УДК 621
DOI https://doi.org/10.32782/2663-5941/2023.2.1/19

Цяпа С.М.
Український науково-дослідний інститут спеціальної техніки та судових експертиз
Служби безпеки України

КОМПЛЕКСНА МЕТОДИКА ЗАХИСТУ ІНФРАСТРУКТУРИ МЕРЕЖІ МОБІЛЬНОГО ЗВ'ЯЗКУ 5G

Проведено аналіз потенційних загроз неавторизованого доступу, несанкціонованого внесення змін у набори потокових даних, блокування функцій програмної платформи та контроль інформаційного каналу, що мають бути враховані при побудові стратегії захисту інфраструктури мережі мобільного зв'язку 5G. Зазначено, що складність задачі пов'язана з багаторівневою структурою мережі, що включає у себе необхідність визначення загроз на рівні мобільного пристрою користувача, радіоінтерфейсу, граничної мережі, транспортної мережі зв'язку, основного домену та зовнішніх інформаційних вузлів. Запропонована комплексна методика захисту відповідних рівнів інфраструктури, що включає у себе організацію програмно-конфігурованої мережі, застосування алгоритмів на основі віртуалізації мережевих функцій та впровадження квантових каналів розподілу ключів шифрування. У результаті дослідження було визначено ефективність захисту інфраструктури від (i) програм-ботів, атаки посередника, DOS/DDoS-атаки, внесення змін у код програмних додатків, втручання у роботу апаратно-програмної платформи, впровадження шкідливого програмного забезпечення; (ii) радіоглушіння, атаки посередника та перехоплення трафіку на рівні радіоінтерфейсу; (iii) загроз для архітектури граничних обчислень з множинним доступом, включення зловмисниками додаткових інформаційних вузлів, атаки побічного каналу, а також проблем з контролем доступу та аутентифікацією на рівні граничної мережі; (iv) DOS/DDoS-атаки, втручання у набір даних користувача, загроз для архітектури граничних обчислень з множинним доступом на рівні транспортної мережі зв'язку; (v) загроз пов'язаних з застосуванням прикладного програмного інтерфейсу і поділення мережі, віртуалізацією апаратних ресурсів, DOS/DDoS-атаки, неавторизованого доступу на рівні основного домену; (vi) вразливостей зовнішніх апаратних ресурсів і програмних додатків хмарних сервісів, програм-ботів, загроз пов'язаних з застосуванням прикладного програмного інтерфейсу і включенням у загальну мережу роумінг-партнерів на рівні зовнішніх інформаційних вузлів.

Ключові слова: *мережі мобільного зв'язку 5G, стратегія захисту, квантовий розподіл ключів, хмарні сервіси, граничні обчислення, віртуалізація мережевих функцій, програмно-конфігурована мережа.*

Вступ

Широкі функціональні можливості мережі мобільного зв'язку 5G зумовлюють складність відповідної архітектури [1-5], що включає у себе інфраструктуру базових станцій та центрів обробки даних, вузли ретрансляторів, організовані відповідно протоколів радіозв'язку, інформаційні вузли мобільних пристроїв користувачів мережі, а також сторонні сервіси, що використовуються при обробці потокових даних. Водночас дослідники зазначають, що на кожному з рівнів мережі існує високий ризик проведення кібератаки з метою перехоплення даних користувача та провайдера з метою їх нелегального використання або внесення несанкціонованих змін, а також порушення стабільної роботи інформаційних каналів і сервісів обробки даних [6, 7]. Таким чином, організація мережі мобільного зв'язку 5G має включати у себе комплексний аналіз можливих сценаріїв реалізації кібератак та впровадження системи захисту, налаштування якої відбувається відповідно показників ефективності виявлення загроз, навантаження на обчислювальний ресурс апаратно-програмної платформи та необхідності роботи у режимі реального часу. Важливість виконання зазначених вимог при цьому вказує на ***актуальність задачі*** розробки універсальної схеми, що складається з мінімального набору алгоритмів, об'єднання яких надасть можливість протидіяти повному спектру потенційних загроз.

Як показав ***аналіз наукових досліджень*** присвячених проблемам захисту розширеної інфраструктури мережі мобільного зв'язку 5G на всіх рівнях, що були вказані вище, високою ефективністю характеризується впровадження архітектури програмно-конфігурованої мереж (SDN: Software Defined Networks) та віртуалізації мережевих функцій (NFV: Network Function

Virtualizations), що має бути враховано при розробці стратегії захисту [8-14]. Відповідні підходи є надзвичайно гнучкими можуть бути застосовані для багатьох типів архітектури каналів передачі даних мережі радіозв'язку, як то схемах «множинні входи і множинні виходи» (MIMO: Multiple-Input Multiple-Output), при неортогональному множинному доступі (NOMA: Non-Orthogonal Multiple Access), у мережі безпосередньої передачі між парами складових (D2D: Device-to-Device), а також при застосуванні процедури розшарування мережі (NS: Network Slicing). Також можна вказати, що активне застосування хмарних сервісів надає можливість застосувати систему квантових обчислень, зокрема, налаштувати квантовий розподіл ключів шифрування (QKD: Quantum Key Distributed) і побудувати багаторівневу систему аутентифікації з квантовими каналами [15-20]. При цьому можна вказати на необхідність побудови цілісної методології захисту мережі мобільного зв'язку 5G від зовнішніх загроз, що базується на SDN, NFV, а також включенні у інфраструктуру мережі квантових каналів та платформи квантових обчислень, і протоколів, що забезпечують виконання стандартів політики конфіденційності, з мінімізацією навантаження на обчислювальний ресурс апаратно-програмної платформи та часу обробки потокових даних, що розглядається як ***невирішена частина загального дослідження***.

Таким чином, ***метою роботи*** стала побудова та оцінка відповідно цільових показників ефективності комплексної методики організації мережі мобільного зв'язку 5G, що забезпечує повний захист її функціональних складових на рівні мобільного пристрою користувача, радіоінтерфейсу, граничної мережі, транспортної мережі зв'язку, основного домену та зовнішніх інформаційних вузлів.

1. Методика захисту інфраструктури мережі шляхом організації SDN, впровадження NFV та налаштування QKD

Як було вказано вище, сучасна парадигма ефективного функціонування та захисту мережевих компонент полягає у їх віртуалізації. При організації SDN проводиться віртуалізація обчислювальних ресурсів апаратної платформи сервісу, управління якими надалі здійснюється централізовано згідно з таблицями маршрутизації у рамках однієї операції відповідно до заданого стандарту OpenFlow або його аналогів [8-14]. Це надає можливість ефективно визначити вразливі вузли мережевої інфраструктури, налаштувати захист системи від загроз пов'язаних з перевантаженням внаслідок кібератак або пікових навантажень при обробці потокових даних, а також загроз контролю зловмисниками окремих інформаційних каналів і вузлів. При цьому, впровадження NFV надає можливість провести процедуру віртуалізації класів функцій мережевих вузлів через об'єднання та поділення груп котрих проводиться оптимізація та масштабування структури програмної платформи сервісу. Функція віртуальної мережі (VNF: Virtualized Network Function) застосовується для комплексу віртуальних машин, відповідно яких централізовано обирається програмне забезпечення, що спрощує розгортання, налаштування та модифікацію програмної платформи, а також системи забезпечення стабільної роботи комплексу відповідно балансування навантаження і реагування на зовнішні загрози у режимі реального часу [8-14]. Це надає можливість збільшити гнучкість керування мережевою інфраструктурою та зменшити загальний кошторис її експлуатації.

Своєю чергою, впровадження в інфраструктуру мережі мобільного зв'язку 5G квантових каналів з метою налаштування QKD надає можливість досягти максимального рівня ефективності шифрування, при якій перехоплення потокових даних можливо лише за умов повного контролю як інформаційного, так і квантового каналу з боку зловмисника. Відповідно до базової схеми, представленої на рис. 1, розподіл ключа шифрування між двома інформаційними вузлами «X» і «Y» відбувається на базі як квантового, так і класичного інформаційного каналу відповідно до наступного алгоритму:

1. На інформаційному вузлі «А» формується випадкова бітова послідовність ключа шифрування $\{x_i\}$ де кількість $i \in [1; I]$ фіксованою.

2. На інформаційних вузлах «А» і «В» незалежно один від одного для кожного елементу послідовності $\{x_i\}$ випадковим чином обирається базис квантового стану, що складають бітові послідовності $\{a_i\}$ $\{b_i\}$ відповідно, де $i \in [1; I]$ На інформаційному вузлі «А» бітова послідовність ключа шифрування $\{x_i\}$ одується через квантові стани елементарних частинок відповідно базису $\{a_i\}$ передається на інформаційний вузол «В», де зчитується відповідно базису $\{b_i\}$

3. Зважаючи на те, що зчитування квантового стану i а інформаційному вузлі «В» може відбуватись лише при збігу станів a_i а b_i у процесі зчитування бітова послідовність $\{x_i\}$ корочується до бітової послідовності $\{y_j\}$ де. $j \in [1; J]$, причому $J \ll I$

4. Для того, щоб на інформаційному каналі «А» можна було здійснити перехід $\{x_i\} \to \{y_j\}$ з каналу «В» через класичний інформаційний канал передається бітова послідовність $\{b_i\}$ що надає можливість визначити значення. i , для яких базиси не збігаються, і видалити з бітової послідовності $\{x_i\}$ ідповідні значення. x_i .

За умови перехопленні зловмисником даних квантового каналу стани частинок зміняться, що порушить процедуру розподілу ключів і цей факт буде зафіксовано системою захисту. Своєю чергою, перехоплення набору $\{b_i\}$ рамках стандартного інформаційного каналу без наборів $\{a_i\}$ $\{x_i\}$ е надає зловмиснику можливість перехопити жоден з елементів послідовності $\{y_j\}$ навіть визначити їх загальну кількість J Таким чином, при регулярному виконанню процедури оновлення ключа шифрування і відсутності можливості повного контролю зловмисником обох каналів відповідний канал передачі даних можна вважати повністю захищеним.

2. Визначення зовнішніх загроз багаторівневої структури мережі мобільного зв'язку 5G

Для визначення зовнішніх загроз багаторівневої структури мережі мобільного зв'язку 5G необхідно провести формалізацію рівнів інфраструктури, інформаційні вузли та канали яких можуть бути використані при проведенні атаки з боку зловмисника. Відповідно до проведеної у рамках дослідження класифікації були виділені наступні потенційні загрози мережевої інфраструктури (рис. 2):

- загрози на рівні мобільних пристрів користувачів (DAS: Device Attack Segment), які представляють собою окремі інформаційні вузли з окремими апаратно-програмними платформами і програмними додатками, що характеризують їх вразливість до зовнішньої атаки;
- загрози на рівні радіоінтерфейсу (AI-AS: Air Interface Attack Segment) мережі мобільного зв'язку;
- загрози на рівні граничної мережі (EN-AS: Edge Network Attack Segment) як частини інфраструктури мережі мобільного зв'язку, обчислювальний ресурс та положення інформаційних вузлів якої дозволяє зменшити навантаження на головні сервери та відповідні інформаційні канали при обробці запитів користувачів;
- загрози на рівні транспортної мережі зв'язку (BH-AS: Backhaul Attack Segment), як частини

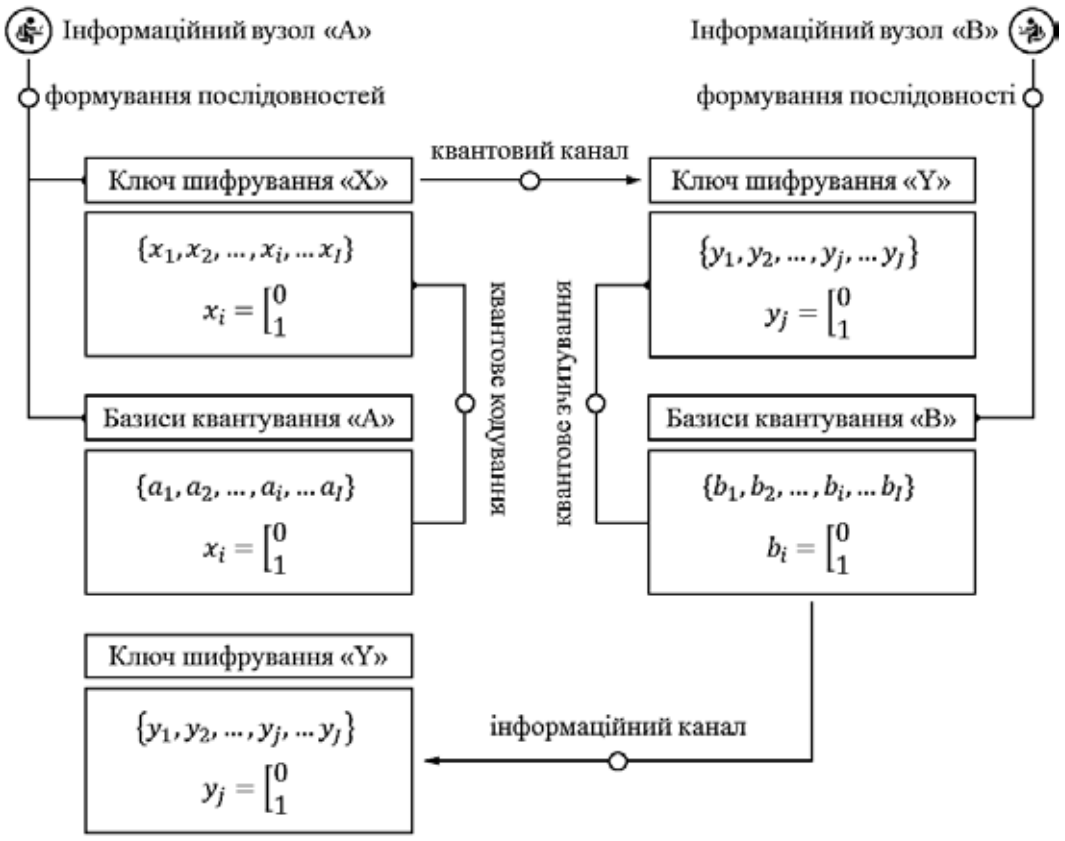

Рис. 1. Узагальнена схема квантового розподілу ключів між інформаційними вузлами «А» і «В»

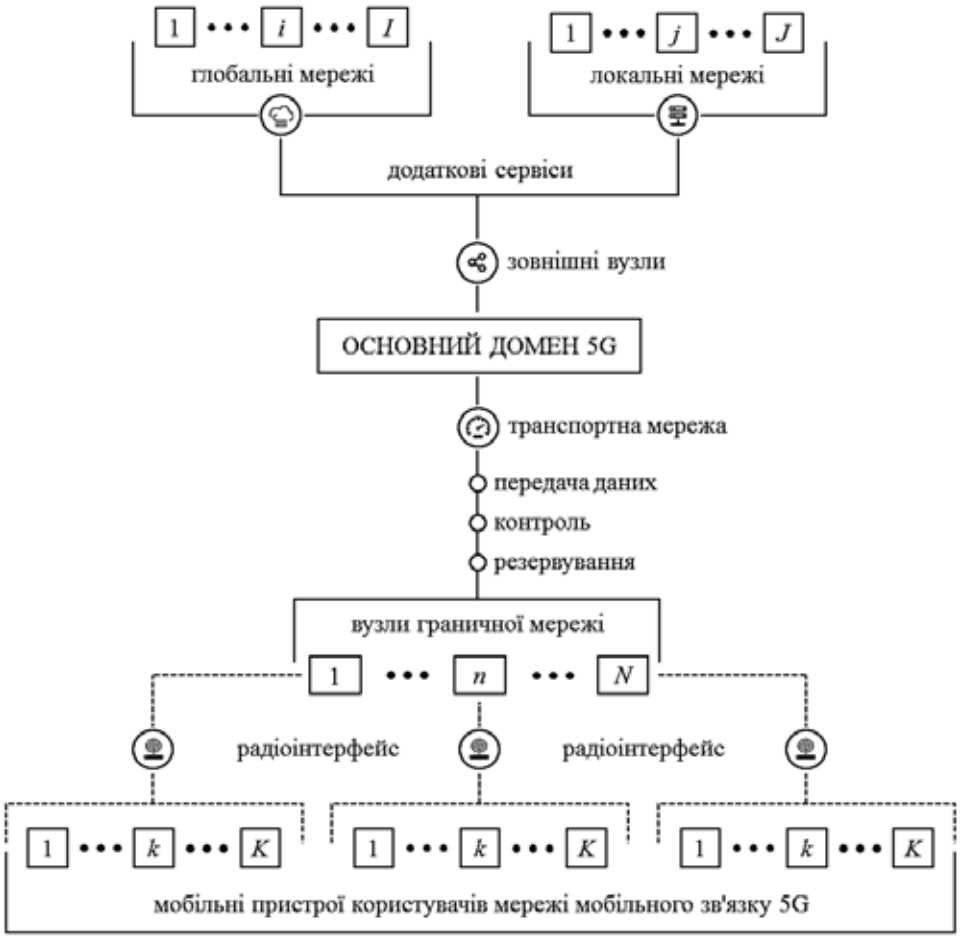

Рис. 2. Діаграма рівнів загроз інфраструктури мережі мобільного зв'язку 5G

інфраструктури мережі мобільного зв'язку, що забезпечує передачу, контроль та резервування потокових даних, які передаються до базової станції;

• загрози на рівні основного домену 5G (5GC-AS: 5G Core Network Attack Segment), що виступає як центральний сегмент мережі, який організує роботу всього комплексу мережі мобільного зв'язку відповідно базових протоколів та політики конфіденційності;

• загрози на рівні зовнішніх по відношенню до основної інфраструктури мережі радіозв'язку інформаційних вузлів (EN-AS: External Network Attack Segment), що надає можливість включити сервіси додаткових локальних і глобальних мереж.

Для побудови та оцінки ефективності методики організації мережі мобільного зв'язку 5G, що забезпечує захист інформаційних каналів і вузлів необхідно провести аналіз загроз на кожному з рівнів та визначити які з них можуть бути вирішені методами організації SDN, впровадження NFV та налаштування QKD, а також через застосування хмарних сервісів захисту.

2.1. Визначення загроз на рівні мобільних пристроїв користувачів

Рівень мобільних пристроїв користувачів є найбільш складним для прогнозування у рамках мережі мобільного зв'язку 5G. На зазначеному рівні кожен з пристроїв є інформаційним вузлом, апаратний ресурс, програмні платформа і додатки якого не можуть бути надійно оцінені, причому зміни у параметрах інформаційних вузлів та їх кількості відбуваються неконтрольовано. Важливо, що користувачі не є персоналом мережі, його поведінка може несвідомо або свідомо порушувати її роботу. Типові загрози на цьому рівні складають наступний набір:

• впровадження шкідливого програмного забезпечення та, зокрема, програм-ботів, що працюють у фоновому режимі та надають можливість встановити зовнішній контроль над функціями пристрою;

• внесення зловмисником змін у код програмних додатків, встановлених користувачем на мобільному пристрої;

• атака посередника при якій зловмисник повністю контролює інформаційний канал між інформаційними вузлами «А» і «В», і має змогу представлятись для користувача «А» користувачем «В», а для користувача «В» користувачем «А»;

• розподілені атаки типу DOS/DDoS через насичення інформаційного вузла великою кількістю зовнішніх запитів з однієї або декількох IP-адрес.

Таблиця 1

Протидія потенційним загрозам інфраструктурі мережі мобільного зв'язку 5G на рівні мобільних пристроїв користувачів

	Політика конфіден-ційності	Організація системи захисту			
		SDN	NFV	QKD	CPS
Шкідливе програмне забезпечення та боти	+	+	×	×	×
Зміни у коді програмних додатків користувача	+	×	×	×	×
Атака посередника	+	+	×	×	×
DOS/DDoS-атака	+	+	+	×	+

У табл. 1 (позначка «+» відповідає високій значимості елементу системи захисту, а позначка «×» відповідає низькій значимості елементу системи захисту) показано, що значна кількість задач вирішується через дотримання політики конфіденційності, а для стабільної роботи за умов загрози DOS/DDoS-атак і фонових програм-ботів ефективно використовується віртуалізація компонент через організацію SDN, впровадження NFV та налаштування QKD, а також через застосування хмарних сервісів захисту (CPS: Cloud Protection Service).

2.2. Визначення загроз на рівні радіоінтерфейсу

Своєю чергою, загрози при передачі даних на рівні радіоінтерфейсу полягають у неможливості контролю інформаційного каналу бездротового зв'язку. Відповідно можливості перехоплення даних, блокування інформаційного каналу, та впровадження у інформаційний канал вузла зловмисника, загрози можуть бути поділені на наступні групи:

• радіоглушіння сигналу радіомережі через передачу радіосигналів, які порушують передачу даних;

• перехоплення трафіку радіомережі між мобільним пристроєм і ретранслятором, а також між ретранслятором та базовою станцією;

• атака посередника, що виконується аналогічно до того, як було описано у попередньому підрозділі.

Таблиця 2

Протидія потенційним загрозам інфраструктурі мережі мобільного зв'язку 5G на рівні радіоінтерфейсу

	Політика конфіден-ційності	Організація системи захисту			
		SDN	NFV	QKD	CPS
Радіоглушіння сигналу радіомережі	×	+	×	+	×
Перехоплення трафіку радіомережі	+	+	×	+	×
Атака посередника	+	×	+	×	×

Як можна побачити у табл. 2 відповідні загрози цілком вирішуються через дотримання політики конфіденційності та впровадження SDN і NFV. Також на цьому етапі для захисту трафіку застосовується підхід по дублюванню інформаційних каналів квантовими, що, як було зазначено вище, не вирішує лише потенційну загрозу атаки посередника.

2.3. Визначення загроз на рівні граничної мережі

Гранична мережа є частиною інфраструктури мережі мобільного зв'язку, інформаційні вузли якої дозволяють зменшити навантаження на головні сервери та інформаційні канали при обробці запитів користувачів, що зумовлює широкий набір загроз на рівні EN-AS:

• вразливості архітектури граничних обчислень з множинним доступом (MEC: Multi-Access Edge Computing), що забезпечують ыынформацыйны канали доступу до хмарних сервісів з метою збільшення ефективності обробки запитів користувачів;

• включення у структуру мережі інформаційних вузлів зловмисників (RNT: Rouge Nodes Threats), на рівні яких здійснюється як перехоплення даних користувачів, так і внесення несанкціонованих змін;

• вразливості системи аутентифікації;

• атака побічного каналу (SCA: Side Channel Attacks), що базується на аналізі зловмисником особливості функціонування інфраструктури граничної мережі;

• вразливість неналежного контролю доступу (IAC: Improper Access Control) при якій протоколи

безпеки через помилки у специфікаціях доступу або неефективність відповідних алгоритмів надають зловмиснику доступ до окремих блоків даних або функцій граничної мережі.

Таблиця 3

Протидія потенційним загрозам інфраструктурі мережі мобільного зв'язку 5G на рівні граничної мережі

	Політика конфіденційності	Організація системи захисту			
		SDN	NFV	QKD	CPS
Вразливості архітектури MEC	×	+	+	×	×
Інформаційні вузли зловмисників	+	+	+	+	×
Вразливості системи аутентифікації	+	×	×	×	×
Атака побічного каналу	×	+	×	×	×
Неналежний контроль доступу	+	+	+	×	+

На даному рівні також більшість проблем вирішуються через належне налаштування інфраструктури мережі через впровадження SDN і NFV (табл. 3). При цьому QKD використовується для запобігання появи інформаційних вузлів зловмисників, включених у структуру мережі, а хмарні сервіси для виявлення неналежного доступу у систему при недотриманні персоналом політики конфіденційності.

2.4. Визначення загроз на рівні транспортної мережі зв'язку

Транспортна мережа зв'язку як частини загальної інфраструктури мережі забезпечує передачу, контроль та резервування потокових даних і характеризується наступним набором потенційних загроз:

• розподілені атаки типу DOS/DDoS через насичення інформаційного вузла великою кількістю зовнішніх запитів з однієї або декількох IP-адрес;

• контроль і перехоплення потокових даних користувача (CUPS: Control and User Plane Sniffing);

• вразливості архітектури транспортної мережі зв'язку з множинним доступом (Backhaul MEC);

• кібератака, що базується на внесення змін у потік керування (FMA: Flow Modification Attacks).

Таблиця 4

Протидія потенційним загрозам інфраструктурі мережі мобільного зв'язку 5G на рівні транспортної мережі зв'язку

	Політика конфіденційності	Організація системи захисту			
		SDN	NFV	QKD	CPS
Розподілені атаки типу DOS/DDoS	×	×	+	×	×
Контроль і перехоплення потокових даних	+	×	+	+	×
Вразливості MEC	×	×	+	+	×
Внесення змін у потік керування	×	×	×	×	+

Як можна побачити з таблиці 4 на рівні транспортної мережі зв'язку вже активно використовуються квантові канали, у той час як значення організації SDN та застосування хмарних сервісів є мінімальним.

2.5. Визначення загроз на рівні основного домену

Загрози на рівні основного домену 5G, що виступає як центральний сегмент мережі, який організує роботу всього комплексу апаратно-програмних платформ інформаційних вузлів мережі мобільного зв'язку, відповідно базових протоколів та політики конфіденційності включає у себе наступні категорії:

• вразливості програмного забезпечення домену 5GC;

• вразливості прикладного програмного інтерфейсу (API: Application Programming Interface), що включає у себе роботу з протоколами взаємодії з апаратними компонентами, виконання програмних алгоритмів s функціонування операційних систем;

• вразливості на рівні виконання процедури розшарування мережі на віртуальні зі спільним мережевим доменом, а також інші підходи по віртуалізації, що є особливістю саме стандарту 5G;

• розподілені атаки типу DOS/DDoS через насичення інформаційного вузла великою кількістю зовнішніх запитів з однієї або декількох IP-адрес;

• несанкціонований контроль доступу (IAC: Improper Access Control) до інфраструктури 5GC.

Як показано у табл. 5 на зазначеному рівні не використовуються квантові канали через те що не відбувається передача даних, але високу ефективність показує налаштування SDN і NFV, а також виявлення зовнішніх атак у режимі реального часу з застосування хмарних сервісів.

Таблиця 5

Протидія потенційним загрозам інфраструктурі мережі мобільного зв'язку 5G на рівні основного домену

	Політика конфіденційності	Організація системи захисту			
		SDN	NFV	QKD	CPS
Вразливості програмного забезпечення домену 5GC	×	×	×	×	+
Вразливості API	×	+	×	×	×
Вразливості віртуалізації	×	+	+	×	+
Розподілені атаки типу DOS/DDoS	×	+	+	×	+
Несанкціонований контроль доступу	+	×	×	×	+

2.6. Визначення загроз на рівні зовнішніх інформаційних вузлів

Нарешті, виявлення загроз на рівні зовнішніх по відношенню до основної інфраструктури мережі радіозв'язку інформаційних вузлів також є складною задачею, що пов'язано з тим, що у даному випадку здійснюється аналіз апаратно-програмних платформ інформаційних вузлів, над якими у провайдера немає повного контролю. У рамках дослідження запропонована наступна класифікація для категорій зовнішніх загроз:

- вразливості апаратної платформи серверних комплексів;
- вразливості хмарного сервісу, що представляють послуги платформи;
- кібератаки з застосуванням програм-ботів
- вразливості програмного забезпечення серверних комплексів;
- вразливості прикладного програмного інтерфейсу (API);
- вразливості на рівні роумінг-партнерів, які надають послуги користувачам мережі на основі угод про роумінг.

Як показано у табл. 6 на зазначеному рівні також не використовуються квантові канали через те що відповідні інформаційні канали виходять за межі інфраструктури мережі мобільного зв'язку 5G. Найбільшу ефективність показує належне виконання політики конфіденційності та налаштування SDN і NFV. Використання послуг хмарних сервісів застовується при компенсації вразливостей, що виникають при взаємодії роумінг-партнерами.

При цьому слід зазначити, що на цьому рівні, так само як і на попередніх, виконання політики конфіденційності з налаштуванням SDN і NFV з включенням у окремих випадках QKD і CPS дозволяють забезпечити повний захист від потенційних зовнішніх загроз, що надає можливість розглядати представлену методику як універсальну стратегію захисту інфраструктури мережі мобільного зв'язку 5G.

Таблиця 6

Протидія потенційним загрозам інфраструктурі мережі мобільного зв'язку 5G на рівні зовнішніх інформаційних вузлів

	Політика конфіденційності	Організація системи захисту			
		SDN	NFV	QKD	CPS
Вразливості апаратної платформи	+	×	×	×	×
Вразливості хмарного сервісу	+	×	×	×	×
Кібератаки програм-ботів	+	+	×	×	×
Вразливості програмного забезпечення	+	×	×	×	×
Вразливості API	×	+	×	×	×
Вразливості на рівні роумінг-партнерів	×	+	+	×	+

Висновки

У результаті проведеного дослідження було проаналізовано особливості побудови комплексної методики організації мережі мобільного зв'язку 5G, що забезпечує повний захист складових мережі на рівні мобільного пристрою користувача, радіоінтерфейсу, граничної мережі, транспортної мережі зв'язку, основного домену 5GC та зовнішніх по відношенню до основної мережі інформаційних вузлів.

При цьому у рамках дослідження було проведено:

- узагальнення схеми квантового розподілу ключів між інформаційними вузлами;
- визначення рівнів загроз інфраструктури мережі мобільного зв'язку 5G, а також категорій загроз, що виникають на кожному з рівнів;
- оцінка ефективності компонент системи захисту відповідно до кожної з категорій загроз.

Список літератури:

1. Behera J. R. Application of CR technique in 5G network: A smart city perspective. *Journal of Advanced Research in Dynamical and Control Systems*. 2020. Vol. 12, No SP7. P. 2383–2388. DOI: https://doi.org/10.5373/jardcs/v12sp7/20202366.

2. Sahu G., Pawar S. S. Smart Healthcare in Smart City using Wireless Body Area Network and 5G. *Networking Technologies in Smart Healthcare*. 2022. P. 1–21. DOI: https://doi.org/10.1201/9781003239888-1.

3. Liu S., Yan Z. Efficient Privacy Protection Protocols for 5G-enabled positioning in industrial IOT. *IEEE Internet of Things Journal*. 2022. Vol. 9, No 19. P. 18527–18538. DOI: https://doi.org/10.1109/jiot.2022.3161148.

4. Mustakim H. 5G vehicular network for smart vehicles in Smart City: A Review. *Journal of Computer, Electronic, and Telecommunication*. 2020. Vol. 1, No 1. DOI: https://doi.org/10.52435/complete.v1i1.44.

5. Siriwardhana Y., Porambage P., Ylianttila M., Liyanage M. Performance analysis of local 5G operator architectures for industrial internet. *IEEE Internet of Things Journal*. 2020. Vol. 7, No 12. P. 11559–11575. DOI: https://doi.org/ 10.1109/jiot.2020.3024875.

6. Overview of 5G security challenges and solutions / Ahmad I. et al. *IEEE Communications Standards Magazine*. 2018. Vol. 2, No 1. P. 36–43. DOI: https://doi.org/10.1109/mcomstd.2018.170006.

7. Agiwal M., Saxena N., Roy A. Ten commandments of emerging 5G networks. *Wireless Personal Communications*. 2017. Vol. 98, No 3. P. 2591–2621. DOI: https://doi.org/10.1007/s11277-017-4991-8.

8. Mahmoodi T. 5G and software-defined networking (SDN). 5G Radio Technology Seminar. *Exploring Technical Challenges in the Emerging 5G Ecosystem.* 2015. DOI: https://doi.org/10.1049/ic.2015.0034.

9. Kaloxylos A., Spapis P., Moscholios I. SDN-based session and Mobility Management in 5G Networks. *Wiley 5G Ref*. 2020. P. 1–17. DOI: https://doi.org/10.1002/9781119471509.w5gref223.

10. Algarni A., Thayananthan V. Improvement of 5G Transportation Services with SDN-based Security Solutions and beyond 5G. *Electronics*. 2021. Vol. 10, No 20. P. 2490. DOI: https://doi.org/10.3390/electronics10202490.

11. Feil P. Workshop on federated testbeds for NFV/SDN/5G: Experiences and feedbacks (FedTest). *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, 06-08 November 2017. Berlin : IEEE, 2017. P. 1-1. DOI: https://doi.org/10.1109/nfv-sdn.2017.8169821.

12. Barakabitze A. QoE management of multimedia services using machine learning in SDN/NFV 5G networks. *Multimedia Streaming in SDN/NFV and 5G Networks*. 2022. P. 73-97. DOI: https://doi.org/10.1002/9781119800828.ch5.

13. Cardenas A., Fernandez D. Network Slice Lifecycle Management Model for NFV-based 5G Virtual Mobile Network Operators. *2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN*), 10-12 November 2020. Leganes : IEEE, 2020. P. 120-125. DOI: https://doi.org/10.1109/nfv-sdn50289.2020.9289883.

14. Le L.-V., Lin B.-S. P., Tung L.-P., Sinh D. SDN/NFV, Machine Learning, and Big Data Driven Network slicing for 5G. *2018 IEEE 5G World Forum (5GWF)*, 09-11 July 2018. CA, Silicon Valley : IEEE, 2018. P. 20-25. DOI: https://doi.org/10.1109/5gwf.2018.8516953.

15. Bausch J. Recurrent quantum neural networks. *Curran Associates: Advances in Neural Information Processing Systems*. 2020. Vol. 33. P. 1368-1379.

16. Benedetti M., Lloyd E., Sack S., Fiorentini M. Parameterized quantum circuits as machine learning models. *Quantum Science and Technology*. 2019. Vol. 4, No 4. P. 043001. DOI: https://doi.org/10.1088/2058-9565/ab4eb5.

17. Orus R., Mugel S., Lizaso E. Quantum computing for finance: Overview and prospects. *Reviews in Physics*. 2019. Vol. 4. P. 100028.

18. The power of Quantum Neural Networks / Abbas A. et al. *Nature Computational Science*. 2021. Vol. 1, No 6. P. 403–409. DOI: https://doi.org/10.1038/s43588-021-00084-1.

19. Adnan M. H., Ahmad Zukarnain Z., Harun N. Z. Quantum key distribution for 5G networks: A review, State of Art and Future Directions. *Future Internet*. 2022. Vol. 14, No 3. P. 73. DOI: https://doi.org/10.3390/fi14030073.

20. Agiwal M., Roy A., Saxena N. Next generation 5G wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*. 2016. Vol. 18, No 3. P. 1617–1655. DOI: https://doi.org/10.1109/comst.2016.2532458.

Tsiapa S.M. A COMPREHENSIVE METHOD OF PROTECTING THE INFRASTRUCTURE OF THE 5G MOBILE COMMUNICATION NETWORK

An analysis of potential threats of unauthorized access, unauthorized changes to stream data sets, blocking of software platform functions and control of the information channel, which must be taken into account when building a strategy for protecting the infrastructure of the 5G mobile communication network, has been carried out. It is noted that the complexity of the task is related to the multi-level structure of the network, which includes the need to identify threats at the level of the user's mobile device, radio interface, edge network, communication transport network, main domain and external information nodes. A comprehensive method of protecting the relevant infrastructure levels is proposed, which includes the organization of a software-configured network, the application of algorithms based on the virtualization of network functions, and the implementation of quantum channels for the distribution of encryption keys. As a result of the study,

the effectiveness of protecting the infrastructure against (i) bots, MitM Attack, DOS/DDoS attacks, changes in the code of software applications, interference with the operation of the hardware and software platform, the introduction of malicious software and the false start of the security system on levels of the user's mobile device; (ii) radio jamming, man-in-the-middle attacks and traffic interception at the radio interface level; (iii) threats to the architecture of edge computing with multiple access, inclusion of additional information nodes by attackers, side channel attacks, and problems with access control and authentication at the edge network level; (iv) DOS/DDoS attacks, interference with the user data set, threats to the architecture of edge computing with multiple access at the level of the communication transport network; (v) threats related to the application of the application software interface and network division, virtualization of hardware resources, DOS/DDoS attack, unauthorized access at the level of the main domain; (vi) vulnerabilities of external hardware resources and software applications of cloud services, bots, threats related to the application of the application software interface and inclusion in the general network of roaming partners at the level of external information nodes.

Key words: *5G mobile communication networks, protection strategy, quantum key distribution, cloud services, edge computing, virtualization of network functions, software-configured network.*