);
- зміна системних налаштувань або конфігурацій серверів;
- модифікація політик безпеки (наприклад, у Active Directory або через групові політики);
- запуск або зупинка критичних сервісів;
- змінення прав доступу до файлів, директорій або системних об’єктів;
- дії, які можуть вплинути на цілісність або доступність системи.

У Linux це можна реалізувати за допомогою **syslog**, **rsyslog**, **journalctl**, де окремі файли журналів призначаються під певні категорії команд. Наприклад:

- */var/log/sudo.log* — для всіх sudo-операцій;
- */var/log/root-actions.log* — для дій користувача root;
- */var/log/security-events.log* — для змін у системних політиках;
- */var/log/auth-priv.log* — для приватних подій авторизації.

Також важливо враховувати, що в середовищах із тисячами робочих станцій та серверів централізація логів є фактично обов’язковою.

Централізоване зберігання журналів

У сучасних корпоративних інфраструктурах усі привілейовані логи потрібно відправляти до спеціалізованих систем збору та аналізу журналів:

- **ELK Stack (Elasticsearch, Logstash, Kibana)**
- **Splunk**
- **Graylog**
- **SIEM-рішення (QRadar, ArcSight, Sentinel, Wazuh)**

Централізація дозволяє:

- зберігати журнали у захищеному середовищі, де їх неможливо видалити або підробити;
- аналізувати мільйони подій у реальному часі;
- швидко будувати кореляції між подіями з різних систем;
- створювати автоматизовані правила виявлення аномалій;
- вмикати тригери на підозрілі дії.

Що саме варто моніторити в журналах привілейованих дій

Для забезпечення ефективного контролю слід налаштувати сповіщення та аналітичні дашборди для виявлення таких подій:

1. **Нестандартні або підозрілі команди.**
   Наприклад, масове видалення файлів, зміна системних конфігурацій, маніпуляції з ACL або спроби доступу до заборонених директорій.
2. **Різке збільшення кількості sudo-запитів.**
   Це може вказувати на підбір паролів або автоматизований скрипт, який намагається отримати доступ.
3. **Помилки входу під привілейованими обліковими записами.**
   Серія невдалих спроб увійти під root/admin — завжди вагомий сигнал для реагування.
4. **Запуск небезпечних скриптів чи програм.**
   Наприклад, сценарії, що змінюють системні параметри або маніпулюють мережевими протоколами.
5. **Дії поза робочим часом.**

Якщо адміністратор вчиняє активні дії вночі або під час вихідних — це потребує аналізу.

6. **Зміни політик безпеки.**

Перевизначення ACL, налаштувань firewall, GPO або групових політик AD.

Переваги поділу журналів у контексті безпеки

Такий підхід забезпечує:

- **швидше виявлення інцидентів**, оскільки критичні події не губляться серед загального шуму;
- **зменшення навантаження на SOC**, адже з'являється можливість відсікати неважливі дані;
- **кращий контроль за адміністраторами**, включно з привілейованими обліковими записами;
- **простішу побудову аналітики та кореляційних правил**;
- **запобігання ескалації привілеїв**;
- **захист від insider threat**, тобто внутрішніх зловмисників;

3. Тимчасові привілеї (Just-In-Time Access, JIT)

Суть:

У сучасних системах безпеки доступ із постійними адміністративними правами вважається одним із найнебезпечніших факторів ризику. Будь-який обліковий запис, що має привілеї *Admin*, *Domain Admin*, *root* або інші високі рівні доступу, у разі компрометації становить критичну загрозу для всієї IT-інфраструктури.

Концепція Just-In-Time Access (JIT) передбачає повну відмову від постійних адмінських прав. Замінює їх механізм тимчасового доступу: привілеї надаються лише на час конкретної задачі — наприклад, на встановлення оновлення, зміну налаштувань сервера, усунення аварії або проведення технічних робіт. Після завершення задачі доступ автоматично відкликається, не залишаючи жодного зайвого вікна можливостей.

Такий підхід різко зменшує площу атаки, унеможливлює зловживання привілеями та фактично ліквідує один із найпоширеніших сценаріїв компрометації

— отримання повного контролю над інфраструктурою через один зламаний обліковий запис.

Розширена практика реалізації тимчасових привілеїв

У багатьох корпоративних середовищах JIT впроваджується через системи класу **PAM (Privileged Access Management)**, такі як:

- **CyberArk**
- **BeyondTrust**
- **Wallix**
- **One Identity Safeguard**
- **Thycotic / Delinea**

Системи PAM дозволяють не лише видавати тимчасові привілеї, а й забезпечують повний контроль над їх використанням. Нижче наведено ключові можливості:

1. Видача прав на обмежений час

Адміністратор або інженер може отримати тимчасовий доступ, який діє від 15 хвилин до декількох годин (частіше 30–120 хв). Після завершення часу привілеї автоматично відкликаються.

2. Логування кожної дії

Усі дії привілейованих користувачів:

- записуються до журналів,
- можуть дублюватися у SIEM,
- інколи записуються як повноцінне відео сеансу (session recording).

Це дозволяє відтворити роботу адміністратора покадрово — корисно під час розслідувань інцидентів або аудитів.

3. Механізм погодження (approval workflow)

Доступ надається лише після підтвердження:

- іншого адміністратора,
- керівника підрозділу,
- чергового спеціаліста SOC.

Це створює подвійний контроль і унеможливлює несанкціоноване підвищення власних привілеїв користувачем.

4. Автоматичне завершення доступу

Як тільки задача виконана — користувач виходить із сесії або завершується робота сервера — система автоматично скидає привілеї.
Якщо ж користувач забув вийти або сесію було «покинуто», PAM самостійно розриває з'єднання.

5. Динамічна видача облікових даних

У деяких системах PAM можна не видавати пароль адміністратору взагалі — система сама входить на сервер від його імені.
Користувач навіть не бачить пароля, що виключає його можливість використати його поза офіційними системами.

JEA (Just Enough Administration) — мінімально необхідні привілеї

У Windows-середовищі додатково використовується концепція **Just Enough Administration (JEA)**.

Вона дозволяє призначати користувачеві *не весь набір команд*, який доступний адміністратору, а лише ті, що потрібні для конкретної дії.

Приклади застосування JEA:

- інженеру техпідтримки дають право лише *перезавантажувати сервер*, але не змінювати конфігурацію;
- адміністратор додатків може лише *встановлювати оновлення*, але не має доступу до реєстру або політик безпеки;
- черговий інженер може *переглядати журнали*, але не може очищати їх або змінювати;
- спеціаліст служби підтримки отримує доступ до *локальних користувачів*, але не до доменної структури.

Це дозволяє максимально точно обмежити діяльність кожного користувача, різко зменшуючи потенційну шкоду від помилок або зловмисних дій.

Переваги JIT та JEA для корпоративної безпеки

1. **Мінімізація ризику компрометації критичних облікових записів.** Жоден акаунт не має постійних адмін-повноважень.
2. **Зменшення площі атаки.**

Навіть якщо пароль украдено — доступ буде обмеженим або взагалі відсутнім.

3. **Повний контроль і аудит.**

   Усі привілейовані дії документуються.

4. **Захист від insider threat.**

   Постійні адмін-акаунти часто стають інструментом зловмисних співробітників.

5. **Прозорість та відповідальність.**

   Легко визначити, хто виконав дію, коли, чому і з яким дозволом.

6. **Сумісність із Zero Trust.**

   JIT є одним із ключових компонентів архітектури «нульової довіри».

4. Регулярна ротація ключів і паролів

Суть:

Регулярне оновлення ключів доступу, службових паролів та інших секретів є одним із базових принципів кібербезпеки. Мета ротації — запобігти довготривалому існуванню критичних секретів, які можуть бути скомпрометовані, викрадені, перехоплені або ненавмисно розголошені співробітниками. Особливо це стосується паролів системних користувачів, сервісних облікових записів, доступів до баз даних, API-токенів, SSH-ключів і ключів шифрування.

Будь-який секрет, який не змінювався роками, становить серйозний ризик — достатньо одного інциденту (фішинг, витік бази, зараження ПК співробітника, помилки конфігурації), щоб зловмисник отримав стабільний доступ до внутрішніх систем. Саме регулярна ротація секретів унеможливлює тривале використання викрадених даних.

Розширена практика: сучасний підхід до ротації секретів

У минулому вважалося, що найкращий спосіб забезпечити безпеку — змушувати співробітників часто змінювати паролі, наприклад кожні 30 або 60 днів.

Проте досвід показав, що:

- **часті зміни паролів знижують безпеку**, оскільки користувачі починають обирати прості, передбачувані або схожі паролі;

- співробітники нерідко записують нові паролі на папірцях, нотатках або в незахищених файлах;
- складні правила (великі/малі літери, спецсимволи, цифри) підштовхують до створення шаблонних паролів (*Qwerty123!*, *Winter2024!*, *P@ssw0rd*).

Ось основні аспекти сучасної практики:

1. Довгі, стійкі паролі для користувачів — замість частих змін

Пароль довжиною 14–20 символів, створений як випадковий набір букв і цифр або як довга фраза, набагато стійкіший до злому, ніж складний, але короткий пароль.

Приклад:

- *gjregfqntdcthdthvjkk* — пароль, який важко зламати, але легко запам’ятати.
- Натомість *P@ssW0rd!* — надзвичайно слабкий, попри «складність».

Золоті правила сучасної політики паролів:

- мінімальна довжина — **12–16 символів**;
- допускаються спеціальні символи, але вони не обов’язкові;
- заборонені очікувані патерни (місяці, роки, імена, клавіатурні послідовності);
- пароль не змінюється регулярно без необхідності.

2. Автоматизована ротація ключів і секретів у сервісах

На відміну від звичайних співробітників, сервісні облікові записи та машинні ключі повинні обертатися автоматично і часто — іноді щодня або навіть щогодини, залежно від критичності сервісу.

Для цього використовують спеціальні платформи управління секретами:

- **HashiCorp Vault**
- **CyberArk**
- **AWS Secrets Manager**
- **Azure Key Vault**
- **GCP Secret Manager**

Ці системи дозволяють:

- автоматично змінювати ключі доступу;
- замінювати API-токени без зупинки сервісів;

- обертати пароль сервісного акаунта без участі людини;
- здійснювати аудит кожної операції з секретами;
- шифрувати секрети як у зберіганні, так і під час передавання.

Таким чином, навіть якщо ключ потрапить до зловмисника, його життєвий цикл становитиме години або дні, а не роки.

3. Перехід до паролbless та FIDO2-токенів

Одним із найефективніших трендів сучасної безпеки є повна відмова від традиційних паролів.

Використання **FIDO2-токенів**, апаратної аутентифікації або біометрії практично виключає можливість:

- фішингу;
- перехоплення пароля;
- підбору або перебору;
- повторного використання скомпрометованих даних.

FIDO2 також забезпечує прив'язку пристрою до конкретного домену, що ускладнює атаки людини посередині (MITM).

4. Перевірка на скомпрометованість: Have I Been Pwned та Lithnet

Навіть найкращий пароль втрачає значення, якщо він уже був у відкритому доступі після витоку бази даних.

Тому ключова частина політики безпеки — регулярна перевірка паролів через:

- **Have I Been Pwned (HIBP)**
- **Lithnet Password Protection** (для Windows середовища)

Ці системи можуть:

- перевіряти паролі під час створення та зміни;
- блокувати паролі, що вже з'являлися у витоках;
- забезпечувати додатковий захист без зниження зручності користувача.

Переваги регулярної ротації секретів

1. Унеможливлює довготривале використання викрадених даних.
2. Зменшує вплив внутрішніх та зовнішніх інцидентів.
3. Захищає автоматизовані системи, які часто забувають оновлювати ключі.

4. Підвищує загальний рівень кібергігієни організації.
5. Допомагає відповідати нормативним вимогам (ISO 27001, NIST, GDPR).
6. Створює стійкішу інфраструктуру, де одиничний витік не є катастрофою.

ВИСНОВКИ

У ході дослідження теми захисту персональних даних у мережах NGN було встановлено, що сучасні телекомунікаційні системи зазнають трансформацій не лише на рівні технологій, а й у сфері вимог до інформаційної безпеки. Еволюція від аналогових 1G до цифрових 2G, широкосмугових 4G та інтелектуальних 5G уже продемонструвала, що зі зростанням швидкості передачі даних, збільшенням кількості підключених пристроїв та поглибленням інтеграції з IoT і хмарними платформами, пропорційно зростає і кількість кіберзагроз. Очікуване впровадження мереж 6G та перехід до концепції Internet of Everything роблять питання захисту персональних даних ще більш актуальним, адже обсяг інформації, що збирається, обробляється та аналізується, набуває безпрецедентних масштабів.

Мережі NGN, як уніфікована інфраструктура нового покоління, поєднують у собі мобільні, стаціонарні, оптичні, бездротові, супутникові та підводні сегменти. Ця гетерогенність створює складність із точки зору безпеки, адже персональні дані можуть передаватися через різні технологічні домени, що мають свої уразливості. У роботі було визначено, що NGN повинні забезпечувати наскрізний захист на всіх рівнях – від фізичного та мережевого до транспортного й прикладного. Компоненти інфраструктури, такі як IP-телефонія, VoIP-сервіси, SIP-трафік та мобільні пристрої, потребують посиленого контролю, оскільки саме вони часто стають ціллю атак, включаючи перехоплення даних, несанкціонований доступ, DDoS, фрод та маніпуляції з маршрутизацією.

Окреме значення займає роль Session Border Controller (SBC) у захисті VoIP-інфраструктури. Розглянуті механізми підтвердили, що SBC є критичним елементом NGN, оскільки він приховує топологію мережі, контролює доступ, фільтрує трафік, запобігає проникненню через VoIP-канали та виявляє атаки завдяки IDS-модулю. Впровадження тимчасових привілеїв (JIT), мінімально достатньої адміністрації (JEA), журналювання дій із підвищеними правами, ротації ключів, сегментації мережі та постійного моніторингу дозволяє суттєво зменшити ризики компрометації персональних даних у NGN-середовищі.

Особливу увагу у роботі було приділено питанням обробки персональних даних у системах штучного інтелекту, що стають невід'ємною частиною NGN. Показано, що ІІ працює на основі великих масивів інформації, і саме це створює ризики, пов'язані з вторинною обробкою, побічними витоками, реконсрукцією особистості та несанкціонованим аналізом даних. Можливі ризики включають не лише порушення приватності, а й дискримінацію, неправильні управлінські рішення та зловживання з боку організацій або зловмисників. Водночас такі методи, як федеративне навчання та генеративно-змагальні мережі, дозволяють зменшити обсяг персональних даних, необхідних для навчання моделей, що робить використання ІІ у NGN більш безпечним.

Проведений аналіз довів, що традиційні механізми захисту більше не відповідають вимогам NGN. Саме тому концепція Zero Trust була визначена як ключова для захисту персональних даних у мережах нового покоління. Її принципи — постійна перевірка, мінімальні привілеї, сегментація, контроль поведінки, моніторинг у реальному часі, автоматична ізоляція загроз — забезпечують багатоетапну й адаптивну оборону. Завдяки поєднанню Zero Trust, PAM, SIEM, SOAR, UEBA, NAC та інших рішень створюється інтегрована система захисту, яка може протистояти як зовнішнім, так і внутрішнім загрозам.

Підсумовуючи, можна стверджувати, що NGN формує нове покоління комунікацій, у якому захист персональних даних стає не просто важливим компонентом — він є фундаментом функціонування самої мережі. Безпека має бути багаторівневою, проактивною та орієнтованою на постійний моніторинг, використання штучного інтелекту, аналіз поведінки та жорстке управління доступом. Лише гармонійне поєднання технічних засобів, сучасних криптографічних підходів, організаційних політик та адаптивних моделей захисту здатне забезпечити надійний захист персональних даних у складній і динамічній екосистемі мереж NGN.

ПЕРЕЛІК ПОСИЛАНЬ

1. Петренко О. М. Методи захисту персональних даних у цифровому середовищі : монографія. Київ : Наук. думка, 2021. 248 с.
2. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: правове регулювання та практичні аспекти : наук.-практ. посібник. Київ : К.І.С., 2015. 220 с.
3. Бем М. В., Городиський І. М. Стандарти захисту персональних даних в соціальній сфері : практичний посібник. Львів, 2018. 110 с.
4. Посібник з європейського права у сфері захисту персональних даних. Київ : К.І.С., 2015. 216 с.
5. Handbook on European Data Protection Law. 2018 edition. Luxembourg : Publications Office of the European Union, 2018. 372 p.
6. Voigt P., von dem Bussche A. The EU General Data Protection Regulation (GDPR): A Practical Guide. 2nd ed. Cham : Springer, 2021. 383 p.
7. Kuner C., Bygrave L. A., Docksey C. The EU General Data Protection Regulation (GDPR): A Commentary. Oxford : Oxford University Press, 2020. 1504 p.
8. Ustaran E. European Data Protection. 3rd ed. Portsmouth : IAPP, 2023.
9. Massey S. R. Ultimate GDPR Practitioner Guide: Demystifying Privacy & Data Protection. 2nd ed. Ely : IT Governance Publishing, 2019.
10. Гуржій Т. О., Петрицький А. Л. Правовий захист персональних даних : монографія. Київ : КНТЕУ, 2019. 216 с.
11. Врублевська-Місюна К. М., Тичина В. П. Міжнародно-правові стандарти захисту інформації про особу // Науковий вісник Ужгородського нац. ун-ту. Серія: Право. 2022. Вип. 74(2).
12. Биков О. М. Захист персональних даних у сучасному інформаційному суспільстві // Юридичний вісник «КРОК». 2024. № 3.
13. Михайлик А. С. Міжнародно-правові стандарти у сфері захисту персональних даних працівників. 2022.

14. Землянська О. В., Праховнік Н. А., Ковтун А. І., Ковтун М. А. Безпека в Інтернеті та захист персональних даних. Київ : КПІ ім. Ігоря Сікорського, 2022.
15. Захист персональних даних в умовах воєнного стану : інформаційний буклет. Київ : Уповноважений ВРУ з прав людини, 2022. 24 с.
16. Security and Privacy for Next-Generation Wireless Networks / ed. by Zhong S., Liang X., Zhu H. Cham : Springer, 2019. 260 p.
17. Lakhtaria K. I. (ed.) Next Generation Wireless Network Security and Privacy. Hershey : IGI Global, 2015. 465 p.
18. Zhang Y., Chen J., Li J. 5G Wireless Network Security and Privacy. Hoboken : IEEE Press – Wiley, 2021.
19. Prasad R., Koren I. Safeguarding 6G: Security and Privacy for the Next Generation. Boca Raton : CRC Press, 2025.
20. Kotzanikolaou P., Mylonas A., Douligeris C. Security and Privacy in Next Generation Networks and Services // In: Next Generation Wireless Network Security and Privacy. IGI Global, 2015.
21. Kuzlu M., Cali U., Pipattanasomporn M. Security and Privacy Concerns in Next-Generation Networks // Next-Generation Networks: Applications and Innovations. Cham : Springer, 2023.
22. Alshamrani A. та ін. Security schemes for the next-generation networks: A survey // GSC Advanced Research and Reviews. 2022.
23. Next Generation Networks and Systems Security and Privacy : Special Issue // Network (MDPI). 2021.
24. Security and Privacy in Next Generation Networks and Services // In: Next Generation Wireless Network Security and Privacy. IGI Global, 2015.
25. Посібник з європейського права у сфері захисту персональних даних. Український переклад. Офіс Ради Європи в Україні, 2021.
26. General Data Protection Regulation (EU) 2016/679. Brussels : European Parliament and Council, 2016.
27. Захист персональних даних : офіційні методичні матеріали Національної поліції України. Київ, 2025.

28.GDPR Compliance Guidelines. Brussels : European Union, 2024.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ

КВАЛІФІКАЦІЙНА РОБОТА

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В МЕРЕЖІ NGN

ВИКОНАВ:
СТУДЕНТ ГРУПИ ТСДМ-62
ВІКТОР БОЦЕНКО

МЕТА РОБОТИ ТА АКТУАЛЬНІСТЬ

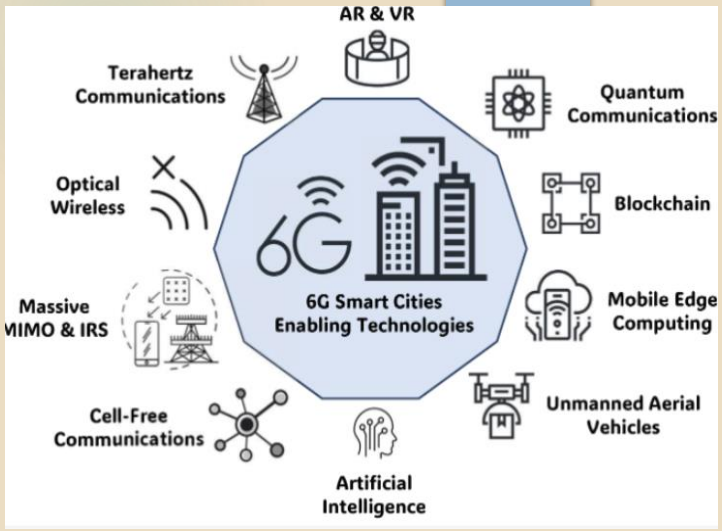
- Мета роботи – розробити та обґрунтувати комплексний підхід до підвищення безпеки персональних даних і VoIP-сервісів у телекомунікаційних мережах NGN шляхом аналізу загроз, вивчення сучасних механізмів захисту та визначення оптимальних технічних і організаційних рішень.
- Об’єкт дослідження – телекомунікаційні мережі наступного покоління, їх архітектура, механізми передавання даних і системи забезпечення інформаційної безпеки.
- Предмет дослідження – методи, моделі та технології захисту персональних даних і VoIP-трафіку в мережах NGN, включаючи використання SBC, механізмів аутентифікації, шифрування, IDS та сучасних концепцій кіберзахисту.

Актуальність.

- Стрімкий розвиток телекомунікаційних технологій, перехід до архітектур NGN, 5G та майбутніх 6G супроводжуються зростанням обсягів даних і появою нових кіберзагроз. Інфраструктури стають гетерогенними, відкритими та високозалежними від віртуалізації, хмарних сервісів і штучного інтелекту, що підвищує ризики витоку, перехоплення та маніпуляції персональними даними. Традиційні моделі периметрового захисту вже не забезпечують належного рівня безпеки, тому виникає потреба у нових підходах, зокрема Zero Trust, посилених механізмах шифрування, захисті VoIP та адаптивних системах кібермоніторингу.

- Мережі 6G розглядаються як наступний етап розвитку мобільних технологій, орієнтований не лише на швидкість, а на створення інтелектуальної цифрової екосистеми. Очікуються швидкості понад 1 Тбіт/с, використання терагерцового спектра, масивних MIMO, квантових та ШІ-керованих технологій.
- 6G перейде від IoT до IoE — мережі, де взаємодіють не лише пристрої, а й дані, сервіси та цифрові двійники. Архітектура буде гнучкою, хмарною й програмно керованою (NaaS). Штучний інтелект стане ключовим механізмом автоматичного управління мережею.
- Загрози 5G збережуться та ускладняться: атаки на SDN, MEC, віртуалізацію та слабкі IoT-пристрої. Через розподіленість мереж периметрова безпека втратить ефективність, тому основою 6G стане Zero Trust та повна автоматизація кіберзахисту.
- Попри інновації, саме безпека визначатиме успіх 6G.

Основні технологічні компоненти 6G: терагерцова комунікація, штучний інтелект, безосередкові мережі, мобільні периферійні обчислення, квантові

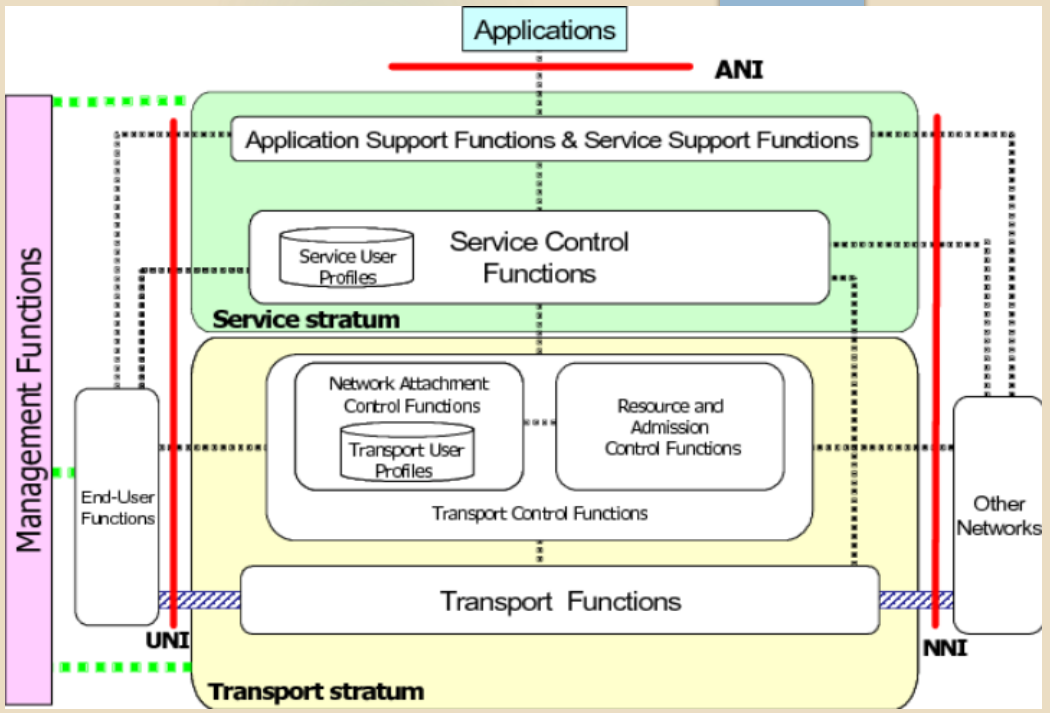




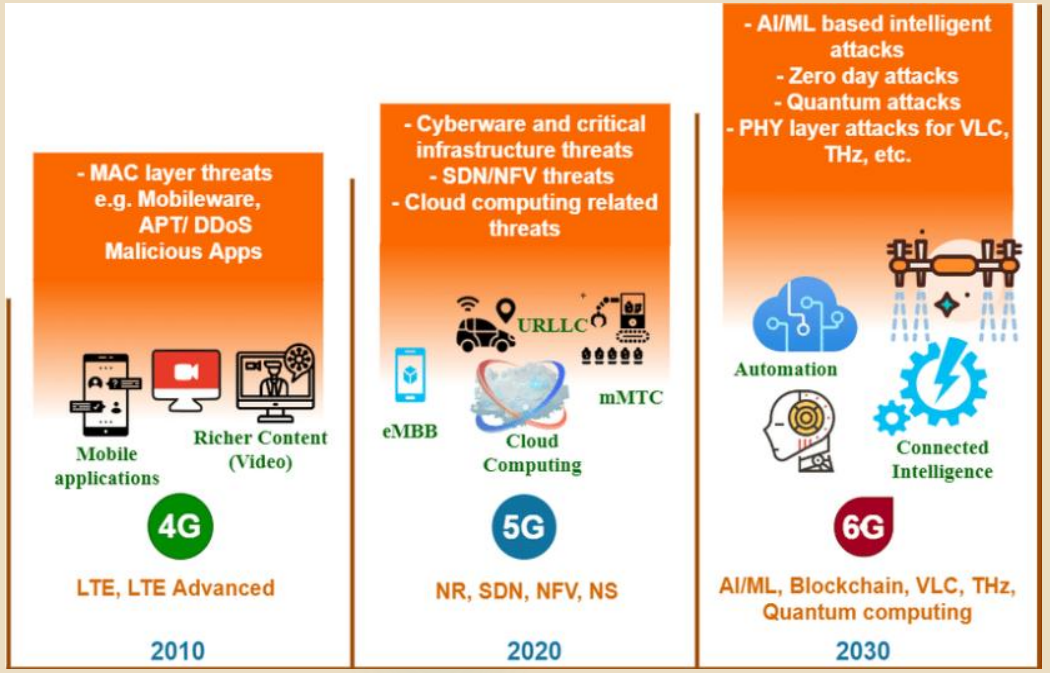
Концептуальна модель 6G, що демонструє взаємодію транспортних, медичних, промислових, роботизованих та супутникових систем через багаторівневу інфраструктуру Інтернету всього (IoE)

Адаптація існуючої архітектури безпеки

- У 6G традиційні механізми безпеки вже неефективні, оскільки мережа охоплює наземні, повітряні, космічні та підводні сегменти й інтегрує дрони, супутники, IoT та ШІ. Це створює нові ризики та вимагає багаторівневої архітектури захисту.
- Ключові виклики включають: безпечну віртуалізацію, контроль уразливостей відкритого ПЗ, захист моделей ШІ, конфіденційність користувачів та перехід до постквантової криптографії.
- 6G стане частиною NGN — інтегрованої інтелектуальної інфраструктури, тому безпека має бути адаптивною, вбудованою та такою, що постійно самовдосконалюється.



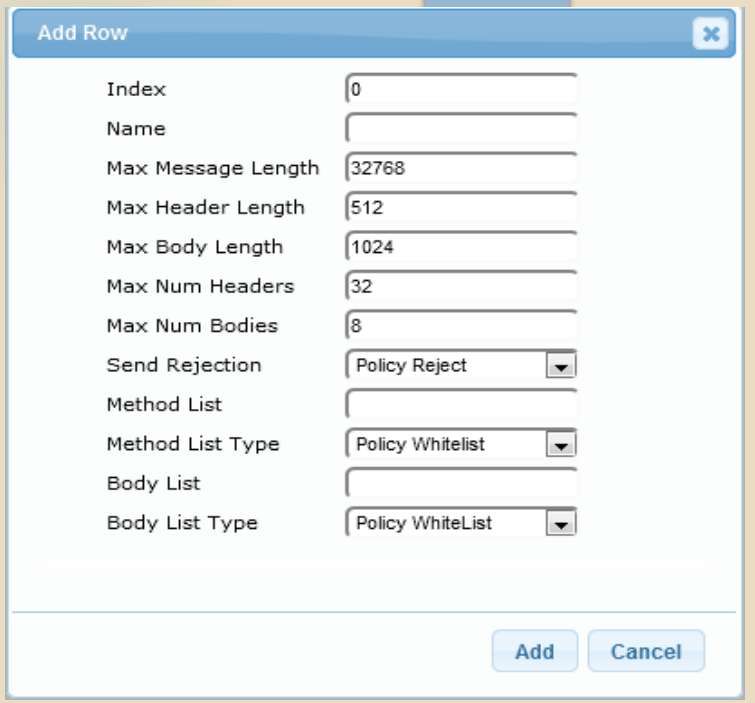
Ієрархічна модель NGN/6G, що відображає розподіл функцій між транспортним, сервісним та прикладним рівнями та їхню взаємодію в інтелектуальній мережевій інфраструктурі



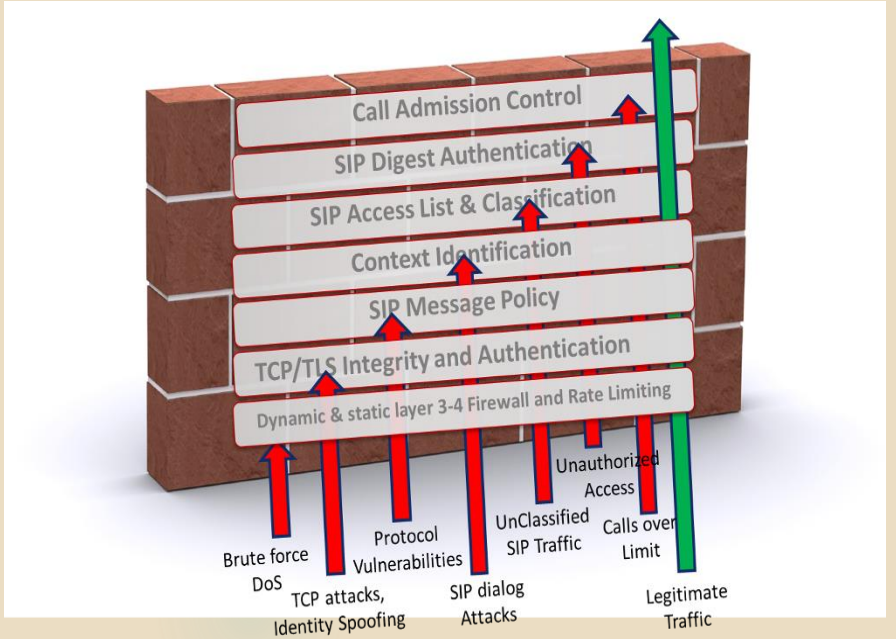
Еволюція загроз для систем мобільного зв'язку від 4G до 6G, що демонструє ускладнення інфраструктури та появу нових класів атак у міру розвитку технологій

ЗАХИСТ VOIP МЕРЕЖ В КОНЦЕПЦІЇ АРХІТЕКТУРИ NGN

- SBC працює у двох режимах — SIP Trunking та Registration — і кожен потребує окремих заходів безпеки. Основний захист включає ізоляцію керувального інтерфейсу, використання нестандартних SIP-портів та налаштування firewall для обмеження доступу. Механізм Call Admission Control запобігає перевантаженням і brute-force атакам. За допомогою SIP-маніпуляцій SBC приховує внутрішню топологію та фільтрує небажані повідомлення. Контроль вихідних дзвінків (через префікси або LDAP) додатково унеможливлює зловживання та фрод.



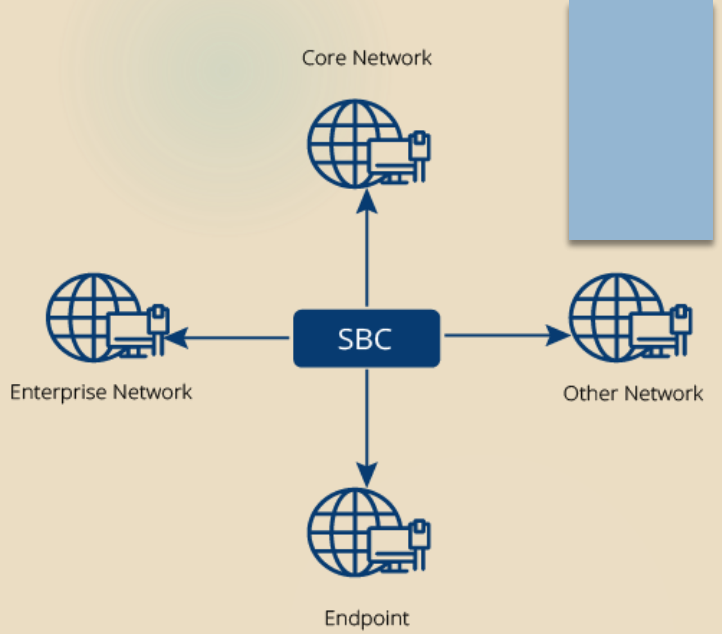
Налаштування політик контролю SIP-повідомлень у SBC: обмеження розміру заголовків, тіла повідомлення, кількості заголовків і методів, а також визначення правил обробки небажаних або некоректних SIP-запитів



Багаторівнева система захисту SIP-інфраструктури: послідовні механізми безпеки SBC (Firewall, TLS-аутентифікація, політики SIP-повідомлень, ACL, SIP Digest, Call Admission Control), які блокують різні типи атак — від brute force і DoS до несанкціонованого доступу та некласифікованого SIP-трафіку

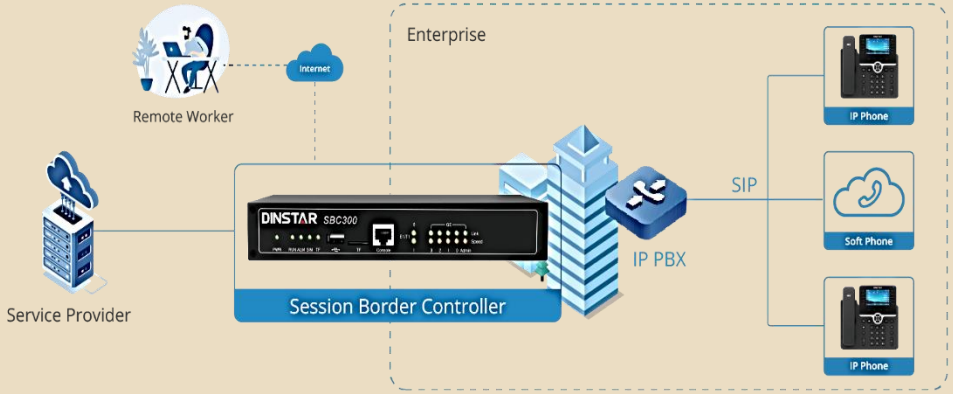
Використання Intrusion Detect System

- Базові механізми безпеки SBC забезпечують первинний захист VoIP-інфраструктури від несанкціонованих викликів, фальсифікацій та маніпуляцій трафіком. Проте сучасні мережі дедалі частіше зазнають складних DoS/DDoS-атак, тому SBC застосовує IDS — систему поведінкового аналізу SIP-трафіку. IDS виявляє аномалії (помилки TLS, спотворені SIP-повідомлення, підбір паролів, збої діалогів, нетипові взаємодії) та виконує реакції: SNMP-сповіщення, тимчасове блокування IP і журналювання інцидентів.
- Політики IDS налаштовуються індивідуально з урахуванням топології, клієнтів і маршрутів. SBC виступає центральною точкою захисту, забезпечує фільтрацію трафіку, захист від brute-force і DDoS, приховує топологію та запобігає шахрайству. Завдяки цьому SBC є ключовим елементом безпеки VoIP навіть у малих компаніях.



Модель роботи SBC як центрального захисного вузла, що забезпечує контроль трафіку між корпоративною мережею, ядром оператора, зовнішніми мережами та кінцевими пристроями

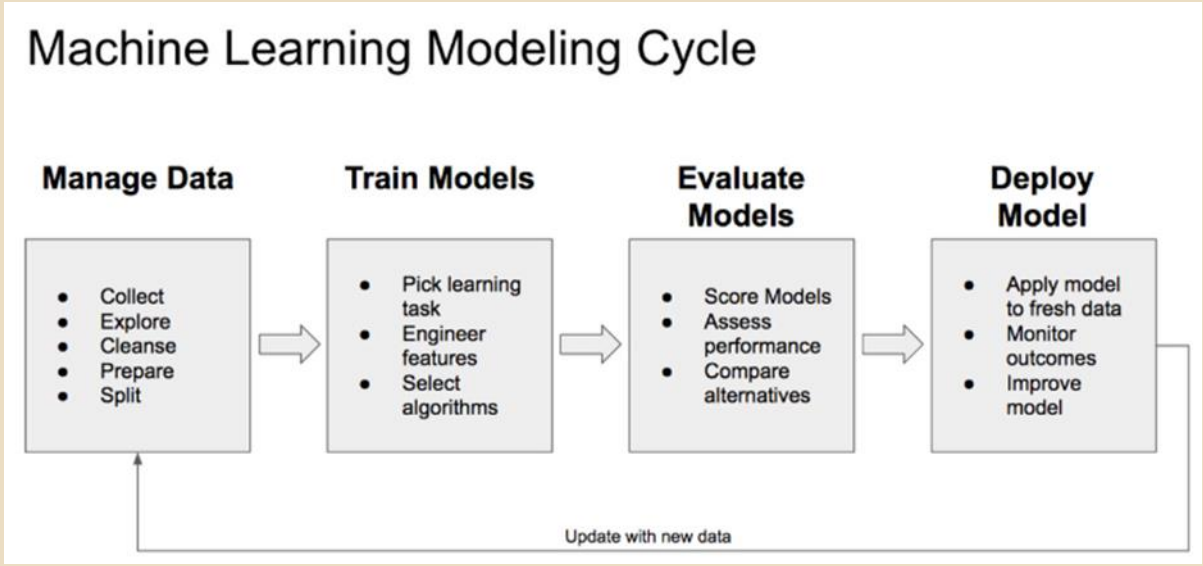
e-SBC



Приклад інтеграції SBC у корпоративну VoIP-інфраструктуру: взаємодія з IP-АТС, SIP-провайдером, віддаленими співробітниками та внутрішніми VoIP-клієнтами. SBC виступає єдиною точкою захисту та контролю всіх VoIP-підключень

Ризики при обробці даних ШІ

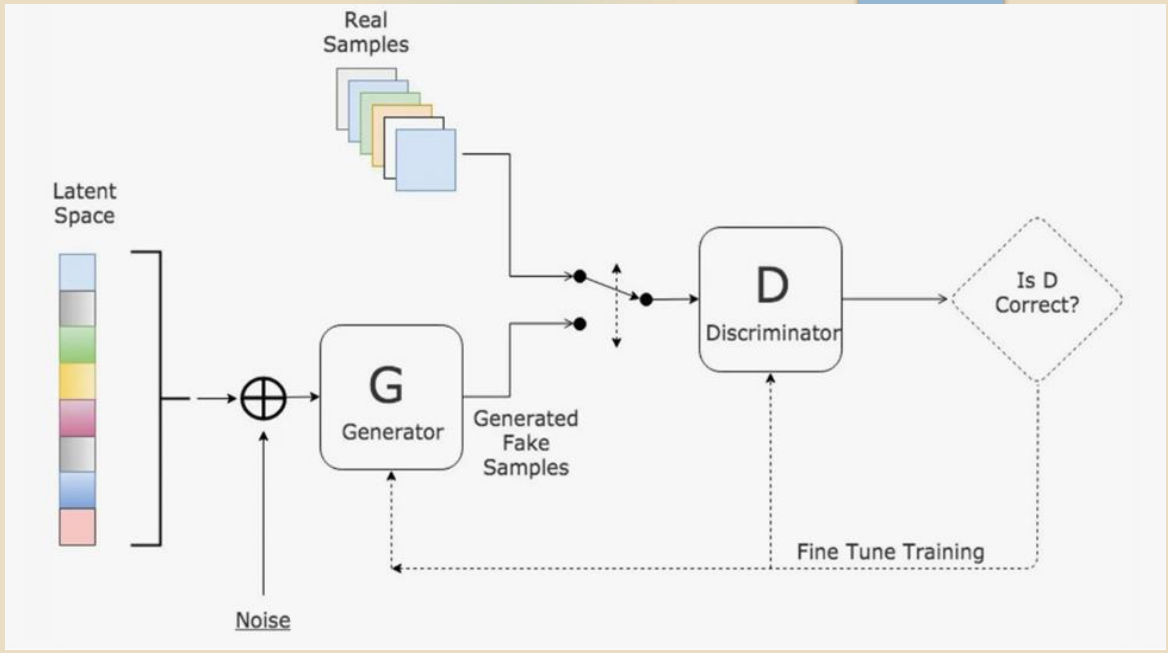
- Системи ШІ працюють на основі великих масивів даних, які використовуються під час навчання та подальшого застосування моделі. Це дає високі можливості, але створює ризики, оскільки серед даних часто є персональна інформація — фото, тексти, поведінкові патерни. Такі дані можуть бути зібрані без згоди, спричиняти витоки, профілювання та дискримінацію. Моделі також здатні відновлювати або виводити приховану інформацію, що ускладнює дотримання законодавства.
- Для безпечного використання ШІ необхідні мінімізація даних, анонімізація, контроль доступу та прозорість обробки.



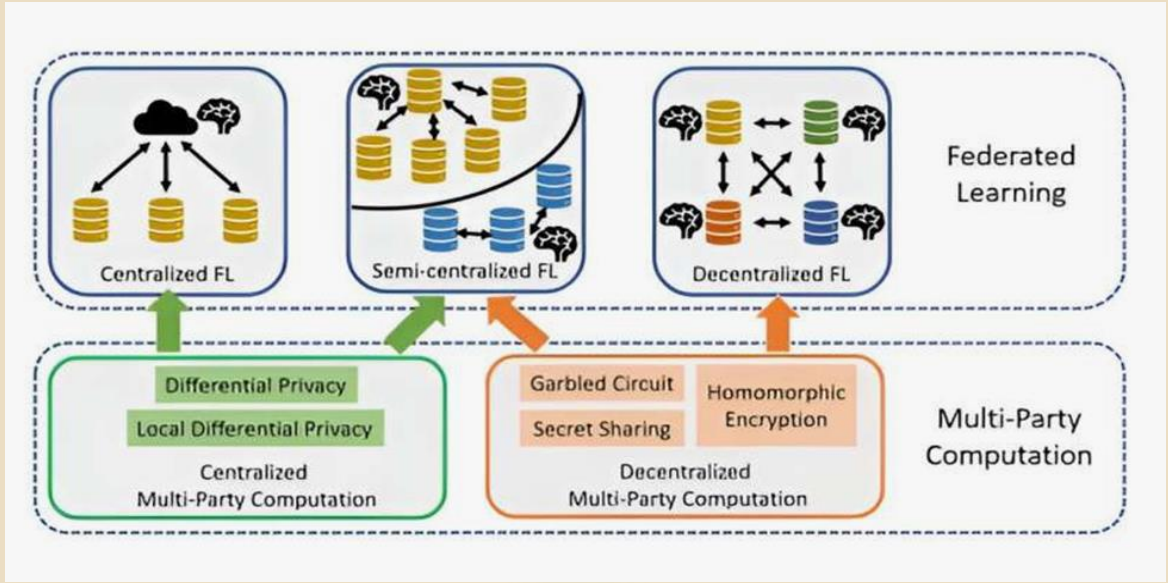
Процес навчання моделі ШІ

Генеративно-змагальні мережі та федеративне навчання

- **Генеративно-змагальні мережі (GAN)** створюють синтетичні дані, подібні до реальних, що дозволяє зменшити використання персональної інформації при навчанні моделей. Вони складаються з генератора і дискримінатора, які вдосконалюються у процесі змагання. Хоча GAN потребують початкового датасету, вони значно знижують обсяг чутливих даних у системах ШІ.
- **Федеративне навчання** дає змогу тренувати моделі без передачі персональних даних — інформація залишається на пристроях, а надсилаються лише оновлені параметри. Метод підвищує конфіденційність, але має обмеження через різну якість локальних даних та ресурси пристроїв.



Generative Adversarial Networks

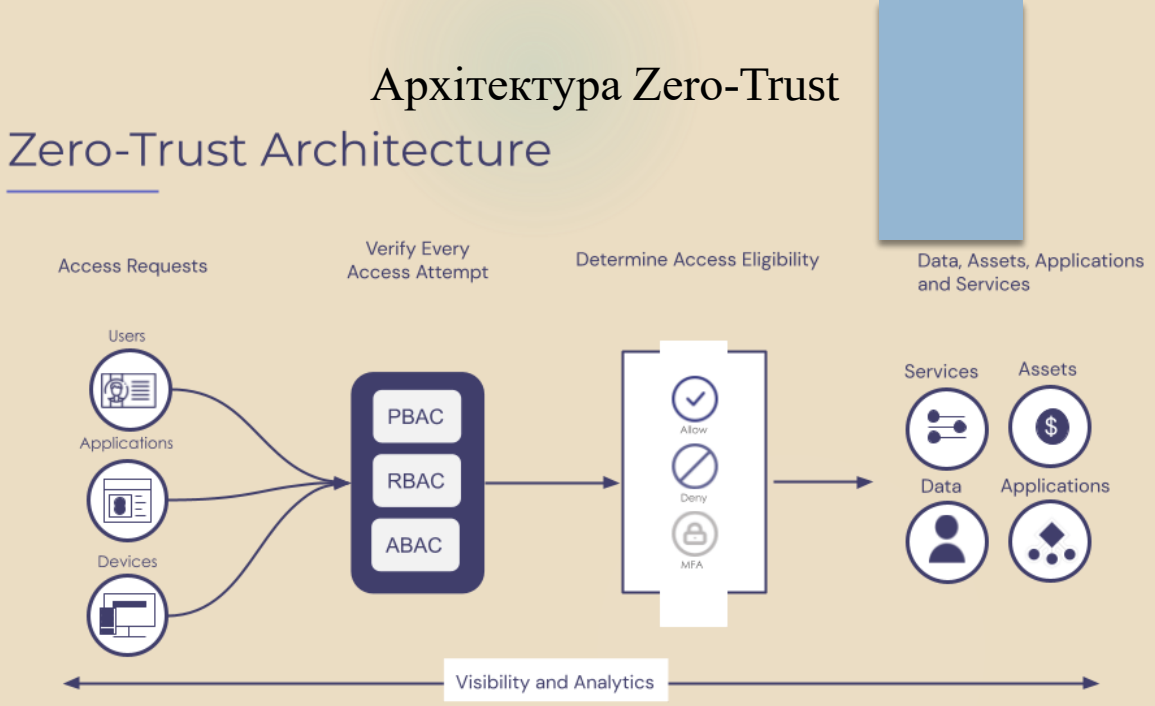


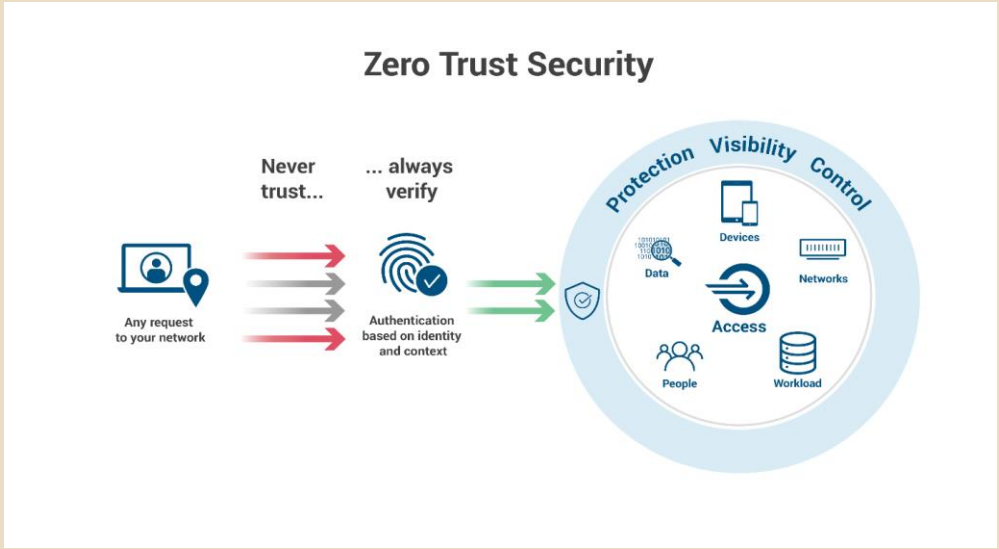
Принцип федеративного навчання

Zero-Trust

- Zero Trust — сучасна стратегія безпеки, що базується на принципі «нікому не довіряти за замовчуванням». На відміну від традиційних моделей, вона не вважає внутрішню мережу безпечною і перевіряє кожен запит незалежно від джерела. Основою впровадження є аудит активів, класифікація даних і визначення їх критичності.
- Модель вимагає мінімальних привілеїв, регулярного перегляду прав доступу, використання RBAC, IAM та MFA. Важливим елементом є сегментація мережі та мікросегментація, які перешкоджають горизонтальному поширенню атак. Zero Trust включає постійний моніторинг через SIEM, SOC, EDR/XDR, UEBA та автоматизоване реагування SOAR.
- Довіра до пристроїв формується тільки після перевірки їхнього стану за допомогою MDM, NAC та політик BYOD. Zero Trust — це не продукт, а комплексна стратегія, що поєднує контроль доступу, багаторівневий моніторинг, сегментацію та автоматизацію, забезпечуючи стійкий захист корпоративної інфраструктури від сучасних загроз.

Архітектура Zero-Trust

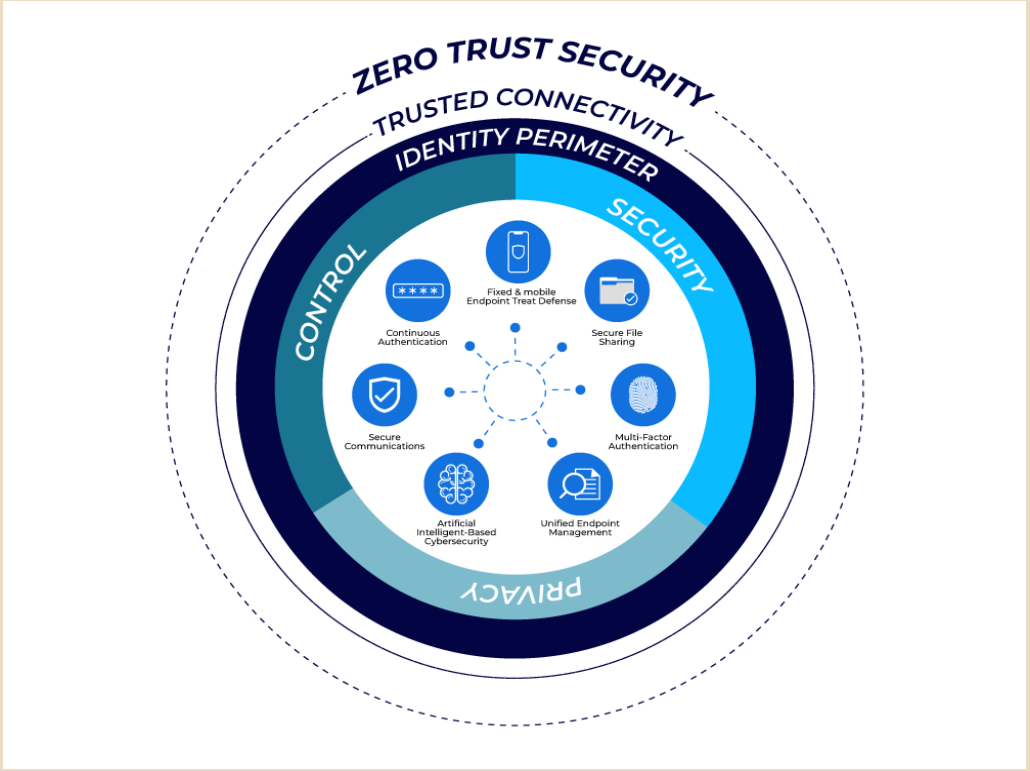




Ключові компоненти моделі Zero Trust: ідентифікація, мінімальні привілеї, сегментація мережі, постійний моніторинг

Практики для внутрішнього захисту серверів та даних

- Внутрішні порушники та зловмисники з доступом до облікових даних становлять серйозну загрозу, тому організації застосовують додаткові механізми контролю.
- **1. Пастки (honeypots).**
- Фіктивні файли дозволяють виявляти підозрілу активність, компрометовані акаунти та ранні спроби перегляду конфіденційних даних. Моніторинг здійснюється через auditd та SIEM.
- **2. Поділ журналів.**
- Привілейовані дії фіксуються окремо, що спрощує виявлення аномальних команд, невдалих входів і змін конфігурацій. Журнали централізуються у Splunk, ELK або SIEM.
- **3. Тимчасові привілеї (JIT).**
- Адміністративні права надаються лише на час виконання задач через PAM-системи. Усі дії логуються, доступ вимагає погодження та автоматично завершується. JEA забезпечує мінімально необхідні команди.
- **4. Ротація секретів.**
- Регулярне оновлення паролів, ключів і токенів знижує ризики компрометації. Використовуються Vault, AWS/Azure/GCP Secret Manager, FIDO2 та перевірка паролів на витоки.



Концепт доступу по Zero Trust: користувач або пристрій запитує доступ — перевірка контексту, статусу, політики — і лише потім дозвіл або блокування

ВИСНОВКИ

- У дослідженні проаналізовано особливості захисту персональних даних у мережах NGN, які поєднують мобільні, стаціонарні, оптичні, супутникові та IoT-технології.
- Показано, що зі зростанням швидкості передавання даних, масштабом підключень та інтеграцією хмарних і ШІ-систем збільшується кількість кіберзагроз.
- Визначено основні уразливості VoIP-інфраструктури та роль SBC у приховуванні топології, фільтрації трафіку та виявленні атак.
- Окрема увага приділена ризикам обробки даних у ШІ та методам їх мінімізації.
- Доведено, що традиційні моделі безпеки не відповідають вимогам NGN, а ключовою концепцією захисту є Zero Trust, яка забезпечує багаторівневу, адаптивну та проактивну оборону.

Дякую за увагу!

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Віктор БОЦЕНКО

Назва: ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В МЕРЕЖІ NGN

Координатор: Володимир РУЖИНСЬКИЙ

Підрозділ: ННІТ

Коефіцієнт подібності 1:0

Коефіцієнт подібності 2:0

Тривога: 1

Після аналізу Звіту подібності констатую наступне:

☐ виявлені в роботі запозичення є сумлінними і не мають ознак плагіату. Тому робота визнається самостійною і допускається до захисту;

☐ виявлені в роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і самостійності її автора. Роботу направити на доопрацювання;

☐ виявлені в роботі запозичення є недобросовісними і мають ознаки плагіату або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень. У зв'язку з чим, робота не допускається до захисту.

…… ……

Дата *Підпис Наукового керівника*