DOI: 10.18372/2310-5461.57.17444
УДК 621.39 (045)

Р. С. Одарченко, д-р техн. наук, професор
Національний авіаційний університет
orcid.org/ 0000-0002-7130-1375
e-mail: odarchenko.r.s@ukr.net;

Д. К. Григоренко, PhD-докторант
ДержНДІ технологій кібербезпеки
та захисту інформації
orcid.org/0000-0002-5582-1346
e-mail: pc_boy@i.ua

В. О. Фесенко, PhD-докторант
ДержНДІ технологій кібербезпеки
та захисту інформації
orcid.org/0000-0002-8933-9291
e-mail: fes_vlad@ukr.net;

Т. С. Дрофа,
ТОВ «Київстар»
orcid.org/0000-0001-5846-6055
e-mail: tdekalo2@gmail.com

УДОСКОНАЛЕННЯ ЯДРА МЕРЕЖІ 5G З МЕТОЮ ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ ЗВ'ЯЗКУ

Вступ

Нові стандарти бездротового зв'язку неминуче ведуть до цифрової трансформації. Крім того, що мережі і системи 5G значно перевершують попередні покоління з точки зору пропускної здатності, вони будуть забезпечувати інфраструктуру для підтримки самих різних сервісів [1]: промисловий інтернет і інтелектуальні системи управління, автономні транспортні засоби та дрони, життєво важлива електронна охорона здоров'я та віддалена хірургія, віртуальна і доповнена реальність, віддалена діагностика та профілактичне обслуговування тощо. Число інтернет-пристроїв стрімко зростає, тому старі стандарти неминуче доводиться модернізувати. Щоб нормально працювати, багатьом пристроям необхідна більш висока пропускна здатність мережі. 5G працює на інших частотах, дає доступ в інтернет більшій кількості пристроїв, має надшвидку швидкість і мінімізує затримки при передачі даних. Такі поліпшення мережі вимагають радикально новий підхід в моделі безпеки, не схожий на використовуваний в стільникових системах до останнього четвертого покоління. Проблема безпеки в стільникових системах виникла спочатку для вирішення дуже конкретної проблеми [2, 3]: як аутентифікація користувачів, що підключаються до мережі, і захищати відповідні дані в дорозі від здатних підслуховувати радіоканал зловмисників. Для захисту мереж 5G від злому необхідно значно вдосконалити технології кібербезпеки. Одні проблеми пов'язані з самою мережею, інші – з підключеними до неї пристроями. І те й інше може бути джерелом ризику для споживачів, комерційних і державних організацій. До появи 5G в мережах було менше фізичних сполучних ланок, тому було простіше забезпечувати їх безпеку і підтримувати працездатність. Для динамічних програмно-реалізованих систем 5G потрібно більше точок маршрутизації. І для забезпечення безпеки кожну з них потрібно постійно перевіряти. Це може здатися складним, проте навіть одна незахищена ланка може підірвати безпеку інших компонентів мережі. Висока пропускна здатність вимагає перегляду методів захисту. Швидкість і продуктивність сучасних мереж обмежені, що фактично полегшує провайдерам завдання відстеження рівня захищеності мережі в реальному часі. Тому переваги розширеного діапазону 5G-мережі можуть одночасно поставити під загрозу її безпеку.

Напрямки трансформації цифрового світу

Наше суспільство стає все більш цифровим та глобально керованим. Перехід від доцифрової епохи, який відбувся лише кілька років тому, до нової цифрової реальності створює благодатний ґрунт для вчених для вивчення ландшафту, який змінюється на наших очах. Багато очікуваних

майбутніх послуг, включаючи електронне здоров'я та автономні транспортні засоби будуть критично залежати від миттєвого, практично необмеженого бездротового підключення. Очікується, що технології мобільного зв'язку досягнуть значного прогресу, ніж усе, що було досі в додатках із бездротовою підтримкою, що зробить повсякденне життя більш безпечним і значно підвищить ефективність бізнесу. Наступне покоління цифрових технологій і програмного забезпечення, яких ще не можна було уявити, ще більше змінить ринки, суспільство та повсякденне життя [3].

На відміну від попередніх поколінь комунікаційних мереж, 5G вважається наріжним каменем цифрової трансформації галузі. Найбільші економіки світу вимагають 5G як невід'ємну частину довгострокового промислового розвитку. Наприклад, Європейський Союз запропонував план 2030 Digital Compass (Цифровий компас), у якому сформульовано плани комерційної цифрової трансформації та цифровізації державних послуг. Він прийняв 5G як основу для Індустрії 4.0. Як перша країна, яка розгорнула 5G, Південна Корея ще більше зміцнила побудову конвергентної екосистеми 5G+ і просувала об'єднані послуги 5G. Японія продовжує пропагувати цінність B5G (Beyond 5G) для засобів існування людей і суспільства. Китай також висунув довгострокову мету на 2035 рік, керуючись науково-технічними інноваціями та поглибленням «5G + промислового Інтернету» як своєї важливої поточної мети [4].

Поточні можливості мережі 5G все ще недостатні, тому потрібно їх продовжувати вдосконалювати в 3GPP R18 і наступних версіях. Перш за все, у майбутньому XR (розширена реальність) стане основним бізнесом, який буде підтримувати мережа. Роздільна здатність XR не тільки буде оновлена з 8K до 16K/32K або навіть вище, бізнес-сценарії доповненої реальності (Augmented Reality) для галузевих додатків також еволюціонуватимуть від однотермінального зв'язку до спільної взаємодії з декількома XR і швидко розвиватимуться після 2025 року [5].

Багатосторонні відеодзвінки та віртуальні зустрічі, представлені дистанційною роботою, стануть нормою. Поточний режим конференції з фіксованим доступом, відео та дзвінками перетвориться на багатосторонню віддалену співпрацю мобільного доступу та мультимедійних даних і взаємодії в реальному часі в бізнесі. Наприклад, корпоративні співробітники можуть отримати доступ до середовища корпоративного офісу з віртуальними зображеннями в будь-який час вдома та спілкуватися з ними.

Таким чином, 5G-Advanced має забезпечити оновлену мережеву архітектуру та розширені можливості інтерактивного зв'язку, щоб задовольнити потреби розвитку бізнесу існуючих чітких голосових методів зв'язку, які розвиваються до повноцінних, інтерактивних та захоплюючих методів спілкування. Це також має дозволити покращити споживчий досвід.

Цифровізація галузі створила набагато складніше бізнес-середовище, ніж споживчі мережі. Підприємствам у різних галузях, таких як промисловий Інтернет, енергетичний Інтернет, шахти, порти та медичне обслуговування, потрібна мережа, щоб надати їм диференційований бізнес-досвід і надати детерміновані гарантії SLA для бізнес-результатів. Наприклад, для промислового Інтернету потрібні детерміновані затримки передачі зв'язку, які обмежені вгору та вниз, а інтелектуальні мережі потребують високоточної синхронізації годинника, високої ізоляції та високого рівня безпеки. Шахти повинні забезпечувати точне позиціонування під поверхнею, порти потребують дистанційного керування портальними кранами, а медичні заклади потребують діагностики в реальному часі та інформації про лікування, синхронізації та підтримки дистанційної діагностики з наднизькою затримкою.

Тому 5G-Advanced має повністю враховувати гарантію детермінованого досвіду для галузевих послуг, включаючи сприйняття послуг у реальному часі, вимірювання, планування та, нарешті, формування загального замкнутого контуру керування. Для різних галузей промисловості 5G має використовувати загальнодоступні мережі, локальні приватні мережі та різні режими гібридної мережі, щоб відповідати галузевим вимогам ізоляції бізнесу та безпеки даних. Таким чином, 5G-Advanced має зосередитися на архітектурі мережі, схемі мережі, формі обладнання та можливостях підтримки обслуговування, які відповідають різноманітному та складному бізнес-середовищу.

Аналіз досліджень і публікацій

Існує велика кількість літератури, присвяченої проблемам інформаційної безпеки в інформаційно-комунікаційних системах та мережах. Завдання створення, організації та дослідження процесів функціонування, вдосконалення та розвитку систем захисту інформації в тій чи іншій мірі знайшли відображення в працях ряду вітчизняних та зарубіжних вчених, серед яких Е. С. Вентцель, В. Ю. Гайкович, В. А. Галатенко, В. А. Герасименко, В. І. Гарбарчук, Ю. В. Демченко, В. І. Завгородній, В. К. Задирака, А. Г. Карпова, В. В. Лебедєва, В. В. Мельникова, А. Н. Назаров, А. С. Олексюк, А. Ю. Першин, А. З. Пєскозуб, А. П. Пятібратова, В. К. Размахнін, С. П. Расторгуєва,

Ю. А. Самохіна і багато інших. Виокремити можна праці [3, 5, 6], які присвячені оцінці систем безпеки стільникових мереж. Проте питання щодо розроблення вимог до систем захисту інформації стільникових мереж нових поколінь досить слабко розроблене вітчизняними вченими, а тому представляє великий інтерес і обґрунтовує актуальність теми дослідження. Безпека є одним з основних проблемних місць комунікаційної мережі в даний час. Розгортання жодної мережі не може відбутися без забезпечення гарантованої безпеки для всіх зацікавлених сторін, наприклад, кінцевих користувачів, постачальників послуг, віртуальних операторів, провайдерів інфраструктури. Таким чином, метою даної роботи є удосконалення ядра мереж 5G з підвищеною конфіденційністю виявлення недоліків систем захисту мереж попередніх поколінь та формування вимог до безпеки майбутніх 5G мереж в цілому та їх окремих компонентів

Постановка задач дослідження

Стандарт 4G теоретично здатний забезпечувати швидкості передачі даних на рівні понад 100 Мбіт/с швидкорухомим абонентам (наприклад, залізничний чи автомобільний транспорт) та швидкість 1 Гбіт/с абонентам з невеликою рухливістю (наприклад, стаціонарні абоненти та пішоходи) згідно з міжнародною специфікацією IMT-Advanced (International Mobile Telecommunications Advanced).

Специфіка LTE (Long Term Evolution) мереж полягає в тому, що їх можна будувати на існуючих мережах операторів GSM (Global System for Mobile communication) та WCDMA (Wideband code division multiple access), що помітно знижує вартість розгортання цих мереж. Мережі 5G взагалі здатні використовувати можливості всіх запущених стільникових мереж попередніх поколінь одночасно разом із новим радіо інтерфейсом New Radio (NR).

Саме з цієї причини оперативне вдосконалення існуючих мереж дозволить Україні, якнайшвидше інтегруватися в світовий інформаційний простір, також розгортати нові, уже з відповідністю до найсучасніших стандартів.

Виходячи з вищесказаного, можна зробити висновок: актуальне вдосконалення інфраструктури широкосмугового доступу до ресурсів мережі Інтернет в межах України, використовуючи високошвидкісні мережі п’ятого покоління можна значно підвищити їх продуктивність та розширити функціонал. Науково-технічне обґрунтоване планування й оптимізація стільникових мереж, дозволить забезпечити всі потреби користувачів з усіма показниками ефективності функціонування (швидкість передавання, затримка, безпека даних, що передаються) є досить складною науково-технічною й економічною проблемою, без вирішення якої неможливе створення інформаційної інфраструктури, що відповідає потребам розвиненого інформаційного суспільства світового рівня.

Підтримка новітніх технологій з широкосмуговим радіо доступом в сучасних стільникових мережах повинна бути реалізована з підвищеною ефективністю передачі даних, при цьому вартість доставки кожного мегабайта трафіку повинна бути знижена з підвищенням якості обслуговування (QoS), необхідного кожному типу трафіку.

Розробка нових методів, дозволятиме підняти показники ефективності функціоналу усіх типів існуючих каналів зв`язку та впровадження нових видів мереж (4 G, 5G).Також обов’язковою умовою є те, щоб вони відповідали необхідним критеріям:

– забезпечують впровадження нових систем мобільного зв’язку і підтримка існуючих (внесені інвестиції повинні бути збережені та давати результат);

– відповідають вимогам архітектури мереж наступного покоління;

– мають ефективні засоби управління трафіком і забезпечення якості надання послуг;

– забезпечують необхідний рівень безпеки даних, що передаються;

– надають зручні засоби технічного обслуговування та експлуатації.

Враховуючи вищесказане проблема полягає ще й в тому, що існуючі системи зв’язку не здатні в повній мірі забезпечити необхідну якість обслуговування та захищеність даних, що передаються урядових ліній зв’язку в умовах повсюдного поширення концепції Інтернету речей а також в умовах ведення бойових дій, гібридної війни та кібервійн. Швидкості передачі даних можуть досягати всього декількох десятків Мбіт/с, що зовсім не відповідає сучасним потребам різних груп користувачів (користувачі загальнодоступних мереж, користувачі мереж спеціального зв’язку, військові тощо). Можливим є перехоплення текстових повідомлень, прослуховування розмов, а потім використання отриманих даних як проти окремих фізичних осіб так і проти військових, уряду тощо. Це все свідчить про низьку ефективність застосованих методів планування радіомереж та недосконаліть застосовуваних технологій для передачі даних, низький рівень конфіденційності даних, що передаються , відсутність здатності до швидкого реагування на кіберінциденти та ін.

Таким чином, актуальною проблемою є розробка мережі урядового (спеціального) радіо-зв’язку

на базі концепції 5G в Україні, що надасть змогу значно підвищити рівень якості надання послуг, а також захищеність даних, що передаються.

Узгоджена архітектура ядра мережі 5G

Існуюча архітектура мережі 5G розроблена для двостороннього потоку даних необхідного розміру з високою швидкістю та надання широкого спектру послуг з використанням NVF (Network Function Virtualization – мереживна віртуалізація) та SDN (Software Defined Networking – програмно вконфігурованої мережі)

Можна визначити основні показники продуктивності мереж 5G [8, 9]:

– пікова швидкість передачі даних на лінії вниз (Downlink) – становить 20 Гбіт/с (показником спектральної ефективності на рівні 25–30 біт/с/Гц);

– на каналі Uplink- лінія вгору, максимальна швидкість передачі становитиме до 10 Гбіт/с (зі спектральною ефективністю 15 біт/с/Гц);

– мінімальна затримка в підсистемі радіо доступу для сервісів URLLC – до 1 мс, для сервісів eMBB – до 4 мс;

– максимальна щільність підключених до мережі в міських умовах пристроїв Інтернету речей – до 1 000 000 пристроїв/км^2;

– автономна робота пристроїв Інтернету речей без підзарядки акумулятора – до 8–10 років;

– підтримка мобільності при максимальній швидкості пересування об’єктів – до 500 км/год.

Для забезпечення цих вимог використовуються наступні ключові принципи до побудови архітектури мережі 5G [10].

1. Поділ мережевих вузлів на окремі складові, які забезпечують роботу протоколів в UP («площині користувачів», User Plane) та CP («площині керування», Control Plane), що значно збільшує можливість в частині масштабування і розгортання (допускаючи централізоване і децентралізоване розташування окремих складових частин вузлів).

2. Елементи мережі поділяються на шари NT – Network Slicing [6], орієнтуючись на надання послуг, що надаються конкретним групам кінцевих користувачів.

3. VNF – Virtual Network Functions, це функція що дозволяє реалізувати елементи у вигляді віртуальної мереживної функції [11].

4. Реалізація концепції хмарних та граничних обчислень (fog та edge computing), можлива завдяки підтримці одночасного доступу до централізованих і локальних служб.

5. Конвергентна архітектура, яка об’єднує різні типи мереж доступу AN (Access Network) – 3GPP (New Radio – NR) і не 3GPP (WiMAX,WiFi та інші) з єдиною опорною CN мережею (Core Network).

6. Підтримка єдиних алгоритмів і процедури автентифікації, не залежно від типу мережі доступу.

7. Можливість підтримки функцій мережі без збереження стану (stateless), де ресурс обчислення відділений від ресурсу зберігання.

8. Опція підтримки роумінгу з маршрутизацією трафіку як через домашню мережу (Home routed), так і за допомогою локального приземленням (Local breakout) в гостьовій мережі (VPLMN).

На рис. 1 зображена архітектура мережі 5G з точки зору сервіс-орієнтованого взаємодії різних мережевих функцій на площині управління.

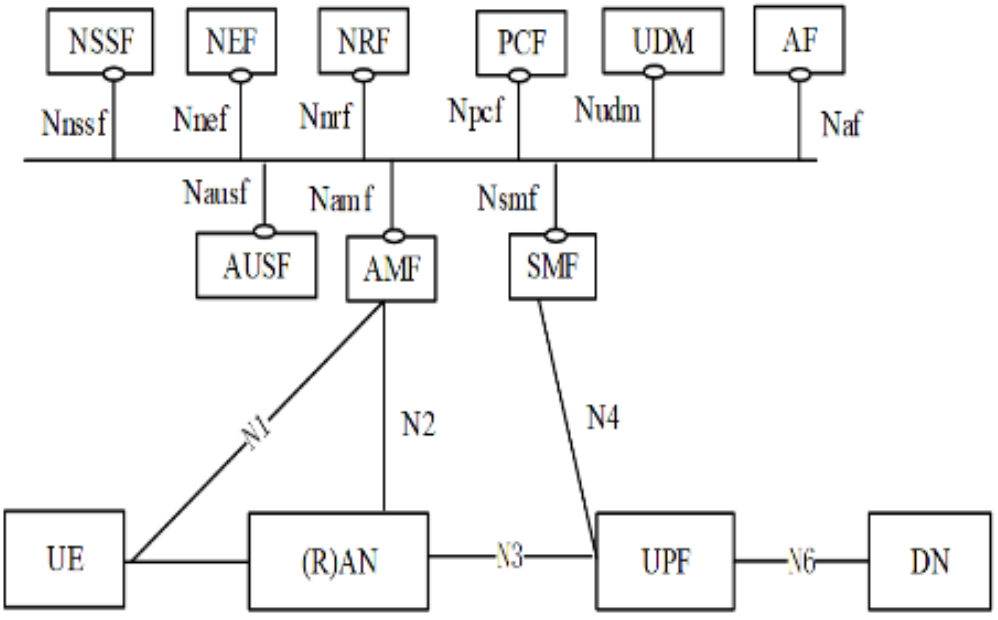

Рис. 1. Архітектура мережі 5G та взаємодія мережевих функцій

Для представлення наявної архітектури мережі 5G задаємо множину мережевих функцій **NF** :

$$\left\{\bigcup_{i=1}^{n}\mathbf{NF}_i\right\}=\{\mathbf{NF}_1,\mathbf{NF}_2,...,\mathbf{NF}_n\}, \quad (1)$$

де $\mathbf{NF}_i \subseteq \mathbf{NF}$, $(i=\overline{1,n})$, n – кількість мережевих функцій, а:

$$\mathbf{NF}_i=\left\{\bigcup_{j=1}^{m_i}\mathbf{NF}_{ij}\right\}=\{\mathbf{NF}_{i1},\mathbf{NF}_{i2},...,\mathbf{NF}_{im_i}\}, \quad (2)$$

при цьому $\mathbf{NF}_{ij}$ $(j=\overline{1,m_i})$ – підмножини мережевих функцій.

Зважаючи на (2) запишемо вираз (1) наступним чином:

$$\left\{\bigcup_{i=1}^{n}\mathbf{NF_i}\right\}=\left\{\bigcup_{i=1}^{n}\left\{\bigcup_{j=1}^{m_i}\mathbf{NF}_{ij}\right\}\right\}=$$
$$=\{\{\mathbf{NF}_{11},\mathbf{NF}_{12},...,\mathbf{NF}_{1m_1}\}, \quad (3)$$
$$\{\mathbf{NF}_{21},\mathbf{NF}_{22},...,\mathbf{NF}_{2\mathbf{m}_2}\},...,$$
$$\{\mathbf{NF}_{n1},\mathbf{NF}_{n2},...,\mathbf{NF}_{nm_n}\}\},\ (j=\overline{1,m_i}).$$

Наприклад, використовуючи [4], при $n=7$, згідно виразу (1) отримаємо наступне:

$$\left\{\bigcup_{i=1}^{7}\mathbf{NF}_i\right\}=\{\mathbf{NF_1},\mathbf{NF_2},\mathbf{NF_3},\mathbf{NF_4},\mathbf{NF_5},\mathbf{NF_6},\mathbf{NF_7}\}=$$
$$=\{\mathbf{NF}_{AUSF},\mathbf{NF}_{UDMF},\mathbf{NF}_{PCF},\mathbf{NF}_{AMF},\mathbf{NF}_{SMF},\mathbf{NF}_{AF},\mathbf{NF}_{UPF}\}= \quad (4)$$
$$=\{\mathbf{AUSF,\ UDMF, PCF, AMF, SMF, AF, UPF}\}$$

де $\mathbf{NF_1}=\mathbf{NF_{AUSF}}=\mathbf{AUSF}$, $\mathbf{NF_2}=\mathbf{NF_{UDMF}}=\mathbf{UDMF}$, $\mathbf{NF_3}=\mathbf{NF_{PCF}}=\mathbf{PCF}$, $\mathbf{NF_4}=\mathbf{NF_{AMF}}=\mathbf{AMF}$, $\mathbf{NF_5}=\mathbf{NF_{SMF}}=\mathbf{SMF}$, $\mathbf{NF_6}=\mathbf{NF_{AF}}=\mathbf{AF}$, $\mathbf{NF_7}=\mathbf{NF_{UPF}}=\mathbf{UPF}$ – мережеві функції.

Архітектура 5G передбачає два способи взаємодії між функціями мережі:

1. Сервіс-орієнтованим, – одна функція мережі (наприклад, **AMF**) дозволяє іншій авторизованій мережній функції отримувати доступ до її сервісів;

2. Частковий інтерфейс – показує, взаємодію яка існує між сервісами мережі, що взаємодіють як точка-точка (наприклад, інтерфейс N11) між будь-якими двома мережевими функціями (наприклад, **AMF** і **SMF**).

Узгоджена мережева архітектура 5G включає в себе наступні основні програмні мережеві функції та модулі (**NF**) [12]:

• управління доступом і мобільністю **AMF** (Access and Mobility Management Function);

• керування сесіями **SMF** (Session Management Function);

• передача даних користувачів **UPF** (User Plane Function);

• модуль управління даними користувачів **UDM** (Unified Data Management);

• єдина база даних **UDR** (Unified Data Repository);

• система зберігання неструктурованих даних (**UDSF** – Unstructured Data Storage Function);

• вибір мережевого шару **NSSF** (Network Slice Selection Function);

• керування політиками **PCF** (Policy Control Function);

• організація взаємодії між зовнішніми додатками **NEF** (Network Exposure Function);

• сховище функцій мережі **NRF**, **NF** Repository Function;

• прикладна функція **AF** (Application Function);

• підтримка обміну короткими текстовими повідомленнями завдяки використанню функції SMSF (SMS Function);

• функція взаємодії з мережею доступу не-3GPP стандартів (N3IWF – Non-3GPP Inter Working Function).

Розробка ядра мережі 5G для застосування в мережах урядового радіозв'язку

Таким чином, було прийняте рішення про необхідність удосконалення архітектури 5G шляхом введення додаткових безпекових функцій та відповідних процедур.

Ключові принципи архітектури для мережі урядового радіозв'язку на основі технології 5G полягають в наступному:

– розподіл мережевих функцій на елементи, які забезпечують роботу протоколів «площини спеціального користувача» (UP – User Plane) і елементи, що забезпечують роботу протоколів «площини управління» (CP – Control Plane);

– виділення мережевих шарів для різних груп спеціальних користувачів, орієнтуючись на надання послуг, що будуть надаватись різним групам користувачів урядового радіозв'язку;

– реалізація мережевих елементів у вигляді віртуальних мережевих функцій – VNF (Virtual Network Functions);

– підтримка єдиних алгоритмів і процедур аутентифікації, прийнятих у мережі урядового радіозв'язку;

– впровадження нових мережевих функцій, завдяки яким буде забезпечуватися надійність та підвищений рівень безпеки мережі урядового радіозв'язку.

Концепція безпеки мереж урядового радіозв'язку на основі п'ятого покоління базується на використанні сучасних технологій, які дають можливість передавати дані в повному обсязі, надійними каналами в повному обсязі.

На рис. 2 представлена запропонована архітектура ядра мережі. Сірим кольором позначені функціональні об'єкти, які відповідають за механізми забезпечення безпеки:

1.Функція сервера аутентифікації – AUSF (Authentication Server Function).

2.Функція наднадійної безпеки – RSF (Reliable Security Function).

3.Функція забезпечення додаткової криптографічної безпеки KSF (Cryptographic Security Function).

Першим етапом є поєднання функцій модуля управління доступом, мобільністю та безпеки, а функція KSF з єдиною базою даних UDM.

Функція аутентифікації (AUSF). Відіграє роль сервера аутентифікації та забезпечує ідентифі-кацію користувачів, оскільки термінує запити генеровані RSF та транслює їх в KSF.

Наступним кроком є узгодження і застосування політик безпеки по відношенню до конкретних користувацьких терміналів (UE).

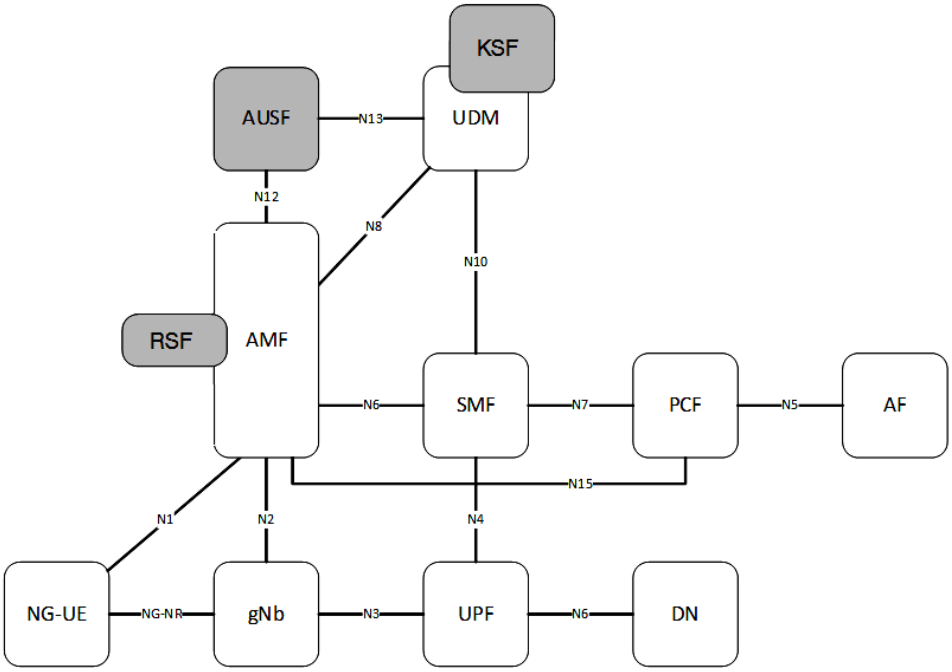

Рис. 2. Архітектура побудови опорної мережі урядового радіозв'язку

Потім відбувається процес шифрування даних і контролю їх цілісності.

KSF– розподіляє персональні секретні ключі, зберігає їх, а також параметри криптографічних алгоритмів. Всі ці дані обробляються та зберігаються в спеціальному центрі роботи з даними та інтегруються з єдиною БД UDM.

В даній архітектурі AMF функція управління доступом і мобільністю забезпечує:

– організацію роботи інтерфейсів у площині управління N1, N2;

– здійснює обмін сигналізації NAS через інтерфейс N1, де відбувається шифрування та захист цілісності сигналізації NAS;

– управління реєстрацією, призначеною для користувача терміналу (UE) в мережі і контроль можливих станів реєстрації (RM-DEREGISTERED, RM-REGISTERED);

– курування з'єднанням яке призначене для користувачів терміналу UE з мережею і контроль можливих станів з'єднання (CM-IDLE, CM-CONNECTED);

– керування доступністю, мобільністю, для користувачів терміналу UE мережі, в стані CM-IDLE та CM-CONNECTED;

– передача коротких повідомлень між користувацьким обладнанням UE та SMF, а також повідомленнями між функціями LMF – Location Management Function та RAN;

– передачу повідомлень між UE і функцією управління місцем розташування LMF (Location Management Function), а також між RAN і LMF;

– виділення ідентифікатора потоку даних EPS (Evolved Packet System) для взаємодії;

– співпраця зі стандартами 3GPP мережами доступу за допомогою модуля взаємодії Non-3GPP Inter Working Function – N3IWF.

Важливою складовою AMF є підфункція управління безпекою та наднадійною безпекою.

SMF – функція керування сесіями зв'язку, яка забезпечує:

– створення, зміна та звільнення сесії, включаючи підтримку каналу між мережею доступу UPF та AN;

– розподіл і управління IP-адресами терміналів користувачів (UE);

– вибір шлюзового з'єднання UPF;

– організація функції керування політиками (PCF);

– управління роботою шлюзу UPF, в тому числі управління застосуванням QoS – політик якості;

– динамічне налаштування терміналів користувача за допомогою протоколів DHCPv4 та DHCPv6 (сервер і клієнт);

– контроль збору тарифікаційних даних і організація інтерфейсу з системою білінгу;

– надання послуг SSC – Session and Service Continuity безперервно та без швів;

– взаємодія з гостьовими мережами в рамках процедур роумінгу.

Функція передачі даних користувачів (UPF) забезпечує:

– інтерфейс підключення до зовнішніх мереж передачі даних, в т.ч. до глобальної мережі Інтернет;

– маршрутизацію і передачу пакетів даних користувачів;

– буферизацію пакетів і ініціацію повідомлення терміналів користувачів (UE) про наявність даних для передачі по лінії вниз (DL);

– маркування пакетів даних відповідно параметрів QoS;

– надання звітів про використання трафіку.

UDM забезпечує можливість керування даними усіх користувачів:

– робота з профілями користувачів, зберігання, модифікація переліку доступних користувачам послуг і відповідних їм параметрів;

– SUPI – керування ідентифікаторами користувачів;

– генерацію облікових даних аутентифікації 3GPP AKA;

– авторизацію доступу на базі даних профілю користувача;

– управління реєстрацією користувача (тобто, зберігання обслуговуючого AMF);

– підтримку безперервності обслуговування/ сеансу зв'язку/зберігання призначених SMF / DNN для поточних сеансів зв'язку;

– управління доставкою SMS повідомлень.

При цьому кілька різних UDM можуть обслуговувати одного й того ж користувача при різних транзакціях.

Функція управління політиками (PCF) в реальному часі формує та визначає для користувача терміналів ті чи інші політики, включаючи параметри якості обслуговування (QoS) і правила тарифікації. Так, для передачі будь якого типу трафіку можуть динамічно створюватися віртуальні канали з різними характеристиками. При цьому до уваги можуть прийматися вимоги сервісу, профіль користувачів, місце розташування, рівень навантаження мережі, обсяг спожитого трафіку тощо.

AF прикладна функція мережі 5G яка взаємодіє з опорною мережею, також до прикладу здатна вирішити деякі завдання:

– управління маршрутизацією трафіку;

– регулювання доступу до модулів взаємодії елементів мережі (NEF);

– взаємодія з політиками.

Залежно від конкретного впровадження на мережі оператора зв'язку, окремі зовнішні платформи та додатки можуть мати прямий (безпосередній) доступ до функцій мережі 5G. Деякі системи будуть здійснювати доступ до мережевих функцій 5G через прикладні програмні інтерфейси API, що надаються модулем забезпечення взаємодії мережевих функцій.

Загалом безпека мережі урядового радіозв'язку включає в себе:

1) Аутентифікацію користувача з боку мережі.

2) Аутентифікацію мережі з боку користувача.

3) Узгодження криптографічних ключів між мережею і призначеним для користувача терміналом.

4) Шифрування та контроль цілісності сигнального трафіку.

5) Захист ідентифікатора користувача.

6) Аутентифікацію абонента, також захист трафіку, враховуючи рівень кінцевих сервісів.

Оскільки без проходження процесу стандартизації, не можливо вносити зміни до архітектури ядра мережі 5G, то пропонуємо винести функціонал запропонованих мережевих підфункцій KSF та RSF на спеціалізований сервер захищеного урядового зв'язку у мережі 5G (рис. 3).

Коли користувачі такої мережі географічно розподілені, різні групи абонентів можуть також обслуговуватися виділеними або спільними мережевими фрагментами. У кожному шар мережі є логічно ізольовані ресурси обчислення та зберігання для виконання завдань обробки та зберігання даних для всіх груп абонентів, які отримують їхні послуги.

В цій схемі також можна забезпечити передчу ключів для шифрування користувальницьких даних «із кінця в кінець» за допомогою, наприклад, механізмів квантового розподілу ключів (рис. 4).

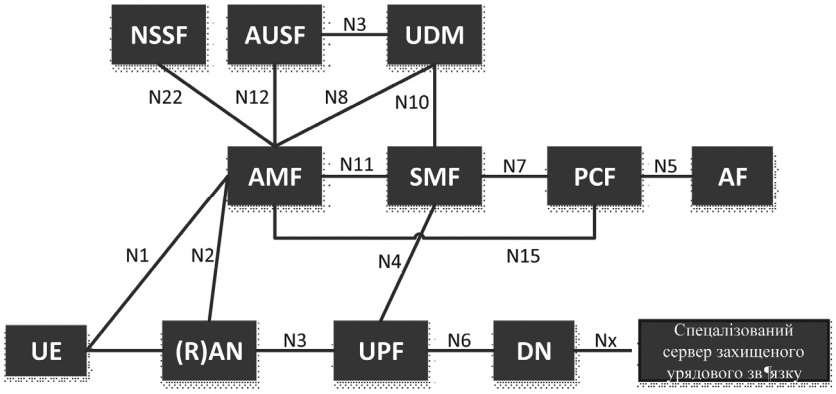

Рис. 3. Підключення спеціалізованого сервера захищеного урядового зв'язку до ядра мережі 5G

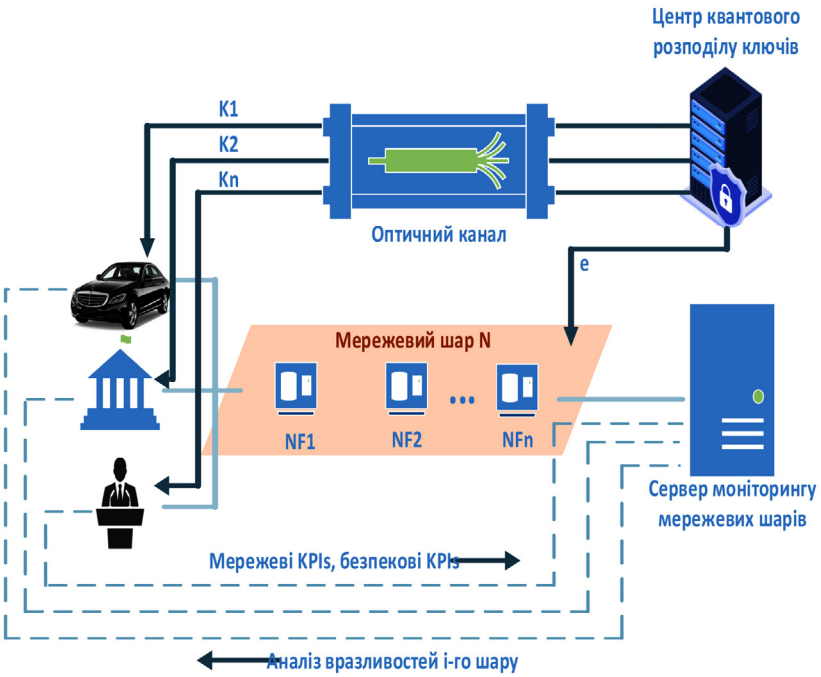

Рис. 4. Графічне представлення надання облікових даних безпеки в схемі управління ключами

Розробка процедури встановлення сеансу захищеного урядового зв'язку

Мережа урядового радіозв'язку також призначена для роботи спільно з мережами 4G. Система передбачає використання ряду макростільників, невеликих осередків та спеціалізованих систем в межах будівлі. Маленькі осередки – це міні-базові станції, призначені для дуже локалізованого покриття, (наприклад в кабінеті першої особи держави, в більшості випадків діапазон коливається від 10 метрів до кількасот метрів, що забезпечує заповнення для великої макромережі. Маленькі стільники необхідні для даної мережі, так як використання міліметрових хвиль не дає змогу забезпечити великий радіус радіопокриття.

Конкретну мережу обслуговує конкретний термінал UE, який буде користуватися лише одним мережевими шаром, який буде виділений для мережі урядового радіозв'язку. При цьому модуль AMF є загальним для всіх шарів, а інші елементи (в т.ч. SMF, UPF) будуть призначені виключно для шару урядового зв'язку.

Реєстрація в мережі передбачає встановлення RRC з'єднання (далі по тексту NAS), термінал UE передає дані до якого мережевого шару йому необхідно потрапити. На підставі отриманих від UE даних, що розміщуються в UDM профілі користувача також розташування абонента, здійснюється вибір елемента AMF, який забезпечить допустимий набір послуг. Вибір AMF здійснюється із залученням модуля вибору мережевого шару NSSF і репозиторію функцій мережі NRF.

На другому кроці призначається модуль управління сесіями SMF і далі – шлюз передачі користувацького трафіку UPF. Призначення SMF / UPF може відбуватися відповідно до статичних налаштувань, або – динамічна (через репозиторій мережевих функцій – NRF). Процес персоніфікації користувача в мережі відбувається за схемою, яка подана на рис. 5.

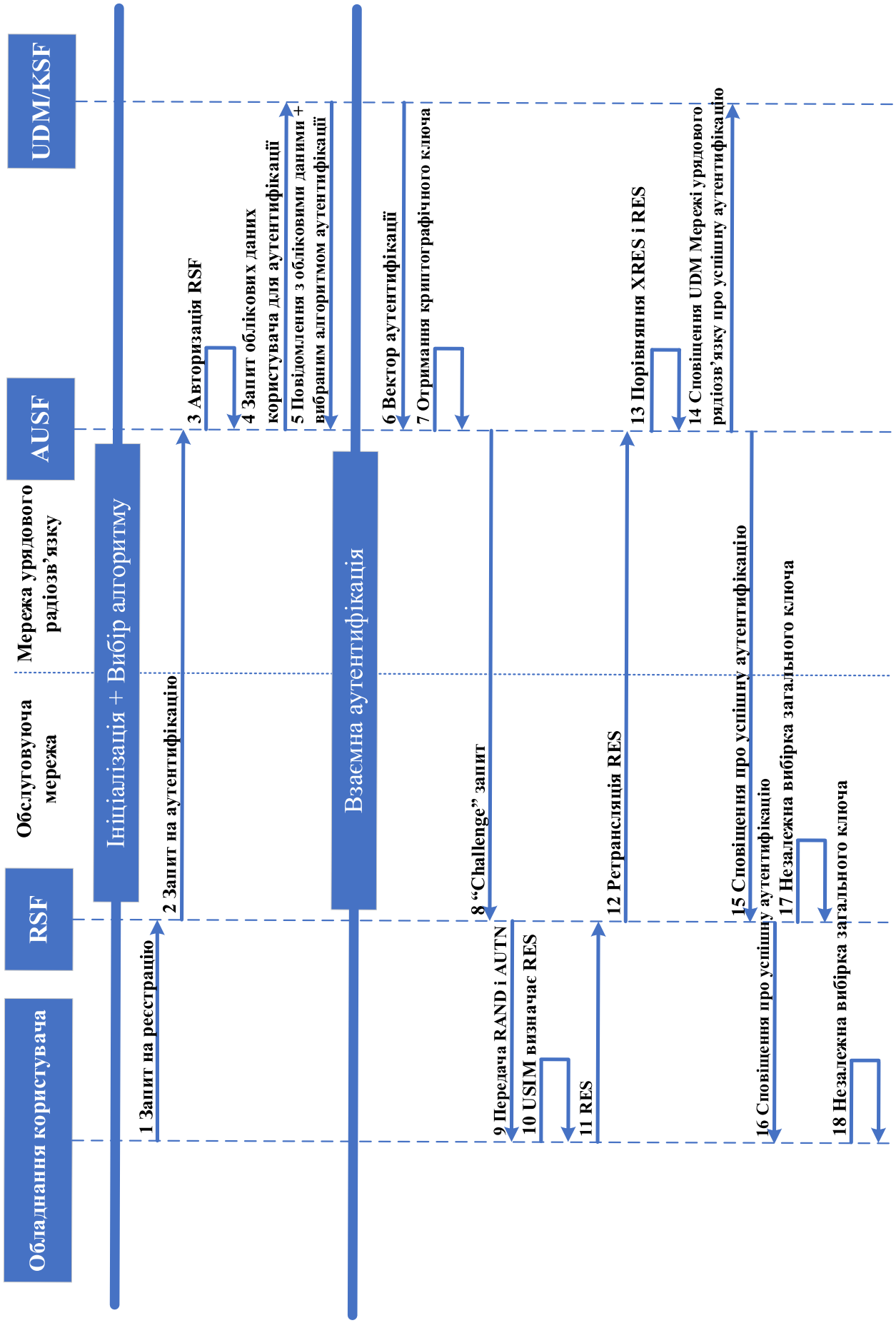

Рис. 5. Аутентифікація в мережі урядового радіозв'язку

У мережі урядового радіозв'язку процес аутентифікації відбуватиметься в дві фази: перша відповідає за ініціацію аутентифікації і вибору методу аутентифікації, друга – за взаємну аутентифікацію між користувачем і мережею.

Ініціація. Користувач відправляє запит на реєстрацію в RSF, яка містить прихований ідентифікатор підписки користувача SUCI.

RSF відправляє в AUSF повідомлення-запит на аутентифікацію (Nausf_UEAuthentication_ AuthenticateRequest), що містить SNN (від англ. Serving Network Name – ім'я обслуговуючої мережі) і SUPI або SUCI.

AUSF відправляє запит на перевірку, чи дозволено запитувачу аутентифікацію RSF та використовувати даний SNN. Якщо обслуговує мережа не авторизована використовувати даний SNN, то AUSF відповідає повідомленням про помилку авторизації «Serving Network Not Authorized» (Nausf_UEAuthentication_Authenticate Response).

Запит облікових даних для аутентифікації з боку AUSF в UDM здійснюється по SUPI або SUCI і SNN.

UDM/KSF вибирає метод аутентифікації базуючись на SUPI або SUCI та інформації про користувача, який буде використовуватися далі та видає облікові дані користувача.

Взаємна аутентифікація. При використанні будь-якого методу аутентифікації мережеві функції UDM/KSF повинні згенерувати вектор аутентифікації (англ. AV).

UDM/KSF генерує вектор аутентифікації, який відправляється в AUSF. Після цього AUSF виходить ключ KRSF з ключа KAUSF і відправляє в RSF запит «Challenge» в повідомленні «Nausf_UEAuthentication_Authenticate Response», що містить також RAND, AUTN і RES. Далі здійснюється передача RAND і AUTN на призначене для користувача устаткування за допомогою захищеного сигнального повідомлення NAS. USIM користувача вираховує RES з отриманих RAND і AUTN і відправляє його в RSF. RSF ретранслює це значення в AUSF для перевірки.

AUSF порівнює зберігається в ньому XRES і отриманий від користувача RES. У разі збігу, AUSF і UDM в домашній мережі оператора повідомляються про успішну аутентифікації, а користувач і RSF незалежно один від одного генерують ключ KAMF з KRSF і SUPI для подальшої комунікації.

Висновки

У даній статті було запропоновано тільки один із можливих випадків використання 5G в мережі урядового радіозв'язку, для якого можна використані запропоновані процедури аутентифікації та авторизації. Завдяки можливостям, які надає 5G, може відбуватися шифрування, контроль трафіку, що є найголовнішим для мереж урядового радіозв'язку. 5G дає можливість здійснити ізоляцію різних слоїв архітектури Network slicing і визначити для шару урядового радіозв'язку власні рівні безпеки. Для даної архітектури було розроблено процедуру встановлення сеансу захищеного урядового зв'язку.

За результатами дослідження отримані наступні результати:

– проаналізовано існуючу архітектуру ядра мережі 5G та основні принципи, яким вона має відповідати;

– розроблено удосконалену архітектуру мережі урядового радіозв'язку на основі технології 5G;

– розроблено процедури встановлення захищеного урядового радіозв'язку на основі технології 5G;

– завдяки можливостям, які надає 5G, буде здійснюватися шифрування, контроль сигнального і користувацького трафіку, що є найголовнішим для мереж урядового радіозв'язку;

– 5G дозволяє здійснити ізоляцію різних шарів архітектури Network slicing і визначити для шару урядового радіоз'язку власні рівні безпеки.

ЛІТЕРАТУРА

[1] 5GPPP White Paper, "Specialized Services, Network Management and 5G. URL: http://5GPPP.eu/wp-content/uploads/2015/06/Specialized-Services-NetworkManagement-and-5G.pdf

[2] Одарченко Р. С. Обгрунтування основних вимог до систем безпеки стільникових мереж 5-го покоління. Безпека інформації. 2015. № 3, т. 21. С. 102–106.

[3] Одарченко Р. С. Стратегії розвитку операторів стільникового зв'язку в Україні. Наукоємні технології. 2014. Вип. 2, т. 26. С. 141–148.

[4] Valery Tikhvinskiy, Grigory Bochechka, Alexander Minov, Andrey Gryazev. Innovation Radar as a Tool of 5G Development Analysis. Proceedings of the 16th International Conference, NEW2AN 2016, and 9th Conference, ruSMART 2016, Internet of Things, Smart Spaces, and Next Generation Networks and Systems, St. Petersburg, Russia, September 26–28, 2016, pp. 383–394.

[5] ITU towards "IMT for 2020 and beyond" – IMT-2020 standards for 5G; Minimum requirements related to technical performancefor IMT-2020 radiointerface(s) ITU (2017).

[6] Ahmad, Ijaz, et al. "5G security: Analysis of threats and solutions." 2017 IEEE Conference on Standar*ds for Communications and Networking (CSCN)*. IEEE, 2017.

[7] Sun, Yanbin, et al. "Automated attack and defense framework toward 5G security."IEEE Network 34.5 (2020): 247–253.

[8] Одарченко Р. С., Харлай Л. О., Абакумова А. О., Чмих П. А. Програмне забезпечення для оцінки ключових показників якості обслуговування зі сторони абонента стільникової мережі. Проблеми інформатизації та управління . 2017. № 3(59). С. 56–61.1.

[9] Одарченко Р. С., Скульська О. Ю., Гнатюк В. О. Метод оцінки ключових показників захищеності в сучасних стільникових мережах. Безпека інформації. 2017. № 1(23). С. 19–26.
[10] Foukas X., Patounas G., Elmokashfi A., Marina M. K. Network Slicing in 5G: Survey and Challenges. IEEE Communications Magazine. 2017. 55(5): 94–100.
[11] "ETSI – Standards for NFV – Network Functions Virtualisation | NFV Solutions"; "Network Functions Virtualisation (NFV); Use NFV is present and SDN is future.Cases"
[12] ETSI, 3GPP. ETSI TS 138 101-1 V15.9.0 (англ.). 2020.

Одарченко Р. С., Григоренко Д. К., Фесенко В. О., Дрофа Т. С.

УДОСКОНАЛЕННЯ ЯДРА МЕРЕЖІ 5G З МЕТОЮ ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ ЗВ'ЯЗКУ

Використання сучасних технологічних рішень для побудови радіо мереж різного призначення є безперечною вимогою сучасності. Але в цій ситуації питання безпеки мереж в цілому і безпеки мережі урядового радіозв'язку виходять на перший план. Крім того, наразі також дуже важливими є показники якості обслуговування абонентів мереж урядового зв'язку. Тому необхідно було провести змістовний аналіз можливостей використання сучасних стільникових мереж зв'язку для визначення можливостей побудови на їх базі мереж урядового радіозв'язку. В результаті виконання роботи було проведено аналіз основних вимог до мереж стільникового зв'язку 5G, зокрема, щодо їх надійності, швидкості передавання даних, затримки, підтримки мобільності та інших важливих для користувача характеристик, проведено дослідження основних вимог до сучасних мереж урядового радіозв'язку. Для цього було розширену класифікацію послуг, які планується надавати абонентам сучасних та перспективних мереж урядового радіозв'язку в Україні. Для цих нових послуг були сформовані нові вимоги, які включають в себе вимоги користувача, що стосуються якості обслуговування (користувацького досвіду) та функціональні вимоги. Було показано, що, завдяки використання принципів Network Slicing, фізична інфраструктура ділиться на віртуальні платформи, кожна з яких задіє ті ресурси і технології, які найкраще підходять для вирішення її завдань. Це надає можливість побудови більш захищених ізольованих між собою слоїв мережі 5G. Також було представлено удосконалену архітектуру мережі урядового радіозв'язку на основі технології 5G. Завдяки можливостям, які надає 5G, буде здійснюватися шифрування і контроль цілісності сигнального і користувацького трафіку, що є найголовнішим для мереж урядового радіозв'язку. Також 5G дозволяє здійснити ізоляцію різних слоїв архітектури Network slicing і визначити для шару урядового радіоз'язку власні рівні безпеки. Для даної архітектури було розроблено процедуру встановлення сеансу захищеного урядового зв'язку.

Ключові слова: 5G; стільникова мережа; урядовий радіозв'язок, архітектура мережі, процедури.

Odarchenko R., Hryhorenko D., Fesenko V, Drofa T.

IMPROVEMENT OF THE 5G NETWORK CORE WITH THE PURPOSE OF INCREASING THE LEVEL OF COMMUNICATION SECURITY

The use of modern technological solutions for the construction of radio networks for various purposes is an indisputable requirement of modernity. But in this situation, the issues of network security in general and the security of the government radio communication network come to the fore. In addition, indicators of the quality of service for subscribers of government communication networks are also very important at the moment. Therefore, it was necessary to conduct a meaningful analysis of the possibilities of using modern cellular communication networks to determine the possibilities of building government radio communication networks on their basis. As a result of the work, an analysis of the main requirements for 5G cellular communication networks was carried out, in particular, regarding their reliability, data transmission speed, delay, mobility support and other characteristics important for the user, and a study of the main requirements for modern government radio communication networks was carried out. For this purpose, the classification of services, which are planned to be provided to subscribers of modern and promising government radio communication networks in Ukraine, was expanded. New requirements were formed for these new services, which include user requirements related to quality of service (user experience) and functional requirements. It was shown that, thanks to the use of the principles of Network Slicing, the physical infrastructure is divided into virtual platforms, each of which uses the resources and technologies that are best suited for solving its tasks. This makes it possible to build more secure, isolated layers of the 5G network. An improved architecture of the government radio communication network based on 5G technology was also presented. Thanks to the capabilities provided by 5G, encryption and control of the integrity of signaling and user traffic will be carried out, which is the most important thing for government radio communication networks. Also, 5G makes it possible to isolate different layers of the Network slicing architecture and define its own security levels for the government radio communication layer. A secure government communication session establishment procedure was developed for this architecture.

Keywords: 5G; cellular network; government radio communications, network architecture, procedures.

Стаття надійшла до редакції 04.10.2022 р.
Прийнято до друку 13.04.2022 р.