© Odarchenko R. Substantiation of the basic requirements for 5th generation cellular networks security systems // Ukrainian Scientific Journal of Information Security, 2015, vol. 21, issue 3, p. 229-235.

ОБГРУНТУВАННЯ ОСНОВНИХ ВИМОГ ДО СИСТЕМ БЕЗПЕКИ СТІЛЬНИКОВИХ МЕРЕЖ 5-ГО ПОКОЛІННЯ

Роман Одарченко

Національний авіаційний університет, Україна

ОДАРЧЕНКО Роман Сергійович, к.т.н.

Рік та місце народження: 1988 рік, с. Култук Слюдянського р-ну Іркутської області, РФ.
Освіта: Національний авіаційний університет, 2010 рік.
Посада: доцент кафедри телекомунікаційних систем з 2012 року.
Наукові інтереси: стільникові мережі зв'язку нового покоління та їх системи безпеки.
Публікації: більше 90 наукових публікацій, серед яких наукові статті та патенти на винаходи.
E-mail: odarchenko.r.s@mail.ru

Анотація. *У даній статті проаналізовано хронологію розвитку стільникових мереж зв'язку в світі. Також були проаналізовані системи безпеки цих мереж, визначені їх проблемні місця. Зокрема, були розглянуті можливі атаки в мережах LTE, що можуть створити потенційні проблеми в майбутньому. Визначено, що на зміну мережам LTE до 2020 року прийдуть мережі 5G. В результаті проведених досліджень стало зрозумілим, що ці мережі відіграватимуть в майбутньому найбільш значущу роль в формуванні електронного суспільства, критичної інфраструктури тощо. Визначені основні рушійні сили розвитку 5G, згруповані в чотири основні характеристики (нові моделі довіри, нові моделі служби доставки, розширений перелік загроз, і збільшення рівня конфіденційності), що створюють визначальний вплив на підходи щодо формування вимог до систем безпеки та конфіденційності в мережах 5G. Були сформульовані ключові напрямки удосконалення систем безпеки стільникових мереж (управління ідентифікацією, безпека радіомережі, підвищення енергоефективності, гнучка і масштабована архітектура, безпека хмарних сервісів тощо), що дозволило обгрунтувати необхідність проведення подальших досліджень, пов'язаних із оптимізацією захисту мереж 5G. Це дозволить створити нову більш гнучку масштабовану архітектуру системи безпеки стільникових мереж, що буде в змозі забезпечити всі вимоги різноманітних різнорідних систем, що входять до сфери застосування стільникових мереж 5-го покоління.*

Ключові слова: *захист інформації, LTE, 5G, стільникові мережі, модель довіри, конфіденційність, загроза, управління ідентифікацією, радіомережа.*

Вступ

16 червня 1993 року офіційно вважається датою, коли в Україні було запроваджено стільниковий зв'язок [1]. З того часу за період майже в 23 роки інформаційно-комунікаційна інфраструктура в Україні кардинально трансформувалась, дійшовши до сучасного вигляду.

В цих умовах, що склались між операторами стільникового зв'язку, конкуренція призводить до того, що на ринку з'являються все нові більш вигідні пропозиції і акційні стартові пакети. Кожна із компаній починає анонсувати запуск мереж наступних поколінь. Проте до зовсім недавнього часу не відбувалося якісного переходу (стрибку) в стільникових мережах в Україні. Ця подія відбулася лише в лютому 2015 році – це запуск мереж 3G. Стратегія та перспективи подальшого розвитку стільникових мереж в Україні розглянуті в роботах [2-3]. Проте в більш розвинутих країнах, зокрема, в США, Європі та країнах Азії вже є доволі багато операторів, які надають послуги за допомогою мереж LTE [4], а вже до 2020 року планується запуск перших мереж 5G у комерційну експлуатацію [5-6].

При цьому кожен користувач будь-якої мережі прагне забезпечити конфіденційність передаваних даних та унеможливити спроби мережевих атак на мобільні пристрої. До того ж набирає популярності концепція Інтернету речей IoT [7], що висуває ще більші вимоги до захисту інформаційної інфраструктури.

Тому питання підвищення рівня безпеки в стільникових мережах виходить на ключові позиції.

Аналіз існуючих досліджень

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 [8-11]. Виокремити можна праці [12,13], 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 обгрунтовує 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 виявлення недоліків систем захисту мереж попередніх поколінь та формування вимог до безпеки майбутніх 5G мереж в цілому та їх окремих компонентів.

Основна частина дослідження

Близько 25 років тому, коли були розроблені системи GSM, були стандартизовані й деякі функції безпеки, які враховували недоліки, виявлені у попередніх аналогових систем, та були спрямовані на боротьбу з виникаючими загрозами.

Перш за все, було введено шифрування радіо інтерфейсу, адже виникла можливість прослуховувати переговори.

По-друге, виник ризик шахрайства, що вважався серйозною проблемою. Це призвело до введення додаткових заходів безпеки – SIM-карт, що дозволило додати більш сильний механізм аутентифікації.

При переході до мереж третього покоління, були зроблені подальші поліпшення систем безпеки. Приклади таких удосконалень включають в себе взаємну аутентифікацію для зменшення загроз, наприклад, підміни базових станцій, і переміщення шифрування вглиб мережі.

Коли було запущено мережі четвертого покоління LTE, одним з основних заходів безпеки стало повернення шифрування даних користувача до базової станції. Зокрема, також було введено більш складний ключ управління для захисту від потенційних фізичних зломів в базових станціях.

Архітектура системи безпеки в мережах LTE — це вже ціла підсистема стільникової мережі стандарту LTE, описана в технічних специфікаціях 3GPP TS 33.401 [14] і 3GPP TS 33.402 [15], яка включає набір методів, що дозволяють забезпечити безпечний зв'язок між вузлами мережі, конфіденційність і цілісність даних користувача. Дана архітектура запропонована консорціумом 3GPP в 2008 році [16]. Поточна версія – Realease 11 [17].

Коротко основні вимоги до механізмів безпеки технології LTE можна охарактеризувати наступним чином [18]:

- забезпечити як мінімум такий же рівень безпеки, як і в мережах типу 3G, не доставляючи незручності користувачам;
- забезпечити захист від Інтернет-атак;
- механізм безпеки для мереж LTE не повинен створювати перешкод для переходу зі стандарту 3G на стандарт LTE;
- забезпечити можливість подальшого використання програмно-апаратного модуля USIM (Universal Subscriber Identity Module, універсальна сім-карта).

У цілому, безпеки, пропоновані LTE дуже схожі на посилені заходи захисту 3G мереж, проте мають свої особливості.

Взагалі, розмірковуючи про обгрунтування необхідності забезпечення безпеки 2G-4G, можна сказати, що тут системи безпеки були введені в основному для захисту основних послуг (спочатку це передача голосу, а пізніше пакетних даних) для того, щоб заробити довіру користувачів, і для захисту екосистеми в умовах правильної взаємодії всіх учасників.

Слід визнати, що цей підхід дуже добре працював. Хоча деякі спроби нападу на системи безпеки мереж GSM стали можливими протягом останніх 10 років, це все одно було за межами економічного життя. Тому основні цілі, для яких розроблялися системи безпеки GSM, були виконані і перевиконані. Це ж саме стосується і нових більш прогресивних мереж третього та четвертого поколінь. Проте і більш сучасні мережі мають багато прогалин в системах безпеки. Розглянемо проблемні місця в мережах LTE [19, 20].

Перша очевидна загроза – атаки DoS (Denial of Service) на мережу. Ємність радіоканалу в LTE передбачається велика, але все ж вона має обмеження. Мережеві ресурси базової станції діляться між абонентами, і хоча є обмеження для монополізації смуги окремим користувачем, проте атака на відмову в обслуговуванні мережі цілком можлива. Зникнення RNC призвело до того, що доступ до ядра мережі LTE можливий безпосередньо з базової станції.

Інша загроза — вірусні атаки. Хоча таким атакам схильні пристрої, а не мережа, технологія LTE збільшує швидкість поширення шкідливих програм, оскільки сам цей стандарт є високошвидкісним. До того ж плата за користування послугами четвертого покоління навряд чи буде залежати від обсягу трафіку — тарифи будуть або безлімітними, або з обмеженням по смузі пропускання. Тому користувачі не зможуть швидко помітити трафік, породжуваний шкідливими програмами і вбудованими в них сканерами уразливостей. А значить, у розробників вірусів буде більше

можливостей для монетизації своїх мобільних розробок: від стеження за конкретною людиною до злодійства одноразових паролів в системах дистанційного банківського обслуговування.

Третя небезпека — атаки на додаткові сервіси. Власне, LTE розроблялося не тільки для забезпечення доступу до Інтернету мобільних користувачів, а скоріше як платформа для впровадження нових послуг: відео, ігрових та багатьох інших. Ці сервіси також можуть бути уразливі для найрізноманітніших атак — як з Інтернету, так і з мобільної мережі. Цілком можливо, що, атакувавши один із сервісів, зловмисники зможуть впровадити в клієнтські пристрої небезпечні програми.

Загроза користувачам LTE може виходити і від сервісів подвійного призначення. Мобільні оператори мають так багато цінної інформації про абонентів, що рано чи пізно захочуть її монетизувати. Типовим прикладом є LBS-сервіси. З одного боку, їх можна використовувати, наприклад, для контролю за переміщенням вантажів, для визначення місцезнаходження дітей і для оповіщення про надзвичайні ситуації, але з іншого — їх же можна використовувати для незаконного стеження. З поширенням інтелектуальних пристроїв число потенційно небезпечних сервісів буде тільки зростати. Злом такого сервісу дозволить зловмисникам отримати доступ до цінної інформації провайдера і побудувати нові схеми злочинів і незаконного отримання грошей.

Ми привели далеко не повний список нових загроз, пов'язаних з появою LTE. Є також проблеми і з самим стандартом. Дуже гостро стоїть завдання взаємодії з недовірених (Не LTE) мережами. Якщо трафік між користувацьким устаткуванням і eNB шифрується (ця вимога стандарту) і загроза порушення конфіденційності стає неактуальною, то, наприклад, взаємодія eNB з радіоконтроллер мережі 3G за замовчуванням ніяк не захищене, а отже, це пролом для можливих атак з боку зловмисників. Як і відсутність обов'язкової аутентифікації між ядром мережі і eNB, цю опцію оператор зв'язку може як використовувати, так і не задіяти в принципі, щоб знизити свої витрати з розгортання мережі LTE.

Але, не дивлячись на всі переваги і на деякі недоліки в системах безпеки, аналітики в усьому світі розуміють, що на зміну LTE за оцінками експертів після 2020 року мають прийти мережі 5-го покоління – 5G. Вони повинні будуть враховувати всі недоліки мереж попередніх поколінь. На рисунку 1 представлені основні напрямки розвитку безпроводових мереж, які відображають як побажання користувачів, так і операторів стільникового зв’язку.

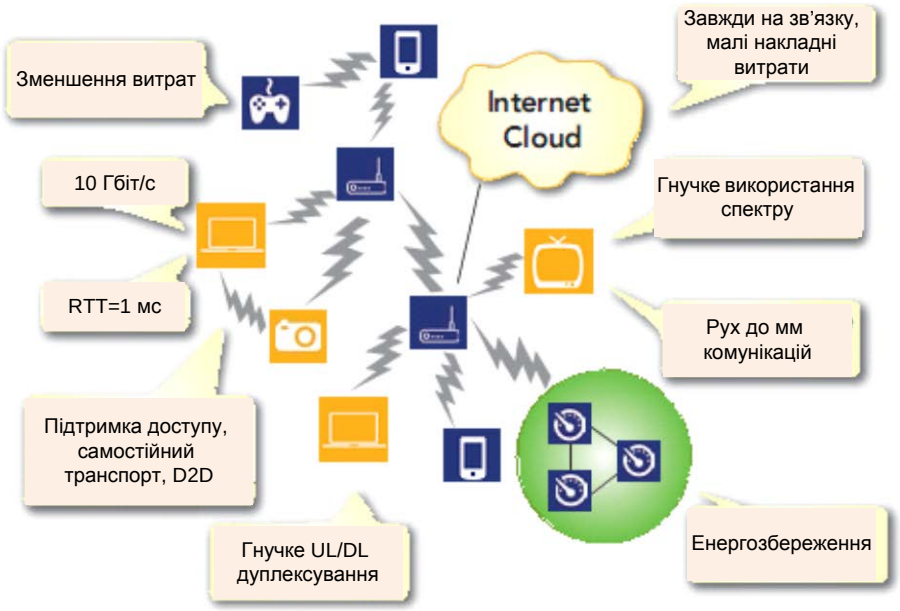

Рис. 1 Шляхи розвитку стільникових мереж зв’язку

На рис. 1 не відображений ще один дуже важливий напрям розвитку мереж стільникового зв’язку – удосконалення систем безпеки. Саме цьому питанню буде присвячене дане наукове дослідження.

До останнього часу основною рушійною силою для еволюції мобільної мережі в основному було підвищення пропускної здатності і зменшення затримки для забезпечення оптимального доступу до мережі Інтернет. Але мережі п’ятого покоління вже потребують принципово нову модель забезпечення інформаційної безпеки, адже вони матимуть вже значно розширений функціонал. По-перше, вони будуть сконструйовані не лише для забезпечення потреб окремих людей та суспільства в цілому, а й для цілей об’єднання цілих індустрій (таких як фабрики, заводи, інтелектуальні системи, системи e-health тощо).

Що характеризує стільникові мережі 5G, так це те, що вони набагато більше, ніж 4G,

відіграватимуть роль в створенні принципово нового «електронного» суспільства. При цьому повний спектр систем безпеки, недоторканності приватного життя і стійкості буде проблемою, яка охоплює далеко не виключно технології 5G, а й все майбутнє «електронне» суспільство.

Основні рушійні сили розвитку 5G можуть бути згруповані в чотири характеристики, кожна з яких має вплив на формування вимог для забезпечення безпеки і недоторканності приватного життя. Ці характеристики наступні: нові моделі довіри, нові моделі служби доставки, розширений перелік загроз, і збільшення рівня конфіденційності.

Отже, ці характеристики впливають на те, як ми повинні підходити до формування вимог до систем безпеки та конфіденційності в мережах 5G.

Нові моделі довіри. Цільові моделі постійно змінюються із плином часу. Як простий приклад, можна навести використання концепції BYOD (Bring Your Own Device) [21]. Раніше всі користувацькі пристрої можна було вважати такими, які заслуговували безперечної довіри, але всі вони були одного типу, видані і керувалися IT-відділом підприємства. Сьогодні користувачі хочуть використовувати свої пристрої, а, створюючі загрози пристрої залишити за межами корпоративних брандмауерів.

Для сучасних мобільних систем, модель довіри досить проста, і вона включає абонента (і його термінал) і два оператора (домашню і гостьову мережі). Натомість мережі 5G спрямовані на підтримку нових бізнес-моделей і включають в себе нові ролі, а тому моделі довіри мають змінитися, породжуючи розширення вимог у таких областях, як аутентифікація між різними суб'єктами, підзвітність і безвідмовність.

Безпека для нових моделей надання послуг. Використання хмарних сервісів і віртуалізації підкреслює залежність від використання безпечного програмного забезпечення, і призводить до появи нового впливу на вимоги до систем безпеки. Сучасні системи, визначені в документації 3GPP, базуються на основі стандартних функціональних вузлів та абстрактних інтерфейсах для забезпечення взаємодії між ними, і, таким чином можуть забезпечити хорошу відправну точка для віртуалізації. Однак, дотепер пропрієтарне апаратне забезпечення досі часто використовується для цих вузлів і інтерфейсів. Така розв'язка апаратного та програмного забезпечення означає, що безпека телекомунікаційної мережі більше не може покладатися на конкретні атрибути безпеки виділеної телекомунікаційної апаратної платформа. З тієї ж причини, стандартні інтерфейси до обчислювальних / мережевих платформ, такі, як ті, що визначені ETSI (Європейським інститутом телекомунікаційних стандартів) в роботі їх мережевих функцій віртуалізації — необхідні для забезпечення керованого підходу до безпеки.

Розширений перелік загроз. Мережі 5G відіграватимуть ще більш центральну роль в якості критичної інфраструктури. Багато людей вже випробували випадки, коли всі види зв’язку переставали надаватися одночасно, наприклад, внаслідок дії природних катаклізмів. І суспільство точно не хоче втрачати подачу електроенергії, мобільну телефонію тощо в в один і той самий час. Крім того, великі проблеми, такі як збільшення загроз кібертероризму, тіньової економіки, електронного шахрайства, також створюються за рахунок нових можливостей мереж 5G.

Збільшення недоторканності приватного життя.

Захист персональних даних було обговорено в рамках програм ЄС. В даний час ця проблема розглядається в органах стандартизації, таких як 3GPP і IETF (Internet Engineering Task Force), обговорюються на багатьох інших форумах.

Таким чином, можемо бачити, що мережі 5G через свою майбутню роль мають стати дійсно одними із найзахищеніших. Отже, розглянемо ключові напрямки удосконалення систем безпеки стільникових мереж 5G.

Забезпечення безпеки. Як вже було відзначено, цілком імовірно, що мережі 5G відіграватимуть найбільш центральну роль в якості критичної інфраструктури в порівнянні з попередніми поколіннями, і тому забезпечення безпеки буде дуже критичним. У проекті 3GPP вже спостерігається необхідність розширення характеристики безпеки від функціональних одиниць для інтерфейсів до специфікацій забезпечених на реалізованих вузлах / інтерфейсах, і тому 3GPP приступило до роботи над розробкою методології забезпечення безпеки SECAM [22]. Тим не менш, у поєднанні з реалізацією на основі хмари є необхідність, швидше за все відокремити гарантування безпеки програмних додатків, більш конкретно від гарантування безпеки самої платформи, і дозволити проведення на вимогу визначення забезпечення рівня безпеки в рамках укладених угод про рівень обслуговування (SLA).

Що стосується ролі 5G мереж як критичної інфраструктури, рішення має бути прийнято, на скільки важливо це і повинно бути. Стандартна гарантія для IT-продуктів заключна в Загальних Критеріях (ISO 15408) [23]. Якщо 5G мають стати спільною платформою для створення суцільного Мережевого суспільства [24, 25], здається, ясно, що Загальні Критерії можуть бути введені в якості додаткових вимог до забезпечення безпеки у верхній частині SECAM.

Припустимо, що в деяких випадках застосування, транспортних засобів / безпеки дорожнього руху буде залежати від мережі 5G безпеку. Сьогодні, автомобільні системи, пов'язані з безпекою повинні відповідати ряду стандартів, наприклад, ISO 26262 [26]. Так само, сектор охорони здоров'я, в тому числі e-health [27] регулюється стандартами, такими як ISO 27799 [28], а в США, наприклад, HIPAA [29]. Для розумних ліній електропередач, безпека забезпечується у відповідності зі стандартами від IEEE, IEC (Міжнародна електротехнічна комісія) і NIST (Національний інститут стандартів і технології). Тому виникає логічне запитання, чи мають 5G

мережі бути частинами вищезазначених та багатьох інших стандартів, якщо будуть задіяні в контурі управління даними критичними інфраструктурами. Відзначають, принаймні, два способи розв'язку цього запитання.

По-перше, розшарування мережі може стати важливим інструментом для обробки дуже різноманітних вимог різних додатків і користувацьких груп. Розшарування часто розглядається як спосіб забезпечення ізольованості підмереж, кожна з яких оптимізована для конкретних типів характеристик трафіку. Однією із таких може бути характеристика пов'язано з вимогами безпеки. При наявності правильно реалізованих, із високим ступенем надійності механізм ізоляції, можна буде обмежити вплив вимог до систем безпеки кожного рівня (шару), а не всієї мережі.

По-друге, у нас є вибір, щоб «винести» вимоги безпеки із мережевих рівнів 5G і просто покласти відповідальність на кінцеві вузли; іншими словами, на підключені пристрої або центри обробки даних. Забезпечення безпеки даних є прикладом служби, які можуть надаватися таким способом.

Таким чином, той факт, що 5G призначені для платформи широкого кола користувачів і додатків не означає, що треба (або навіть бажано) для 5G нести всю відповідальність безпеки і пов'язані з цими витрати. З іншого боку, 5G мережі можуть забезпечувати деякі додаткові послуги безпеки.

Управління ідентифікацією. Стандарт 4G LTE вимагає наявність USIM (Універсальний модуль ідентифікації абонента), щоб отримати доступ до мережі. Цей спосіб доступу, принаймні на початку, буде невід'ємною частиною 5G з таких причин, як високий рівень безпеки і зручність. Вбудовані SIM також значно знижують складність розгортання мереж, пов'язаних із зв'язком машина-машина. Тим не менш, існує загальна тенденція приносити власний спосіб ідентифікації (наприклад, із концепції BYOD), що для 5G надасть переваги від більш відкритої архітектури управління ідентифікацією, яка надасть багато різних альтернатив. Одним із прикладів може бути підприємство з існуючими власними рішеннями для управління безпечними ідентифікаторами (ID), що можуть бути повторно використані для доступу до мереж 5G. Розглядаючи нові шляхи для встановлення ідентичності пристроїв / абонентів, можна стверджувати, що вони є ключовим фактором який безперечно має увійти до нових моделей довіри для 5G.

Загроза перехоплення IMSI залишається достатньо високою, тому робота в даному напряму для посилення захисту IMSI заслуговує уваги для 5G в майбутньому.

Безпека радіомережі 5G. У зв'язку із розширеною кількістю загроз і нових технологій, що забезпечує користувачам альтернативне програмувати своїх власних пристроїв (навіть на рівні радіодоступу), захист від атак на радіо мережі повинен бути більш чітко вираженим в новій архітектурі мереж 5G, що має враховувати захист від загроз таких як DoS (відмова в обслуговуванні) через потенційно некоректно працюючі пристрої і додаючи заходів з пом'якшення наслідків нового дизайну радіопротокола.

Хоча радіомережі LTE мають відмінний захист від криптографічного підслуховування, немає ніякого захисту проти зміни або ін'єкцій трафіку в площині абонента. Тому в 5G цей напрям досліджень також заслуговує значної уваги, особливо зважаючи на важливі можливі застосування 5G.

Гнучка і масштабована архітектура безпеки. У зв'язку із можливістю віртуалізації і більш динамічної конфігурацій, що входять до бачення 5G, здається логічним, розглянути більш динамічну і гнучку архітектуру безпеки для неї. Безпека для синхронних аспектів, таких, як сигналізація RAN, може бути розташована поряд з доступом з високим ступенем незалежності від асинхронних аспектів безпеки, таких як ті, що пов'язані з користувацькою площиною. Це дозволить більш ефективне забезпечення безпеки, а також обмежить загрози для чутливої користувацької інформації в той же час. Нові проекти безпеки з високим рівнем гнучкості можуть також краще слугувати для вирішення непотрібних конфліктів між зручністю і безпекою.

Енергоефективна безпека. У той час, як сервіси забезпечення безпеки пов'язані із витратами, це не являється більше проблемою для мобільних телефонів і аналогічних пристроїв. Витрати енергії на шифрування одного біту в один або два рази менше величини витрат на передачу одного біта [30]. Тим не менш, для найбільш енергонезалежних пристроїв з необхідним тривалим часом роботи, може виникнути необхідність розглянути ще більш легші рішення.

Хмарна безпека. Забезпечення хмарної безпеки вже надзвичайно гаряча тема, і вона безперечно буде додана до списку проблем 5G. Наведемо тільки короткий перелік пріоритетів для забезпечення хмарної безпеки в контексті 5G, керуючись вище викладеним матеріалом:

- Розробка гіпервізорів і віртуалізації мережі з високим рівнем гарантії ізоляції. Як уже згадувалося, інвестиції в цій області може окупитися, так як це значно спростить обробку різноманітних вимоги до систем безпеки в тій же інфраструктурі.

- Забезпечити більш ефективні рішення для шифрування даних, дружніх для хмар (гомоморфне шифрування, що дозволяє виконувати операції по шифрованих даних).

- Розробка простих у використанні, надійних в управлінні хмарних систем і додатків, які працюють на них.

Висновки

Розглянутий розвиток стільникових мереж зв'язку як в Україні, так і в світі надав змогу обґрунтувати необхідність дослідження стільникових мереж п'ятого покоління, окреслити їх основні переваги. Також були проаналізовані системи безпеки стільникових мереж. Проте, не зважаючи на всі переваги систем безпеки вже

існуючих мереж 2-4 поколінь, залишається дуже багато проблемних місць, які необхідно вирішувати.

В результаті проведених досліджень стало зрозумілим, що мережі 5G відіграватимуть в майбутньому поки що найбільш значущу роль в формуванні електронного суспільства, критичної інфраструктури тощо. Тому дуже актуальними і важливими є питання, пов'язані із забезпеченням інформаційної безпеки в майбутніх мережах 5G. Основні рушійні сили розвитку 5G, згруповані в чотири основні характеристики (нові моделі довіри, нові моделі служби доставки, розширений перелік загроз, і збільшення рівня конфіденційності) створюють визначальний вплив на підходи щодо формування вимог до систем безпеки та конфіденційності в мережах 5G. Тому були сформульовані ключові напрямки удосконалення систем безпеки стільникових мереж (управління ідентифікацією, безпека радіомережі, підвищення енергоефективності, гнучка і масштабована архітектура, безпека хмарних сервісів тощо), що дозволило обгрунтувати необхідність проведення подальших досліджень, пов'язаних із оптимізацією захисту мереж 5G.

Література

[1] Мобільний зв'язок в Україні [Електронний ресурс]– Електронні текстові дані – Режим доступу: http://uateka.com/uk/article/society/1227/.

[2] Перспективи та рекомендації по впровадженню стільникового зв'язку 4-го покоління / В. В. Ткаченко, Р. С. Одарченко, В. С. Повхліб, Т. Р. Андрійченко // Проблеми навігації та управління рухом : Всеукр. наук.-практ. конф. молодих учених і студентів; м. Київ, 21–22 листопада 2011 р. : тези доповідей / редкол. : М. С. Кулик та ін. – К. : НАУ, 2011. – С. 122.

[3] Одарченко Р.С. Стратегії розвитку операторів стільникового зв'язку в Україні // Наукоємні технології. — Том 26, № 2 (2015). — С. 141-148.

[4] [Електронний ресурс]– електронні текстові дані – Режим доступу: http://www.gsacom.com/downloads/pdf/GSA_Evolution_to_LTE_report_060514.php4.

[5] 4G America's recommendation on 5G Requirements and Solutions, October 2014, p. 40.

[6] Understanding 5G [Електронний ресурс]– Електронні текстові дані. – Режим доступу: http://www.arnitsu.com.

[7] Белоцерковский А.Е. Интернет вещей – это будущее, которое уже наступило [Електронний ресурс]– електронні текстові дані – Режим доступу: http://www.therunet.com/interviews/5015-internet-veschey-eto-buduschee-kotoroe-uzhe-nastupilo.

[8] Киселев В.Д., Есиков О.В., Кислицын А.С. Современные проблемы защиты в системах ее передачи и обработки / Под ред. проф. Е.М. Сухарева. – М.:«Солид», 2000. – 200 с.

[9] Шаньгин В.Ф., Соколов А.В. Защита информации в распределенных корпоративных сетях и системах. – Изд-во: ДМК, 2002. – 134 с.

[10] Гарбарчук В., Зинович З., Свиц А. Кибернетический подход к проектированию систем защиты информации / Украинская академия информатики; Волынский гос. ун-т им. Леси Украинки; Люблинский политехнический ун-т. – К.; Луцк; Люблин, 2003. – 658 с.

[11] Задірака В.К., Бабич М.Д., Березовський А.І. та ін. Т-ефективні алгоритми наближеного розв'язування задач обчислювальної математики. – К., 2003. – 216 с.

[12] Одарченко Р.С., Беженар Ю.В., Ксендзенко А.О. Аналіз вразливостей систем захисту інформації в мережах Wi-Max та методів їх усунення // Защита информации. Сб. научных трудов.- К.: НАУ, 2011. – Вып. 18. – С. 39-44.

[13] Одарченко Р.С., Лукін С.Ю. Економічна ефективність впровадження систем захисту стільникових мереж 4G // Системи обробки інформації. Збірник наук. праць Інформаційна та економічна безпека. – Х.: Вид-во Харківського університету Повітряних Сил ім. Івана Кожедуба. – 2012. – Вип. №4 (102) Том 2 - С. 51-56.

[14] The mobile broadband standard - 3GPP TS 33.401 [електронний ресурс]– Електронні текстові дані – режим доступу: http://www.3gpp.org/DynaReport/33401.htm.

[15] The mobile broadband standard - 3GPP TS 33.402 [Електронний ресурс]– Електронні текстові дані – Режим доступу: http://www.3gpp.org/DynaReport/33402.htm.

[16] SP-39 1.0.0 2008-03-20 [Електронний ресурс]– Електронні текстові дані – Режим доступу: http://www.3gpp.org/ftp/Specs/html-info/33401.htm.

[17] Rel-11 SP-57 2012-09-12 [Електронний ресурс]– Електронні текстові дані – Режим доступу: http://www.3gpp.org/ftp/Specs/html-info/33401.htm.

[18] 3G security; Network Domain Security (NDS); IP network layer security [Електронний ресурс]– Електронні текстові дані – Режим доступу: http://www.3gpp.org/ftp/Specs/html-info/33210.htm.

[19] Скорость и безопасность в LTE [електронний ресурс] – Електронні текстові дані – режим доступу: http://www.osp.ru/nets/2012/06/13032673/.

[20] Угрозы безопасности в сетях LTE: устройства, основные элементы сети и сервисы [Електронний ресурс]– Електронні текстові дані – Режим доступу: http://telekomza.ru/2015/01/26/ugrozy-bezopasnosti-v-lte-ustrojstva-osnovnye-elementy-seti-i-servisy/.

[21] Ткаліч О.П., Одарченко Р.С., Рибальченко Є.В., Марченко О.В., Шеремет Є.Ю., Лагодний О.В. Підвищення ефективності використання корпоративної мережі за концепцією BYOD // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем. №7 – Житомир: ЖВІ НАУ, 2013. – С. 77-87.

[22] Security Assurance Methodology (SECAM) for 3GPP Nodes [Електронний ресурс] – Електронні текстові дані. – Режим доступу: http://www.3gpp.org/news-events/3gpp-news/1569-secam_for_3gpp_nodes.

[23] Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model [Електронний ресурс]– Електронні текстові дані – Режим доступу: http://www.iso.org/iso/catalogue_detail.htm?csnumber=50341.

[24] Castells, Manuel and Cardoso, Gustavo, eds., The Network Society: From Knowledge to Policy. . Washington, DC: Johns Hopkins Center for Transatlantic Relations, 2005, pp. 12-16,

[25] Network society [Електронний ресурс]– Електронні текстові дані – Режим доступу: https://en.wikipedia.org/wiki/Network_society.

[26] Road vehicles — Functional safety — Part 1: Vocabulary [Електронний ресурс]– Електронні текстові дані – Режим доступу: http://www.iso.org/iso/catalogue_detail?csnumber=43464.

[27] eHealth [електронний ресурс]– Електронні текстові дані – Режим доступу: https://en.wikipedia.org/wiki/EHealth.

[28] Health informatics — Information security management in health using ISO/IEC 27002 [Електронний ресурс]– Електронні текстові дані – Режим доступу: https://www.iso.org/obp/ui/#iso:std:iso:27799:ed-1:v1:en.

[29] FHealth Insurance Portability and Accounting Act [Електронний ресурс] – Електронні текстові дані – Режим доступу: https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act.

[30] C. Margi, B. Trevizan, G. de Sousa, M. Simplicio, P. Barreto, T. Carvalho, M. Nдslund, R. Gold, «Impact of Operating Systems on Wireless Sensor Networks (Security) Applications and Testbeds», Proceedings of ICCCN 2010, pp. 1-6, 2010.

УДК 621.396:621.395:007.681 (045)

Одарченко Р.С. Обоснование основных требований к системам безопасности сотовых сетей 5-го поколения

Аннотация. *В данной статье проанализировано хронологию развития сотовых сетей связи в мире Также были проанализированы системы безопасности этих сетей, определены их проблемные места. В частности, были рассмотрены возможные атаки в сетях LTE, которые могут создать потенциальные проблемы в будущем. Определено, что на смену сетям LTE к 2020 году придут сети 5G. В результате проведенных исследований стало ясно, что эти сети будут играть в будущем наиболее значимую роль в формировании электронного общества, критической инфраструктуры и тому подобное. Определены основные движущие силы развития 5G, сгруппированные в четыре основные характеристики (новые модели доверия, новые модели службы доставки расширенный перечень угроз, и увеличение уровня конфиденциальности), создающие определяющее влияние на подходы к формированию требований к системам безопасности и конфиденциальности в сетях 5G. Были сформулированы ключевые направления совершенствования систем безопасности сотовых сетей (управление идентификацией, безопасность радиосети, повышение энергоэффективности, гибкая и масштабируемая архитектура, безопасность облачных сервисов и т.д.), что позволило обосновать необходимость проведения дальнейших исследований, связанных с оптимизацией защиты сетей 5G. Это позволит создать новую более гибкую масштабируемую архитектуру системы безопасности сотовых сетей, которая будет в состоянии обеспечить все требования различных разнородных систем, входящих в сферу применения сотовых сетей 5-го поколения.*

Ключевые слова: *защита информации, LTE, 5G, сотовые сети, модель доверия, конфиденциальность, угроза, управление идентификацией, радиосеть.*

Odarchenko R. Substantiation of the basic requirements for 5th generation cellular networks security systems

Abstract. *This paper analyzes the history of cellular networks in the world were also analyzed the security of the network, identified by their weak points. In particular, they discussed possible attacks in networks of LTE, which can create potential problems in the future. It was determined that replacing LTE networks by 2020 will come online 5G. As a result of the research it became clear that these networks will play in the future, the most significant role in the formation of e-society, critical infrastructure and the like. The main driving forces of 5G, grouped into four main characteristics (new trust models, new models of service delivery of an expanded list of threats, and increase the level of confidentiality), creating a decisive influence on the approaches to the development of requirements for systems of security and privacy in 5G networks. We formulated the key directions of improvement of safety systems for cellular networks (identity management, safety radio network, energy efficiency, flexible and scalable architecture, security and cloud services, etc.), which allowed to justify the need for further studies related to the optimization of network security 5G. This will create a new, more flexible, scalable security architecture of cellular networks, which will be able to provide all the requirements of a variety of disparate systems within the scope of the 5th generation cellular networks.*

Key words: *information security, LTE, 5G, cellular networks, trust model, privacy threats, identity management, radio network.*

Отримано *26 жовтня 2015 року*, затверджено редколегією *17 листопада 2015 року*