РОБОТА
на здобуття премії Президента України для молодих вчених

«Цифрова стійкість держави як ключовий чинник сталого розвитку в умовах повоєнного відновлення»

Сергій ГНАТЮК,
доктор технічних наук, професор,
проректор з наукових досліджень
та трансферу технологій

Роман ОДАРЧЕНКО,
доктор технічних наук, професор,
декан Факультету аеронавігації,
електроніки та телекомунікацій

Анастасія СІМАХОВА,
доктор технічних наук, професор,
професор кафедри бізнес-
аналітики та цифрової економіки

Державне некомерційне підприємство «Державний університет
«Київський авіаційний інститут», м. Київ, 2025 р.

План

- Актуальність роботи
- Удосконалення інформаційно-комунікаційних систем та мереж з метою підвищення потенціалу цифрової інфраструктури держави
- Методологія оцінки та підвищення ефективності функціонування мережі стільникового оператора
- Удосконалення механізмів забезпечення кібербезпеки стільникових мереж 5G
- Виявлення цілеспрямованих атак в кіберпросторі
- Кібербезпека критичної інформаційної інфраструктури держави
- Потенціал цифровізації для сталого розвитку та повоєнної відбудови економіки України
- Масштаби реалізації та практична значимість
- Висновки

Гнатюк С.О., Одарченко Р.С, Сімахова А.О, м. Київ, 2025 р.

Актуальність

- В країні, яка наразі перебуває в активній фазі повномасштабної війни, захист критичної інформаційної інфраструктури є надзвичайно важливим та складним процесом, який складається з багатьох факторів, таких як: визначення переліку критичних об'єктів, оцінка ступеня їх вразливості та можливих варіантів запобігання атакам.
- Цифрова трансформація передбачає перетворення всіх сфер суспільного життя під впливом передових інноваційних інформаційно-комунікаційних технологій (ІКТ). Це визначає актуальність прискорення цифрової трансформації як в Україні, так й інших країнах світу.
- Важливість наукової роботи відповідає інтересам громадян України, формуванню високого рівня інформаційної, цифрової, економічної безпеки країни. Безперечно, повоєнна економіка за всіх форм її організації має спрямовуватись на забезпечення належного рівня життя населення шляхом надання рівних можливостей для реалізації на конкурентній основі власного потенціалу громадян у всіх сферах життєдіяльності.
- Наукова робота відповідає декільком напрямам з переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 31 грудня року, наступного після припинення або скасування воєнного стану в Україні, відповідно Постанови Кабінету Міністрів України від 30.04.2024 р. № 476, зокрема «Інформаційно-комунікаційні та радіоелектронні системи та технології для забезпечення національної безпеки і оборони. Інформаційна безпека та кібербезпека», «Інформаційно-комунікаційні системи та мережі» та «Цифровізація соціально-гуманітарних процесів та освіта в цифрову епоху».
- Крім цього, наукова робота відповідає Цілям сталого розвитку ООН до 2030 р., оскільки більшість із 17 цілей сталого розвитку ООН до 2030 р. впливають на повоєнну відбудову України через подолання бідності, продовольчу безпеку, забезпечення добробуту та зайнятості людей будь-якого віку, скорочення соціальної нерівності, раціональне використання природних ресурсів, збереження довкілля для майбутніх поколінь тощо.

- Мета роботи: дослідження цифрової стійкості та розробка пропозицій щодо їх повоєнного відновлення України

Гнатюк С.О., Одарченко Р.С, Сімахова А.О, м. Київ, 2025 р.

Основні характеристики технологій 5G/6G, пов’язані зі сталим розвитком

Енергетична ефективність

Мережі 5G і майбутні мережі 6G покликані зменшити споживання енергії за рахунок більш ефективної передачі даних і більш розумної інфраструктури, сприяючи зменшенню глобального вуглецевого сліду.

Масштабний зв’язок

5G дозволяє підключити мільярди пристроїв Інтернету речей по всьому світу, прокладаючи шлях до «розумних» міст, «розумного» сільського господарства та «розумної» промисловості, які сприяють більш стійким практикам за рахунок оптимізації ресурсів і скорочення відходів

Підвищена надійність та швидкість мережі

Ці мережі забезпечують надійний високошвидкісний зв'язок, що може сприяти цифровій інклюзії, надаючи доступ до освіти, телемедицини та інших основних послуг навіть у віддалених районах, підтримуючи такі цілі, як якісна освіта та охорона здоров'я.

Наднизька затримка

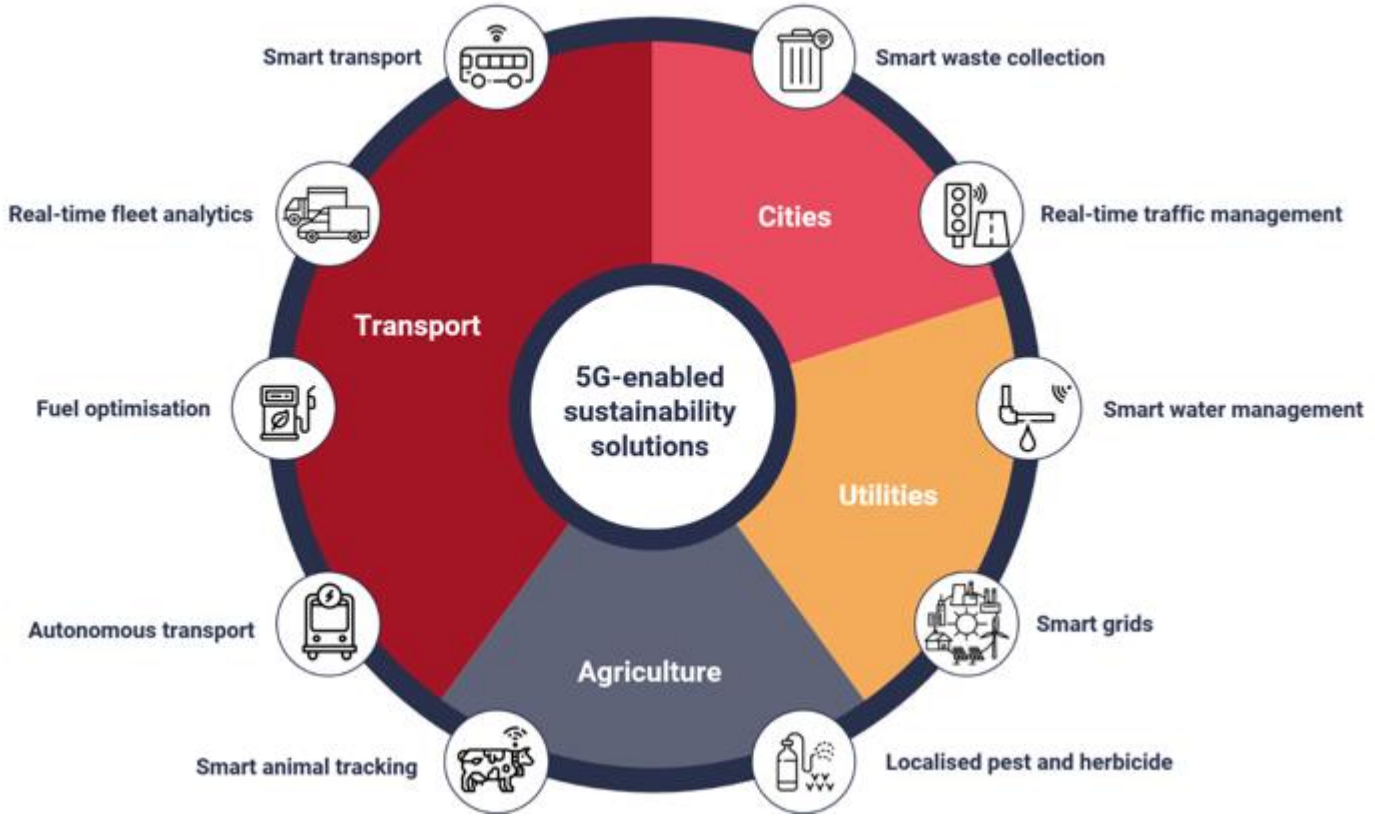
Мережі 5G і 6G розроблені таким чином, щоб забезпечити неймовірно низьку затримку, що має вирішальне значення для додатків, які працюють у режимі реального часу. Ця функція підтримує інновації в охороні здоров'я (дистанційні операції), транспорті (автономні транспортні засоби) та «розумних» мережах для ефективного управління енергоспоживанням.

Інтеграція з передовими технологіями

5G/6G буде інтегруватися зі штучним інтелектом, периферійними обчисленнями та блокчейном, щоб забезпечити такі інновації, як прогнозоване технічне обслуговування в промисловості, інтелектуальні системи моніторингу навколишнього середовища та безпечний обмін даними для ініціатив сталого розвитку.

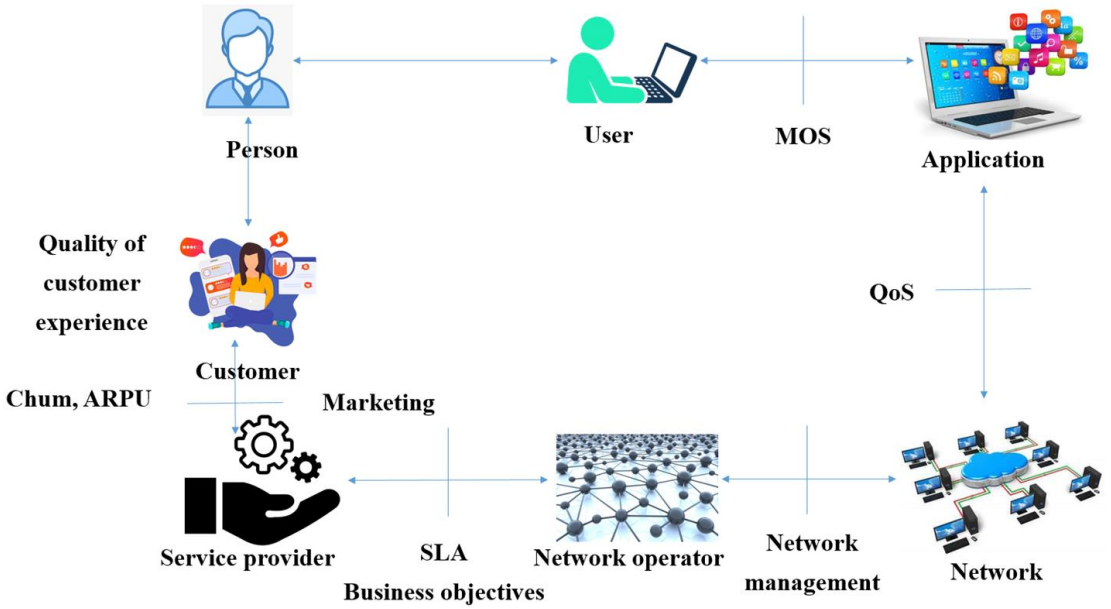
Гнатюк С.О., Одарченко Р.С, Сімахова А.О, м. Київ, 2025 р.

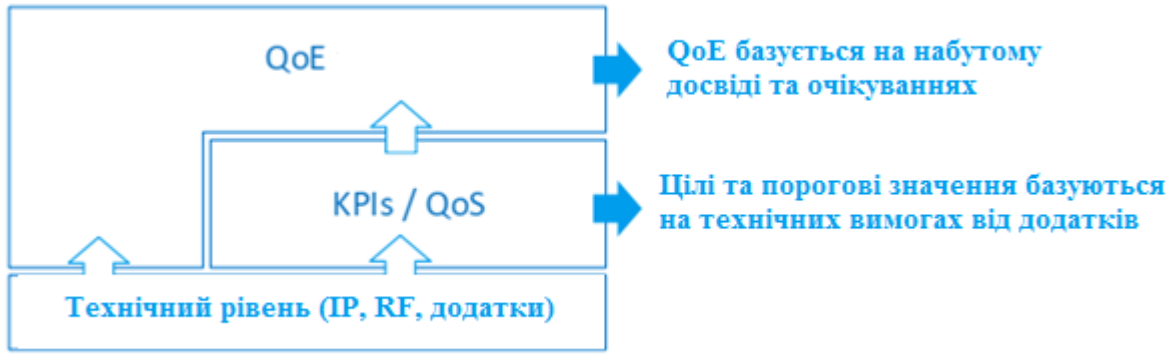
Ключові напрямки впровадження 5G



Гнатюк С.О., Одарченко Р.С, Сімахова А.О, м. Київ, 2025 р.

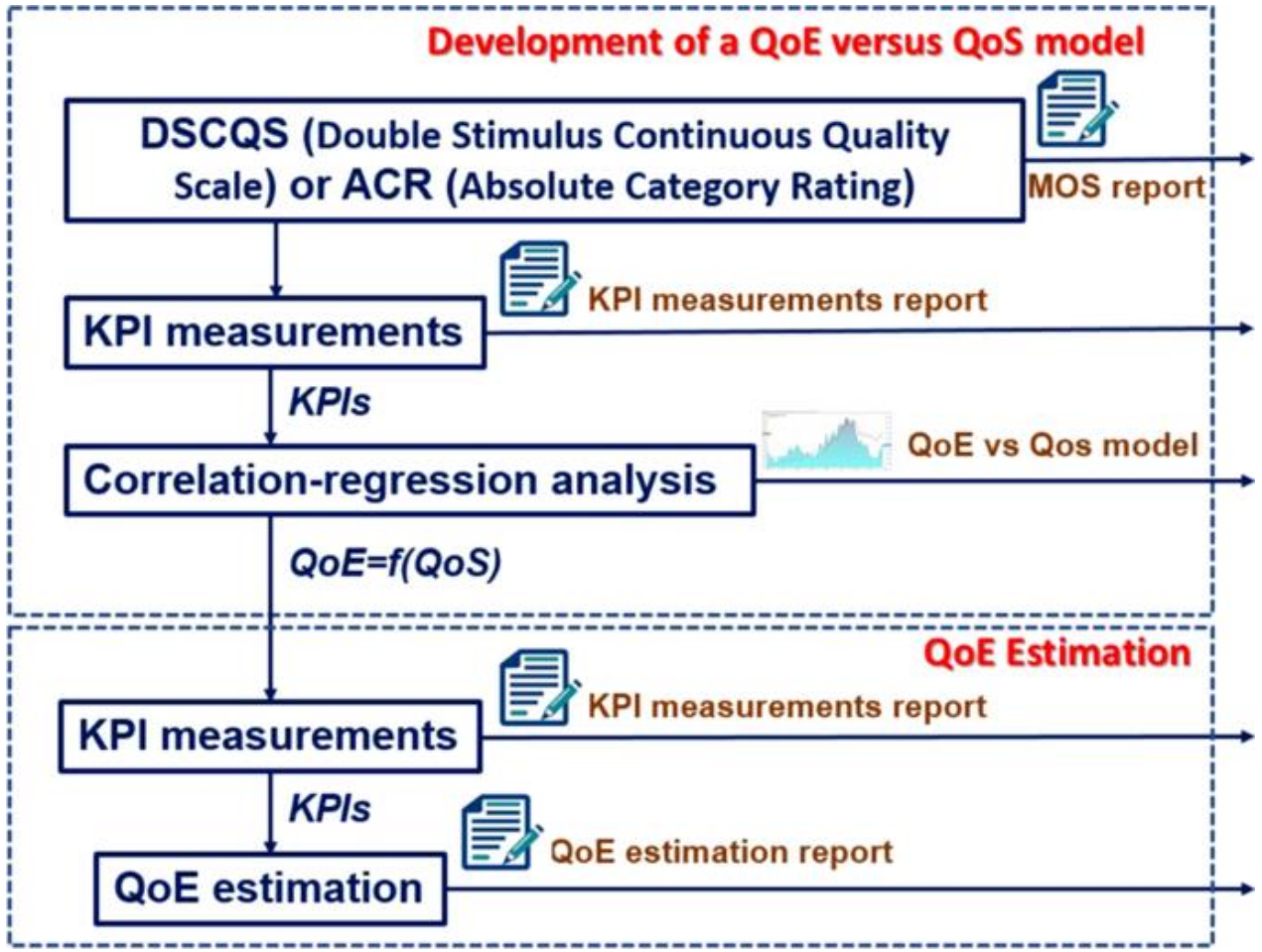
Модель забезпечення QoE





Гнатюк С.О., Одарченко Р.С, Сімахова А.О, м. Київ, 2025 р.

Методологія оцінки та підвищення ефективності стільникових мереж зв'язку



MOS

- Збір скарг від абонентів за певний період часу (щодня, щотижня).
- Сортування отриманих звернень по категоріям: Покриття, Складнощі з передачею даних, Складнощі із дзвінками.

KPI

- Визначення ключових KPI для кожної категорії та технології.
- Присвоєння коефіцієнтів погіршення кожному з показників KPI, відповідно до категорії та впливу на якість сервісу.

QoE/QoS

- Опрацювання отриманих даних за допомогою алгоритмів машинного навчання.
- Отримання результату співвідношення QoE/QoS.

Гнатюк С.О., Одарченко Р.С, Сімахова А.О, м. Київ, 2025 р.

Алгоритм ШІ

```
MAIN
        FOR EACH tree FROM Trees
        subset = getSubset(tree)

        FOR EACH set FROM subset
        buildBranching(set)
        WHILE exitCondition IS TRUE

        showResult()
        END

END

PROCEDURE buildBranching(data)
        setsOfVariables =
selectSetsOfVariables(data)

        FOR EACH var FROM setsOfVariables
        compareWithSample(var)
        sort(var)
        calculateInEveryPoint(var)
        END

        RETURN getBestValue(var)
END
```

Важливим етапом методу є правильний відбір наборів даних. Набір даних, необхідний для аналізу, має вигляд таблиці з полями:

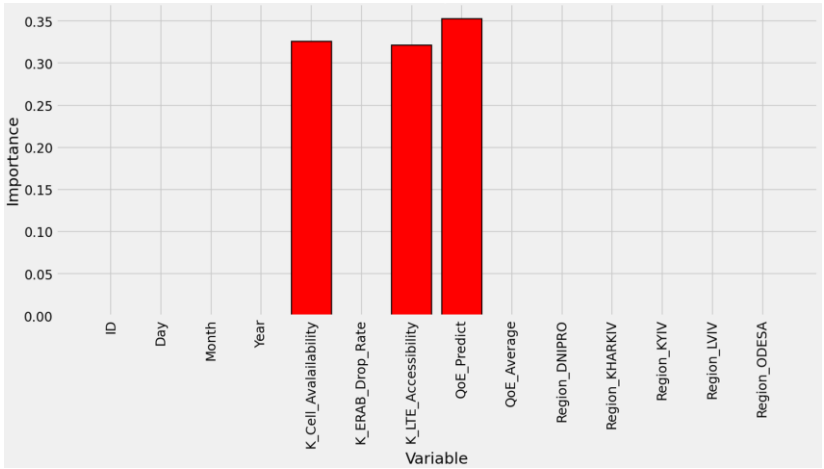
1. Номер скарги.
2. День.
3. Місяць.
4. Рік.
5. Тип скарги (Покриття, Труднощі з передачею даних, Труднощі з дзвінками).
6. Технологія (2G/3G/4.5G).
7. Визначені KPI.
8. Вагові коефіцієнти для KPI.
9. Оцінка послуг, отриманих абонентом.

Ігнатюк С.О., Одарченко Р.С, Сімахова А.О, м. Київ, 2025 р.

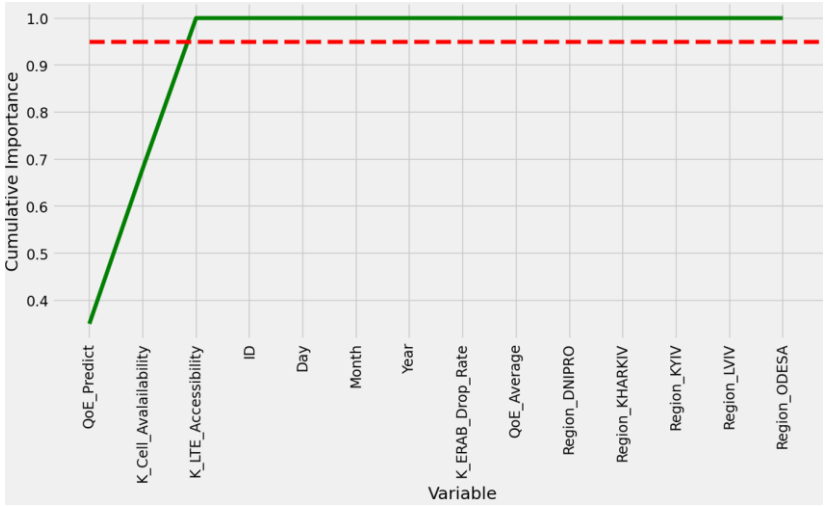
Експериментальні дослідження

	A	B	C	D	E	F	G	H	I
1	ID	Day	Month	Year	Region	K_Cell_Avalailability	K_ERAB_Drop_Rate	K_LTE_Accessibility	QoE
2	419	9	1	2022	KYIV	3.5	0.109396	3.5	1
3	418	9	1	2022	KYIV	15	0.019996	15	3
4	366	8	1	2022	KYIV	5.25	0.050622	5.25	1
5	365	8	1	2022	KYIV	24	0.036122	24	5
6	364	8	1	2022	KYIV	14.5	0.0099	14.5	3
7	363	8	1	2022	KYIV	19.75	0.003176	19.75	4
8	362	8	1	2022	KYIV	10.25	0.056362	10.25	2
9	313	7	1	2022	KYIV	4.75	0.11408	4.75	1
10	312	7	1	2022	KYIV	20.75	0.111158	20.75	4
11	311	7	1	2022	KYIV	18	0.107638	18	4
12	272	6	1	2022	KYIV	20.5	0.017044	20.5	4
13	271	6	1	2022	KYIV	0	0.0186	0	1
14	223	5	1	2022	KHARKIV	2	0.088838	2	1
15	222	5	1	2022	KHARKIV	17.75	0.007366	17.75	4
16	221	5	1	2022	KHARKIV	3	0.08425	3	1
17	220	5	1	2022	KHARKIV	24	0.006282	24	5
18	219	5	1	2022	KHARKIV	12.75	0.083514	12.75	3

Набір даних



Значення кожної змінної

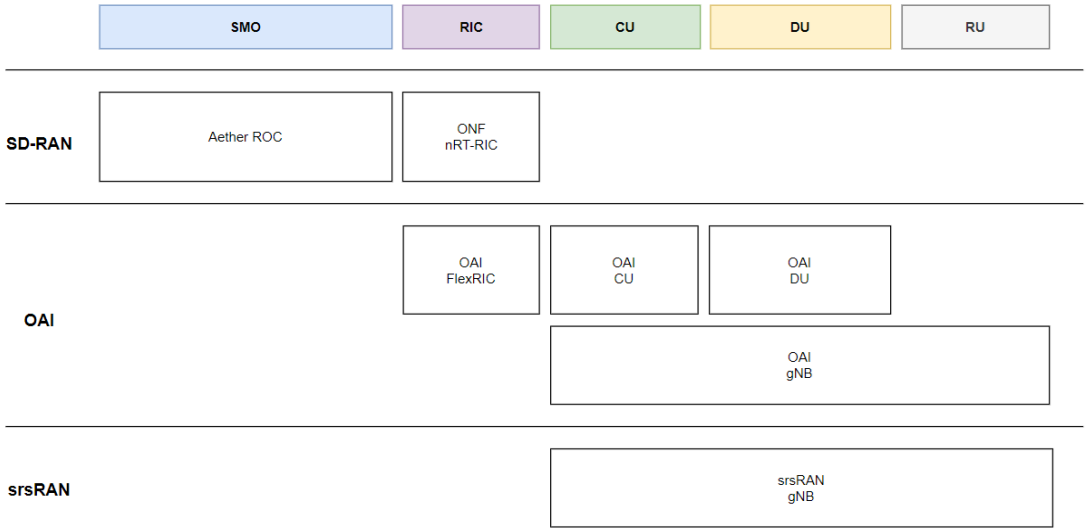


Кумулятивні властиві значення

Гнатюк С.О., Одарченко Р.С, Сімахова А.О, м. Київ, 2025 р.

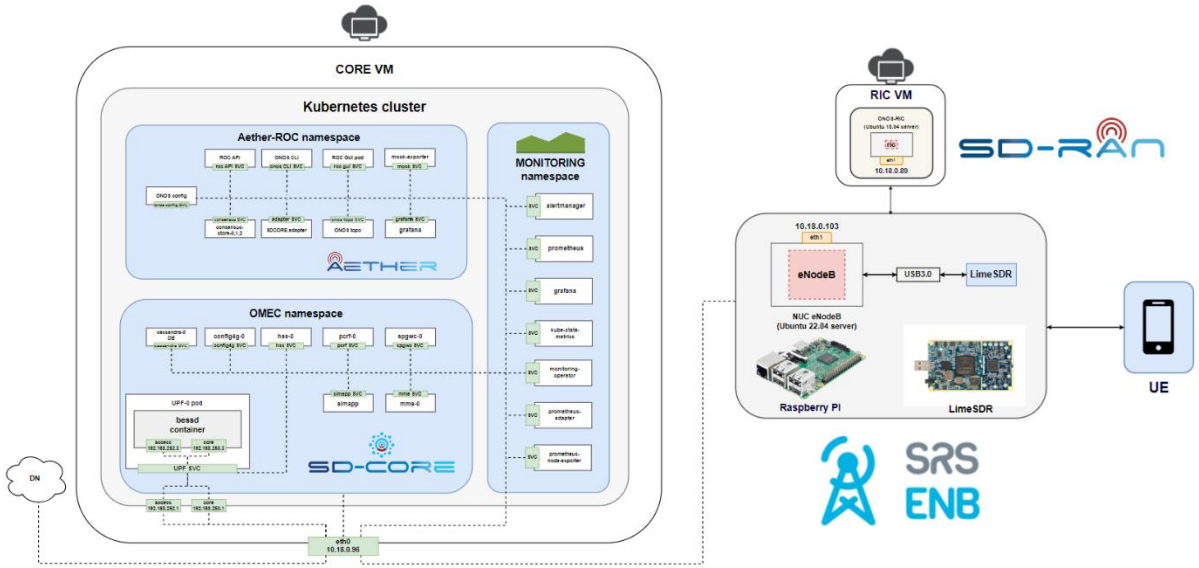
Варіанти розгортання мережі 5G на основі рішень з відкритим вихідним кодом

Project	VNFs	Install methods	VNF deployment	Limitations
Open5GS	NRF, AMF, SMF, UPF, AUSF, UDM, UDR, PCF, NSSF, BSF, SCP	Package manager	systemd services	- No Interworking with EPC - No NB-IoT - No OCS/OFCS - No eMBMS - No SRVCC - No Roaming - No Emergency Call
Free5GC	NRF, AMF, SMF, UPF, AUSF, UDM, UDR, PCF, NSSF, N3IWF	Compiling NFs through make commands	systemd services/docker containers/kubernetes pods	Not mentioned, stated or documented
SD-CORE	NRF, AMF, SMF, UPF, AUSF, UDM, UDR, PCF, NSSF	Automated script, that installs all necessary tools and NFs for Kubernetes deployment	kubernetes pods	- Only one instance of the UPF-adapter pod should be deployed. - Scale up or down instances of AMF/SMF/Sctp-Lb can be done manually. - Webui pod crash problem, usually simapp pod deletion helps UPF Pod needs to have UE pool configuration



Гнатюк С.О., Одарченко Р.С, Сімахова А.О, м. Київ, 2025 р.

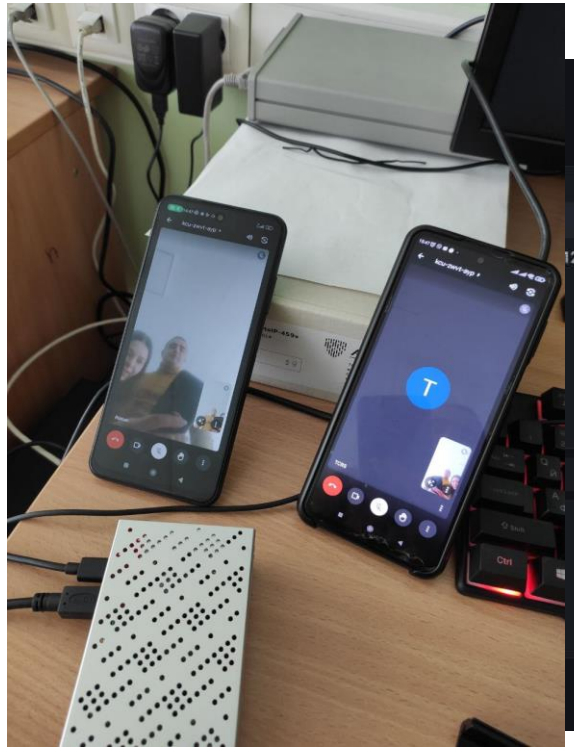
Розгортання мережі для тестування розробленої методології

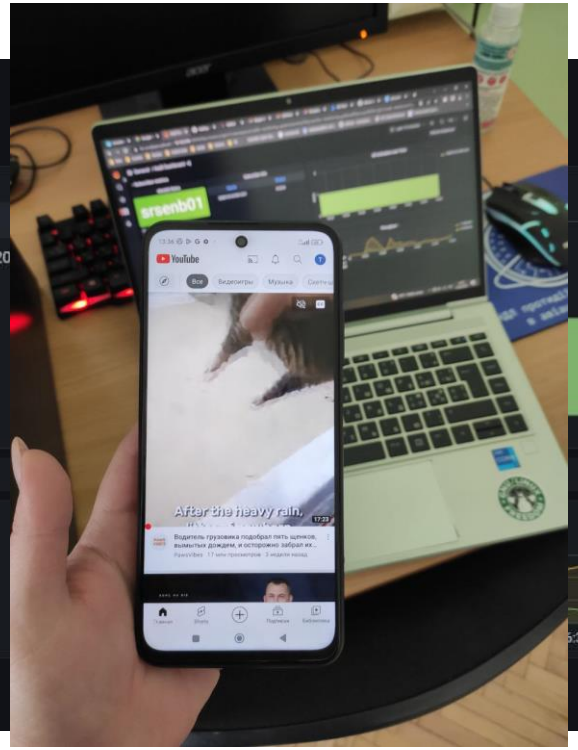


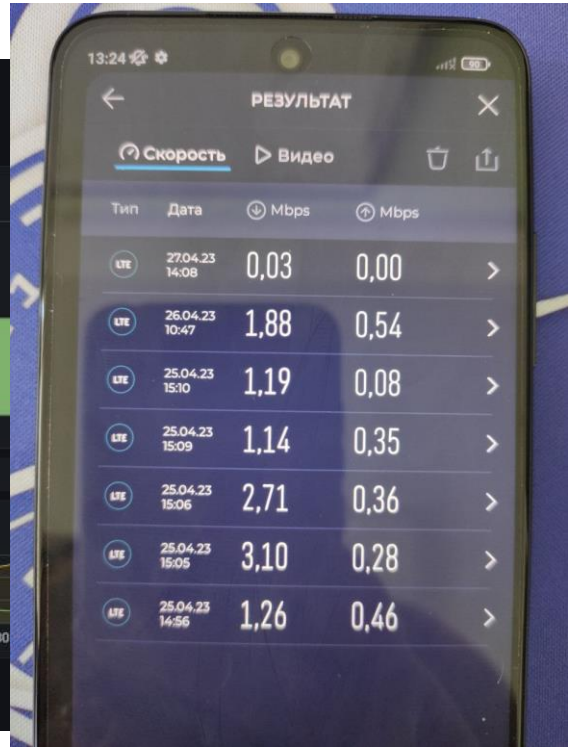
#	Компонент	Рішення
1.	Ядро мережі	SD-CORE/Віртуальна машина на сервері
2.	RAN (Radio Access Network)	srsENB/Raspberry PI, LimeSDR
3.	RIC (RAN Intelligent Controller)	SD-RAN/ Virtual machine on the server
4.	SMO (Service Management Orchestration)	Aether ROC/Virtual machine on the server
5.	UE (User Equipment)	GRSIMWrite4.2.10/smartphone with LTE support, blank SIM-card

Гнатюк С.О., Одарченко Р.С, Сімахова А.О, м. Київ, 2025 р.

Результати тестування 4G в Національному авіаційному університеті





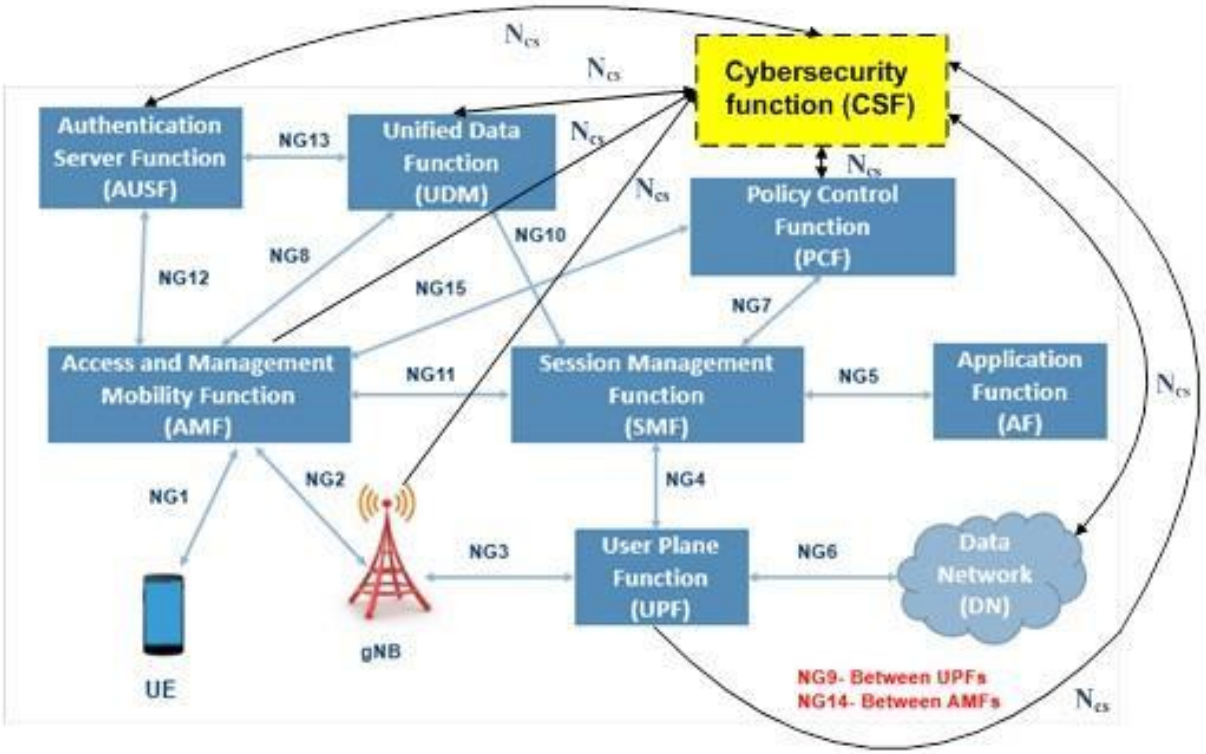


GlobalLogic®
A Hitachi Group Company

Гнатюк С.О., Одарченко Р.С, Сімахова А.О, м. Київ, 2025 р.

Вимоги безпеки, якими має керувати та обробляти архітектура безпеки в мережах 6G

1. **Рішення безпеки віртуалізації.** Проблеми безпеки віртуалізації потребують використання системи із захищеним рівнем віртуалізації, який включає технологію безпеки, яка визначає приховане шкідливе програмне забезпечення, наприклад руткіти.
2. **Автоматизована система керування:** керувати вразливими місцями, спричиненими використанням, оновленням і видаленням відкритих вихідних кодів, є найважливішою справою при вирішенні питань безпеки з відкритим вихідним кодом.
3. **Безпека даних за допомогою штучного інтелекту:** щоб гарантувати, що системи штучного інтелекту захищені, вони повинні бути прозорими щодо того, як вони захищають своїх користувачів і систему мобільного зв'язку від протидії зовнішнім загрозам.
4. **Збереження конфіденційності користувачів:** особисту інформацію користувачів слід зберігати та використовувати відповідно до протоколів, узгоджених між постачальником послуг, мобільним телефоном оператор мережі (MNO), абонент і оператор мережі, щоб забезпечити їх безпеку.
5. **Постквантова криптографія:** система 6G має позбутися існуючої асиметрії ключові методи шифрування, оскільки квантові комп'ютери зроблять їх незахищеними. Рішення для постквантової криптографії (PQC), такі як криптографія на основі решітки, криптографія на основі коду, багатовимірна поліноміальна криптографія та підпис на основі хешу, були в центрі уваги багатьох дослідників.



Гнатюк С.О., Одарченко Р.С, Сімахова А.О, м. Київ, 2025 р.

Опис проблеми

Постановка проблеми:

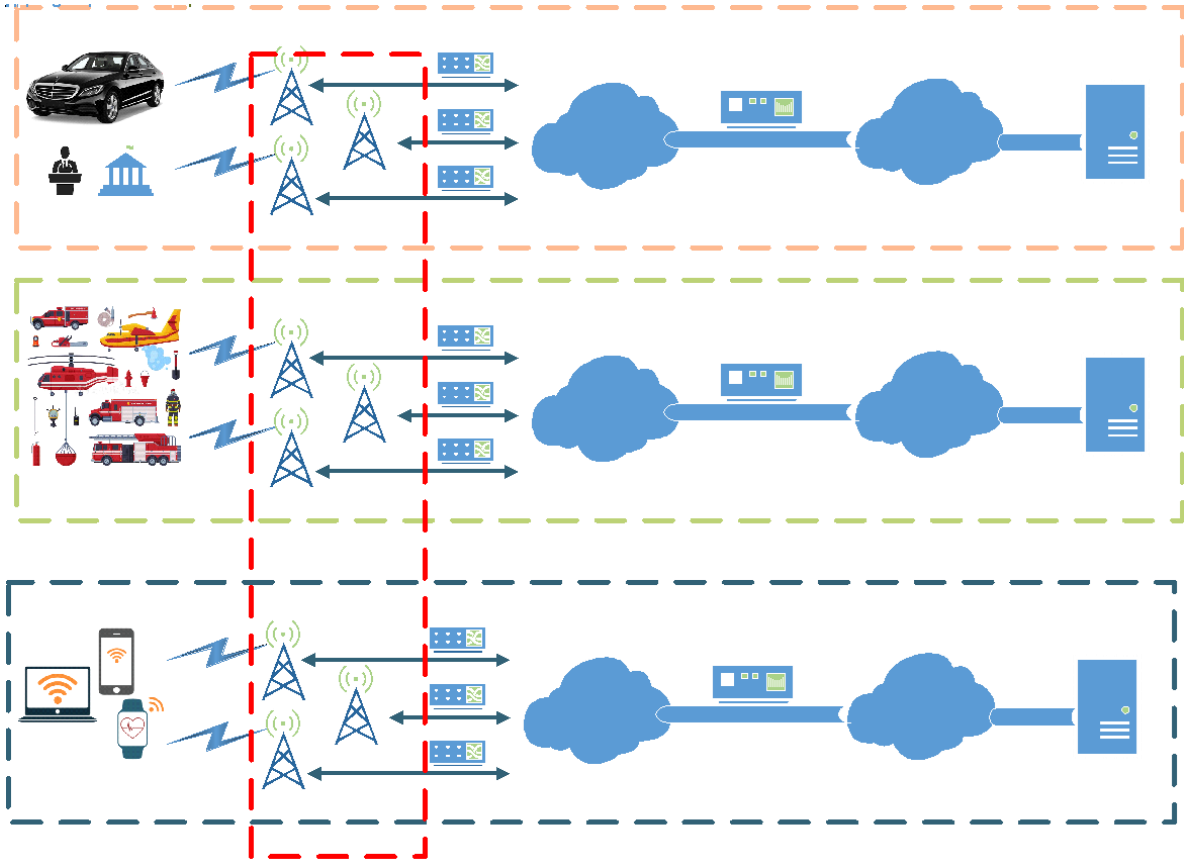
- Мережі 5G/6G як частина критичної інфраструктури;
- 5G/6G з'єднає інші сектори критичної інфраструктури;
- необхідно визначити нові вимоги до безпеки

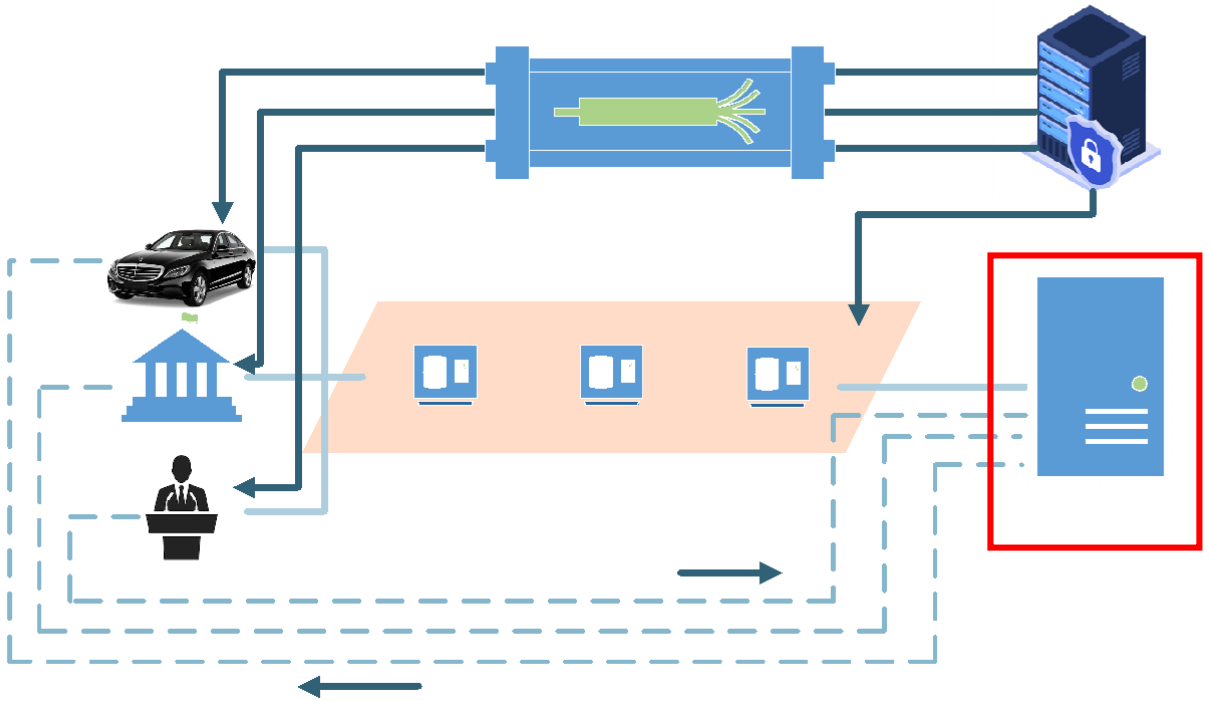
Негативний вплив:

- новий ландшафт кіберпотоків у 4G/5G;
- Мережі 5G більш вразливі до кібератак, ніж їхні попередники;
- 99% кібератак так чи інакше проходять через мережу.

Гнатюк С.О., Одарченко Р.С, Сімахова А.О, м. Київ, 2025 р.

Нова архітектура кібербезпеки 5G/6G

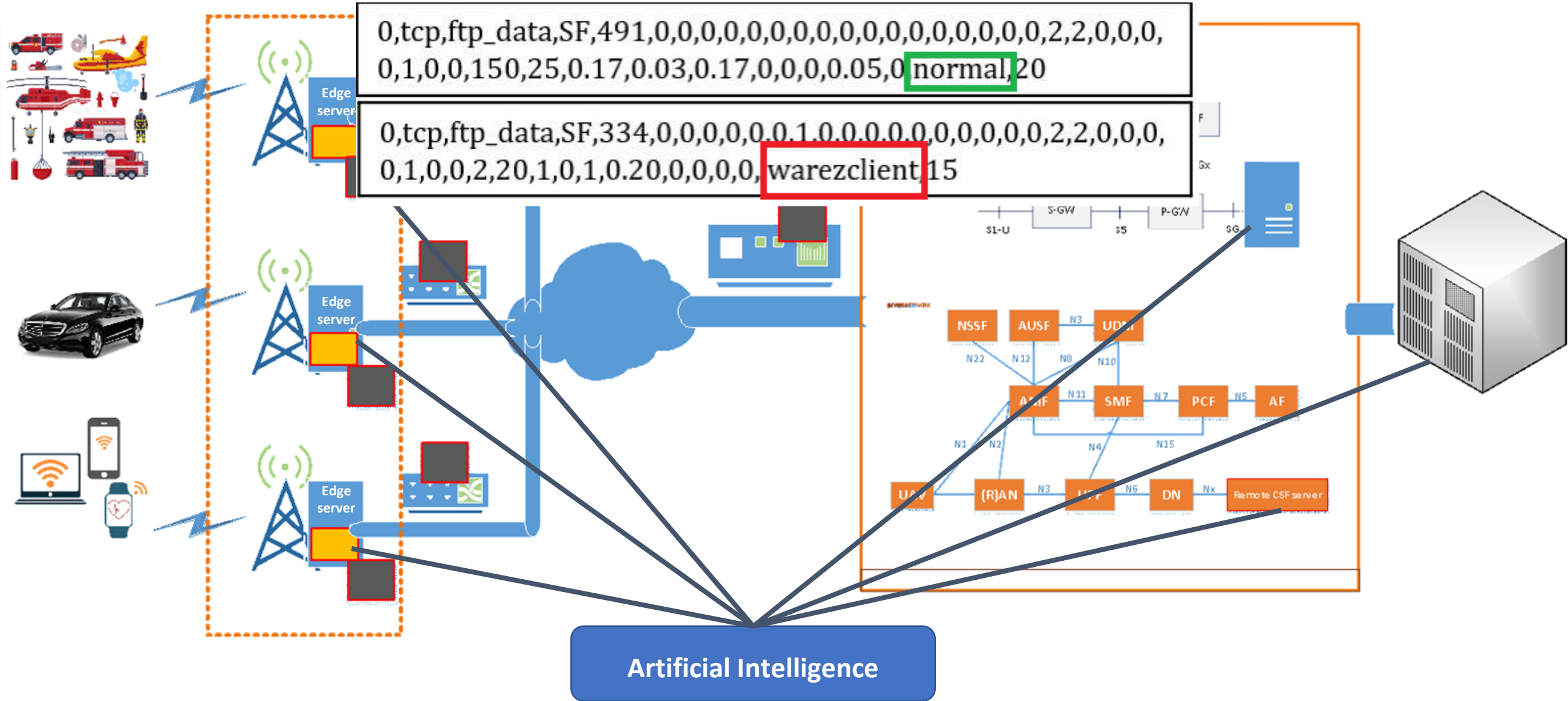




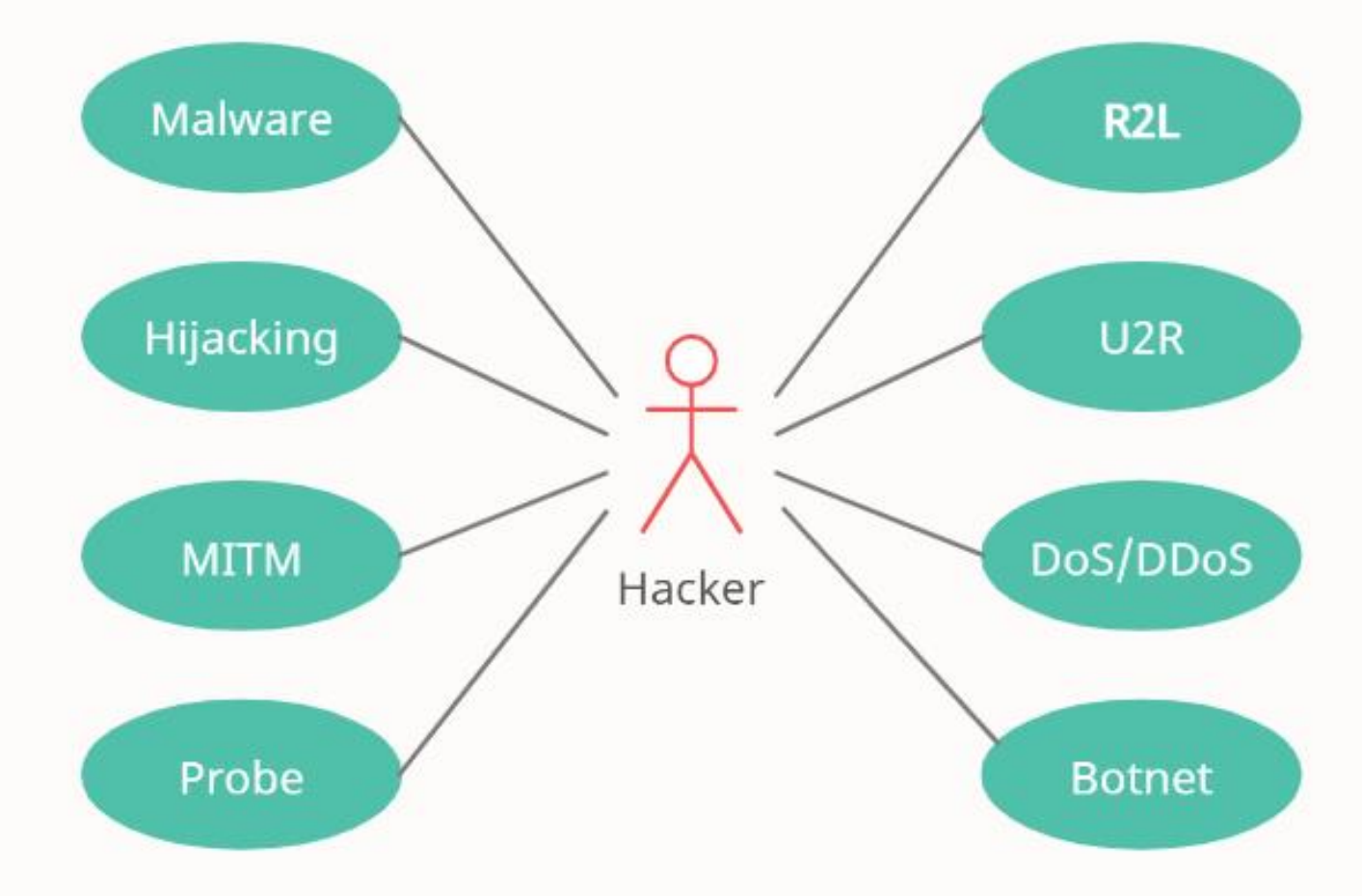
- Мережа 5G/6G може підтримувати різні сценарії використання, і кожен з них може обслуговуватися одним або декількома сегментами мережі.
- Горизонтальні варіанти використання також можуть обслуговуватися виділеними або спільними сегментами мережі.
- Кожен фрагмент мережі володіє логічно ізольованими обчислювальними

- Мережеві KPI: мобільність, доступність, пропускна здатність, затримка, джиттер тощо.
- KPI безпеки: доступність, конфіденційність, цілісність
- NF - мережеві функції (SMF, UPF, UDM тощо)
- K1. K2. K3 - ключі безпеки

Пропоноване архітектурне рішення

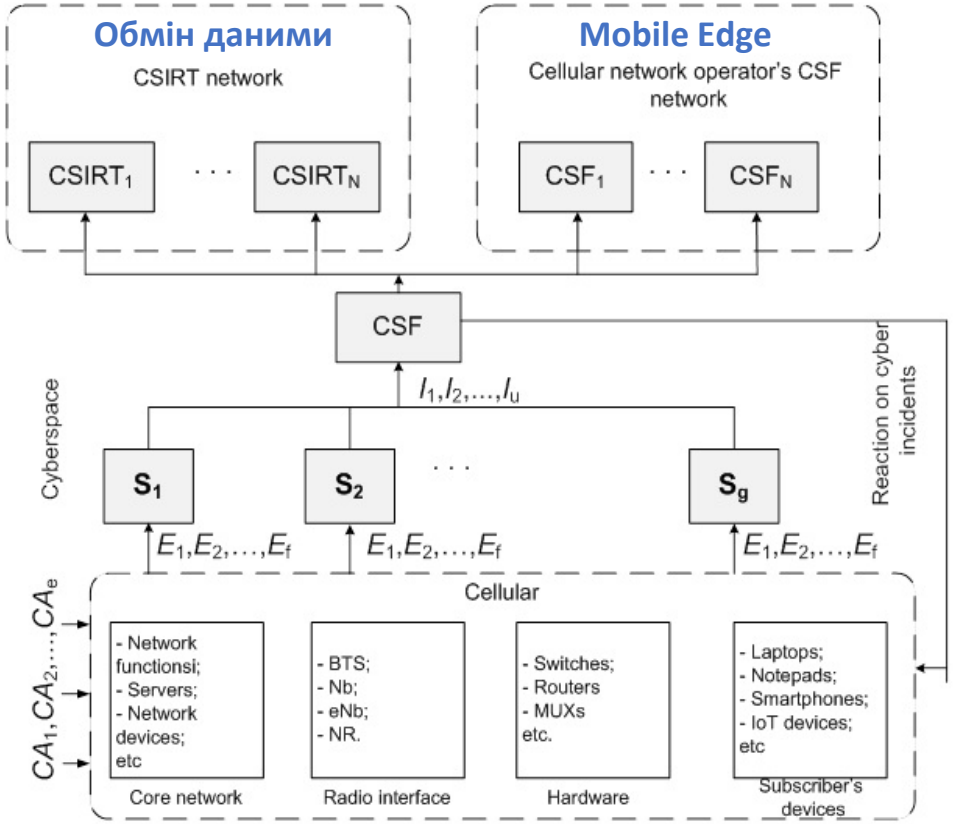


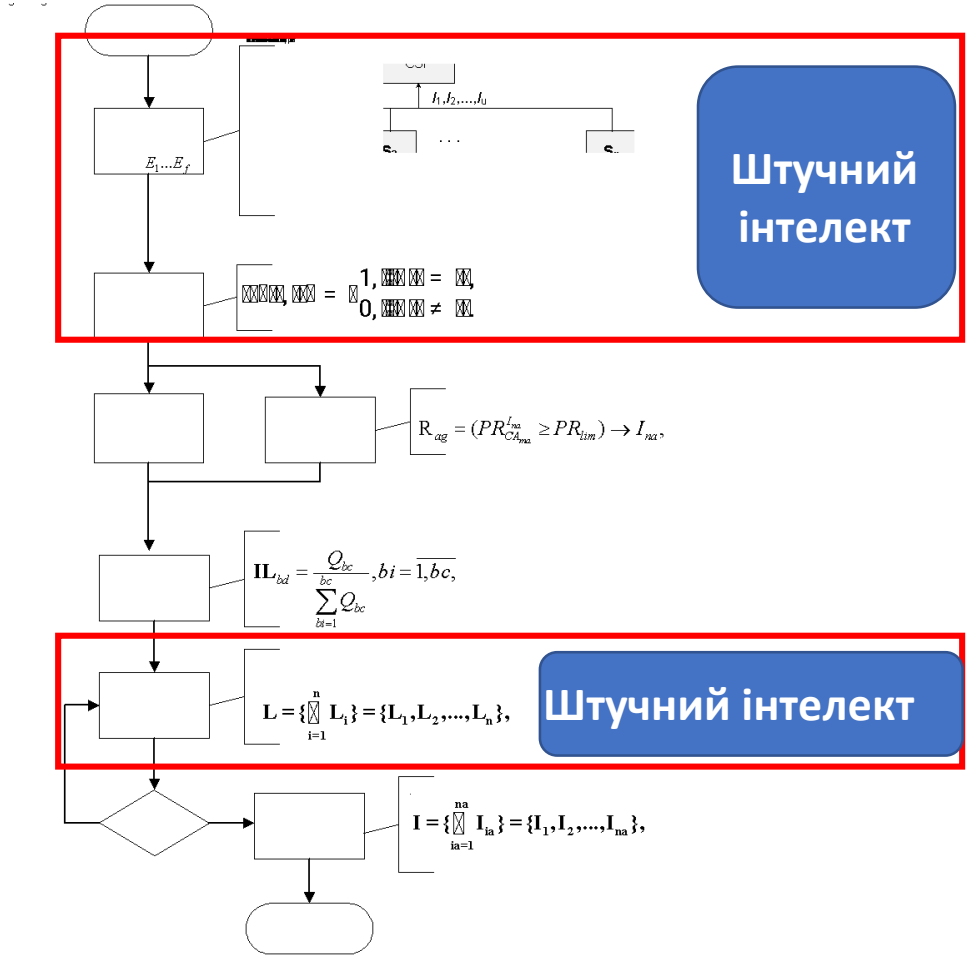
Типові випадки використання



Гнатюк С.О., Одарченко Р.С, Сімахова А.О, м. Київ, 2025 р.

Реалізація запропонованого підходу





E1... Ef - події інформаційної безпеки;
CA1... CAe - кібератаки;
S1 ... Sg - мережеві датчики;
I1 ... Iu - кіберінциденти.

Тестування рішень на основі ШІ

```
class IDS:
    def __init__(self, file_name, model_type, file_name2=None):
        import pandas as pd

        def encode_text_dummy(df, name):
          dummies = pd.get_dummies(df[name])
          for x in dummies.columns:
              dummy_name = str(name)+ "-" +str(x)
              df[dummy_name] = dummies[x]
          df.drop(name, axis=1, inplace=True)

        def encode_numeric_zscore(df, name, mean=None, sd=None):
          if mean is None:
              mean = df[name].mean()

          if sd is None:
              sd = df[name].std()

          df[name] = (df[name] - mean) / sd

        def expand_categories(values):
            result = []
            s = values.value_counts()
            t = float(len(values))
            for v in s.index:
                result.append("{}:{}%".format(v,round(100*(s[v]/t),2)))
            return "[{}]".format(",".join(result))

        def analyze(df):
            print()
            cols = df.columns.values
            total = float(len(df))

            print("{} rows".format(int(total)))
            for col in cols:
                uniques = df[col].unique()
                unique_count = len(uniques)
                if unique_count>100:
```

```
ast_flag done
22542, 122)
oved1 ========== aq
125971, 127) (22542, 122)
2020-11-29 14:46:59.332580: W tensorflow/stream_executor/platform/default/dso_loader.cc:59] Could not load dynamic library 'cudart64_101.dll'; dlerror: cudart64_101.dll not found
2020-11-29 14:46:59.334156: I tensorflow/stream_executor/cuda/cudart_stub.cc:29] Ignore above cudart dlerror if you do not have a GPU set up on your machine.
utcome
ack          956
uffer_overflow    30
...
arezclient       890
arezmaster        20
ame: outcome, Length: 23, dtype: int64
2020-11-29 14:47:08.336086: W tensorflow/stream_executor/platform/default/dso_loader.cc:59] Could not load dynamic library 'nvcuda.dll'; dlerror: nvcuda.dll not found
2020-11-29 14:47:08.337014: W tensorflow/stream_executor/cuda/cuda_driver.cc:312] failed call to cuInit: UNKNOWN ERROR (303)
2020-11-29 14:47:08.349456: I tensorflow/stream_executor/cuda/cuda_diagnostics.cc:169] retrieving CUDA diagnostic information for host: DESKTOP-O1O4SGV
2020-11-29 14:47:08.350511: I tensorflow/stream_executor/cuda/cuda_diagnostics.cc:176] hostname: DESKTOP-O1O4SGV
2020-11-29 14:47:08.353492: I tensorflow/core/platform/cpu_feature_guard.cc:142] This TensorFlow binary is optimized with oneAPI Deep Neural Network Library (oneDNN)to use the following CPU instructions in performance-critical
perations:  AVX2
o enable them in other operations, rebuild TensorFlow with the appropriate compiler flags.
2020-11-29 14:47:08.448281: I tensorflow/compiler/xla/service/service.cc:168] XLA service 0x2223ac56f70 initialized for platform Host (this does not guarantee that XLA will be used). Devices:
2020-11-29 14:47:08.449490: I tensorflow/compiler/xla/service/service.cc:176]   StreamExecutor device (0): Host, Default Version
poch 1/1000
```

Тип атаки	Кількість атак	Виявлення атак
LAND	100	**96**
NEPTUNE	100	**98**
POD	100	**100**
SMURF	100	**91**
…	…	…
MSSQL	100	**84**
Portmap	100	**97**

ПІДХІД:

1. Два набори даних DOS:

DOS1: 'LDAP', 'MSSQL', 'NetBIOS', 'Syn', 'UDP', 'UDPLag' (380 МБ) -.

DOS2: атака 'Portmap' (85 МБ, будемо називати її 'Portmap') -.

2. Набір даних NSL-KDD розділений на тестовий (навчальні дані - 90% інформації) та тренувальний (10% інформації).

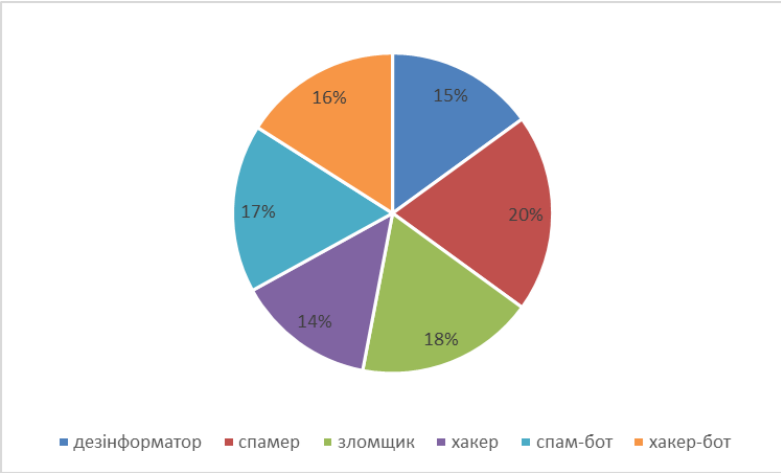
3. Набори даних DOS1 та DOS2 також були розбиті на два набори даних, кожен з яких: навчальний набір даних містить 80% даних, а тестовий набір даних, відповідно, 20% даних.

Результати: Цей метод було обрано для генерування розбиття даних. Точність моделі у випадку NSL-KDD є найкращою після процесу навчання. Ми навчаємо модель з кожним набором даних окремо на наборі 0.9611049372916336, у випадку DOS1 - 0.9937894736842106, а у випадку DOS2 - 0.9998956703182055.

Середня точність = 90%

Виявлення цілеспрямованих атак в кіберпросторі

Розроблено систему виявлення атак та ідентифікації зловмисників, у тому числі на об'єктах критичної інфраструктури держави. Визначено основні фактори, що впливають на вибір найбільш ефективного методу розрахунку коефіцієнтів важливості для підвищення об'єктивності та простоти експертного оцінювання безпекових подій у кіберпросторі. Запропоновано методику проведення експериментального дослідження, в якій визначено мету та завдання експерименту, вхідні та вихідні параметри, гіпотезу та критерії дослідження, достатність об'єктів експерименту та послідовність необхідних дій.

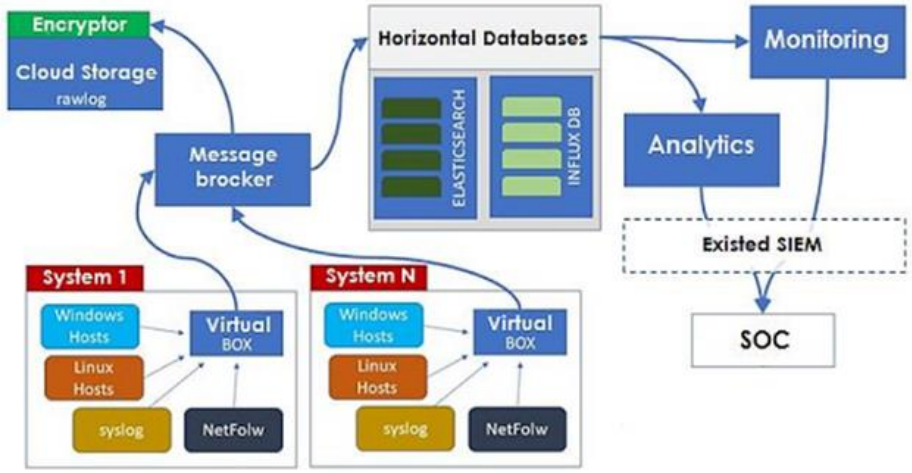


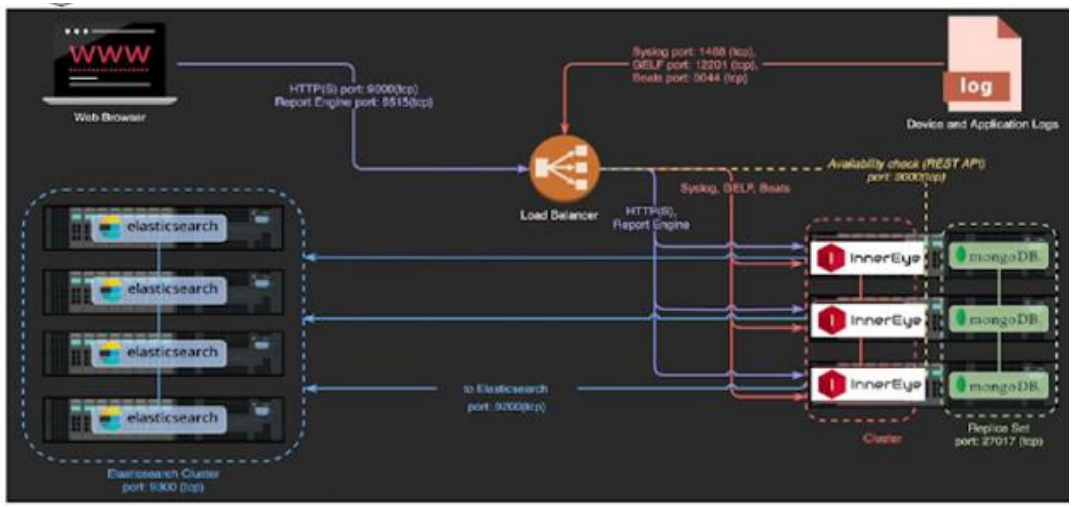
В ході експерименту відповідно до заданих параметрів мережі та хостів, було змодельовано 300 000 поточних станів кіберпросторового середовища, з яких 207 були характерними для дій певних категорій зловмисників. Управління всіма поточними станами середовища здійснювалося з використанням 50625 правил, при цьому загальний розподіл виявлень у відсотках за категоріями виглядає наступним чином: дезінформатор (15%), спамер (20%), зломщик (18%), хакер (14%), спам-бот (17%), хакер-бот (16%).

Гнатюк С.О., Одарченко Р.С, Сімахова А.О, м. Київ, 2025 р.

Кібербезпека критичної інформаційної інфраструктури держави

Розроблено систему кореляції подій та управління інцидентами кібербезпеки (СКУІК), що автоматизує процес визначення пріоритетів загроз безпеці та порушень вимог інформаційної безпеки на основі аналізу та кореляції подій. Вона аналізує всі входи та виходи із системи, доступ до ресурсів, запити до баз даних, транзакції тощо. СКУІК забезпечує: збір, зберігання та аналіз подій із будь-яких джерел у потрібний час; виявлення аномалій або несанкціонованих дій на основі аналізу подій; настроювані графічні панелі для моніторингу подій; API для інтеграції зі сторонніми системами та сервісами. СКУІК відзначається високою гнучкістю та горизонтальною масштабованістю. Для зберігання подій використовується NoSQL СУБД Elasticsearch, а для конфігураційних даних та правил – NoSQL СУБД MongoDB.





Гнатюк С.О., Одарченко Р.С, Сімахова А.О, м. Київ, 2025 р.

Групування країн Центральної та Східної Європи за потенціалом цифровізації

Група	Країни	Індикатор	Група за доходом
Високий потенціал цифровізації	Швейцарія, Німеччина, Австрія, Словенія	NRI рейтинг ≤ 27, DSGI рейтинг ≤ 40,	Високий дохід
Середній потенціал цифровізації	Румунія, Болгарія, Польща, Словаччина, Угорщина, Хорватія, Сербія, Чехія	28≤ NRI рейтинг ≤ 60, 41≤ DSGI рейтинг ≤ 67,	Високий дохід, Вище за середній дохід
Нижче за середній потенціал цифровізації	Україна, Молдова	NRI рейтинг > 60, DSGI рейтинг >68	Вище за середній дохід, Нижче за середній дохід

Для підвищення рівня цифровізації України необхідно створювати пільги та субсидії для цифрового бізнесу та цифрових розробок, сприяти державно-приватному партнерству у цій сфері та залученню іноземних інвестицій в цій напрям, створення кластерів бізнес-університет, розвиток цифрової інфраструктури

Гнатюк С.О., Одарченко Р.С, Сімахова А.О, м. Київ, 2025 р.

Схема економічного відновлення та встановлення економічної безпеки для України та країн Європи в повоєнний період

Ключовим фактором післявоєнного розвитку України, підвищення рівня життя населення та повернення українців є стимулювання розвитку цифровізації та розвитку малого та середнього бізнесу, як основи економіки. Цифровізація позитивно впливає й на підвищення конкурентоспроможності економіки через розвиток електронної торгівлі, ефективне використання штучного інтелекту, нових наукових досягнень.

Гнатюк С.О., Одарченко Р.С, Сімахова А.О, м. Київ, 2025 р.

Масштаби реалізації та практична значимість:

- Отримані результати пройшли апробацію та обговорювалися на міжнародних науково-технічних конференціях в Україні та за її межами, зокрема в Німеччині, США, Латвії, Польщі, Грузії та Казахстану. За тематикою роботи опубліковано 43 публікацій у зарубіжних наукових виданнях, які індексуються у міжнародних наукометричних базах Scopus та Web of Science.
- Отримано 3 патенти інших країн на винахід. Отримано 5 свідоцтв про реєстрацію авторського права на твір.
- Результати роботи було впроваджено в навчальний процес Державного некомерційного підприємства “Державний університет “Київський авіаційний інститут” під час викладання дисциплін: “Стільникові мережі 5G”, “Мережі та технології радіодоступу”, “Інформаційна безпека держави”, “Інформаційні та телекомунікаційні мережі”, “Соціально-економічна діагностика в умовах глобалізації”, “Міжнародні стратегії економічного розвитку”.
- Результати наукової роботи були використані під час діяльності Асоціації «Космос», зокрема, положення щодо сталого розвитку повоєнної економіки України, напрямків покращення кібербезпеки держави в умовах глобальних викликів, перспектив інформаційно-комунікаційних технологій для підвищення конкурентоспроможності України (довідка №05/05 від 14.05.2024).
- Окремі результати роботи були використані у діяльності Ради молодих учених при Міністерстві освіти і науки України (довідка РМУ при МОН № 2530 від 11.05.2024) та ВГО «Інноваційний університет» (довідка ВГО “Інноваційний університет” №1229 від 13.05.2024).

Висновки:

- Процеси цифровізації та кібербезпеки відіграватимуть важливу роль у післявоєнній цифровізації системи безпеки європейських країн. У післявоєнний період як для України, так і для Європи важливим буде подолання економічної, енергетичної, міграційної, продовольчої та демократичної кризи. Важливе значення у цьому процесі матиме побудова нової європейської стратегії безпеки (у трикутнику НАТО-ЄС-Україна).
- Представлено новий метод оцінки рівня кібербезпеки критичної інформаційної інфраструктури держави.
- Запропоновано напрямки підвищення ефективності функціонування мережі стільникового оператора. Удосконалено механізм забезпечення кібербезпеки стільникових мереж 5G.
- Розроблено систему для виявлення кібератак та ідентифікації зловмисників, зокрема на об'єктах критичної інфраструктури держави. Визначено ключові чинники, що впливають на вибір оптимального методу обчислення коефіцієнтів важливості, з метою підвищення об'єктивності та спрощення експертного оцінювання кіберінцидентів.
- Робота містить пропозиції щодо післявоєнної відбудови України, підвищення рівня кібербезпеки.