© Odarchenko R., Gnatyuk V. Conceptual framework of modern cellular network cybersecurity rising // Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 2, p. 143-149.

КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ / CYBERSECURITY & CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

КОНЦЕПТУАЛЬНІ ЗАСАДИ ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ СУЧАСНИХ СТІЛЬНИКОВИХ МЕРЕЖ

Роман Одарченко, Віктор Гнатюк

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 95 наукових публікацій, серед яких наукові статті та патенти на винаходи.
E-mail: odarchenko.r.s@mail.ru

ГНАТЮК Віктор Олександрович

Рік та місце народження: 1990 рік, м. Нетішин, Хмельницька область, Україна.
Освіта: Хмельницький національний університет, 2012 рік.
Посада: асистент кафедри телекомунікаційних систем з 2015 року.
Наукові інтереси: інформаційна безпека, управління інцидентами інформаційної безпеки.
Публікації: більше 20 наукових публікацій, серед яких наукові статті, тези та матеріали доповідей на конференціях, авторські свідоцтва.
E-mail: viktorgnatyuk@meta.ua

Анотація. *У даній роботі проаналізовано еволюцію стільникових мереж зв'язку від 1-го до 5-го поколінь. Крім того, були проаналізовані системи безпеки цих мереж і також була показана їх еволюція. Більш детально були розглянуті можливі технічні рішення для систем безпеки найсучасніших на даний час мереж LTE. В результаті проведених досліджень стало зрозумілим, що ці мережі та мережі 5G відіграватимуть в майбутньому найбільш значущу роль в формуванні електронного суспільства, будуть використані для забезпечення потреб та вимог критичної інфраструктури тощо. На основі проведених досліджень було запропоновано концепцію побудови системи кібербезпеки стільникових мереж, при цьому окреслені ключові напрямки удосконалення сучасних систем безпеки: управління ідентифікацією, безпека радіомережі, підвищення енергоефективності, гнучка і масштабована архітектура, безпека хмарних сервісів тощо. 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 даного типу мереж, в тому числі і 5-го покоління. Також були запропоновані технічні удосконалення архітектури та технологій стільникових мереж LTE з огляду на новітні розробки в цій області.*

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

Вступ

Побудова інформаційного суспільства в Україні є одним з найактуальніших завдань сьогодення. Велике значення при цьому відіграє впровадження перспективних інформаційних технологій та методів автоматизації. Питання використання глобальної інформаційної мережі Інтернет є одним з пріоритетних напрямів державної політики у сфері інформатизації. В Стратегії розвитку інформаційного суспільства в Україні до пріоритетів формування сучасної

інформаційної інфраструктури країни віднесено створення високошвидкісних мереж широкосмугового мобільного доступу до Інтернет на всій території України [1, 2]. Йдеться про широкосмуговий доступ на базі використання технологій мобільного зв'язку третього і четвертого поколінь 3G і 4G (від англ. Generation – покоління). На вирішення питань щодо впровадження 4G технологій на території України спрямовано реалізацію національного проекту «Відкритий світ» [3], яким передбачається створення інформаційно-комунікаційної освітньої мережі національного рівня на базі технологій радіозв'язку четвертого покоління.

Стандарт 4G обіцяє набагато більші швидкості передачі даних: понад 100 Мбіт/с швидкорухомим абонентам (наприклад, потягам і автомобілям) та 1 Гбіт/с абонентам з невеликою рухливістю (наприклад, пішоходам і фіксованим абонентам) згідно з міжнародною специфікацією International Mobile Telecommunications Advanced (IMT-Advanced) від 2008 року [4].

Особливістю розвитку LTE-мереж є можливість їх побудови на вже розвинених мережах, як операторів GSM, так і операторів CDMA, що помітно знижує вартість розгортання мереж. Складність переходу до LTE-мереж в Україні зумовлена проблемами отримання ліцензій для нового спектру частот і необхідністю спеціальних абонентських пристроїв, здатних одночасно працювати в мережах LTE і 3G [2].

Виходячи з вищесказаного, можна сказати, що розвиток інфраструктури широкосмугового доступу до Інтернет на всій території України на базі створення високошвидкісних мереж четвертого покоління є задачею актуальною та перспективною. Для рядового користувача 4G основні переваги цілком очевидні: по-перше, висока швидкість передачі даних, по-друге, малий час відклику, а по-третє, абонентський пристрій буде працювати навіть в зоні дії подавлювача стільникових телефонів.

Проте в цих умовах для користувачів важливо не тільки завжди отримувати високошвидкісний та якісний доступ до мережевих ресурсів незалежно від місця знаходження, але і з забезпеченням необхідного рівня безпеки даних, що передаються.

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 Г.Ф. Конахович, О.Г. Корченко, О.К. Юдін, С.О. Гнатюк, 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. Пескозуб, А.П.Пятібратова, В.К. Размахнін, С.П. Расторгуєва, Ю.А. Самохіна і багато інших [5-8]. Виокремити можна праці [9, 10], 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 із найпроблемніших місць будь-якої стільникової 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 розробка концепції підвищення рівня кібербезпеки в сучасних стільникових мережах.

Основна частина дослідження

Нові покоління мобільного зв'язку починали розроблятися практично через кожні десять років з моменту переходу від розробок першого покоління аналогових стільникових мереж в 1970-х роках (1G) до мереж з цифровою передачею (2G) в 1980-х роках. Від початку розробок до реального впровадження проходила достатня кількість часу (наприклад, мережі 1G були впроваджені в 1984 році, мережі 2G - в 1991 році). У 1990-х роках почав розроблятися стандарт 3G, заснований на методі множинного доступу з кодовим поділом каналів (CDMA); він був впроваджений тільки в 2000-х роках. Мережі покоління 4G, засновані на IP-протоколі, стали розроблятися в 2000 році і почали впроваджуватися в багатьох країнах з 2010 року. Процес еволюції стільникових мереж зведений до табл. 1.

Технології продовжать свій розвиток в напрямку до більш високої продуктивності і все більшого числу можливостей. На додаток до існуючих технологій радіодоступу, з'являться також нові технології, які дозволять вирішувати ті завдання, які неможливо вирішити за допомогою 3G/4G. Прозора інтеграція існуючих і нових технологій сприятиме підвищенню якості користувацького досвіду і появи цілого ряду нових послуг.

Разом із еволюцією технологій, що використовуються в стільникових мережах, паралельно еволюціонували і їх системи безпеки (рис. 1). 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 радіоінтерфейсу. 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, наприклад, введення аутентифікації для зменшення різних типів загроз (наприклад, підміни базових станцій) і переміщення шифрування вглиб мережі.

Еволюція стільникових мереж Таблиця 1

Покоління	Ключові характеристики	Основні стандарти
1G	Аналогові стандарти з частотною модуляцією в тракті передачі розмовного сигналу. Багатостанційний доступ з частотним поділом каналів (FDMA).	NMT -450, NMT -900, AMPS та ін.
2G	Цифрове кодування та передавання мови і коротких текстових повідомлень. Часове і кодове розділення каналів (TDMA і CDMA).	GSM, ADC (D - AMPS), JDC, CDMA - IS -95, DCS-1800, PCS - 1900 та ін.
2,5G	Цифрові мережі з передаванням мови, тексту, підключенням до Internet.	GPRS
2,75G	Цифрові мережі з передаванням мови, тексту, підключенням до Internet, збільшена швидкість передавання даних.	EDGE
3G	Набір послуг, який включає до себе як високошвидкісний мобільний доступ до послуг мережі Інтернет, так і технологію радіозв'язку, підтримку мультимедіа, передачу з розширеним спектром.	CDMA 2000, WiMAX (IEEE 802.16), DECT, UMTS
3,5G	Доступ високошвидкісного приймання пакетних даних стандарту мобільного зв'язку 3-го покоління.	HSDPA, HSUPA та ін.
4G	Архітектура All-over-IP. Глобальний роумінг. Пікові швидкості приблизно в 100 Мбіт/с на пристроях високої мобільності (зразок стільникових телефонів) і приблизно 1 Гбіт/с на стаціонарних пристроях (зразок домашнього модему 4G).	LTE-Advanced, WirelessMAN-Advanced
5G	Новий стандарт – реліз наступний після 4G у розробці.	Поки відсутні

При переході до мереж третього покоління, були зроблені подальші поліпшення систем безпеки, наприклад, введення аутентифікації для зменшення різних типів 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. Також було введено більш складний ключ управління для захисту від потенційних фізичних зломів в базових станціях.

Коротко основні вимоги до механізмів безпеки технології LTE можна охарактеризувати наступним чином [11]:

– 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.

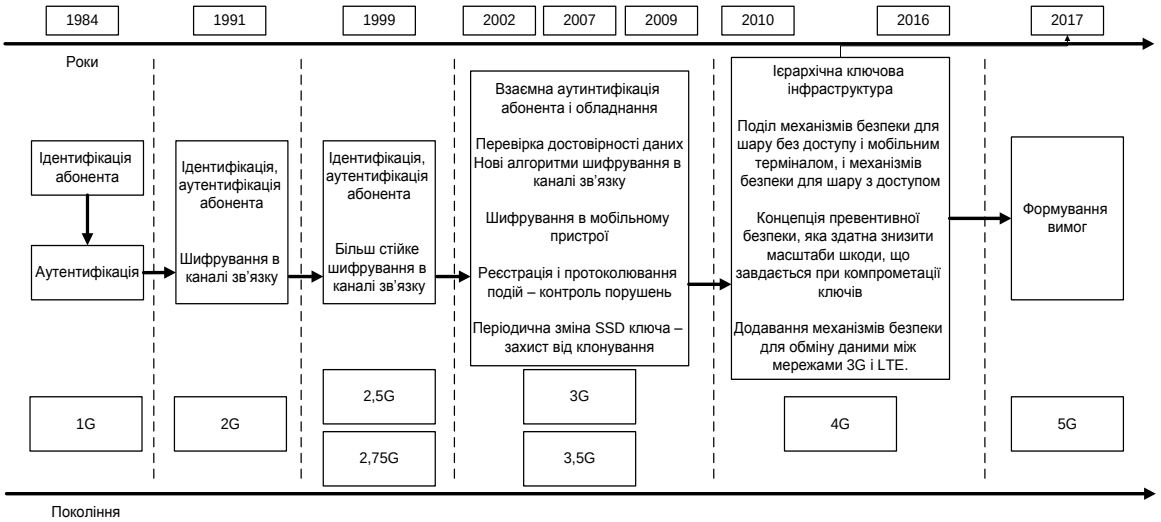

Рис. 1. Еволюція систем безпеки стільникових мереж

До табл. 2 окремо зведено відомості про наявні засоби захисту інформації в мережах LTE [12] та Wi-MAX [9].

Характеристика систем безпеки стільникових мереж 4G Таблиця 2

Властивості системи	LTE	Wi-MAX
1. Ідентифікація мобільних користувачів	Використання ME/USIM; MME; протокол PDCP; ієрархія ключів EPS; алгоритм аутентифікації HMSC-SHA-1-96 з розміром ключа 160 та 512 біт; протоколи обміну ключами через мережу Інтернет IKEv1 та IKEv2	Сертифікат X.509, ідентифікуючий абонентську станцію, а також сертифікат X.509, що ідентифікує виробника абонентської станції; 160-бітовий ключ авторизації (authorization key, AK); 4-бітовий ідентифікатор ключа авторизації; 128-бітовий ключ шифрування ключа (Key encryption key, KEK); Ключ HMAC для нисхідних (downlink) та висхідних (uplink) повідомлень при обміні ключами TEK; Список data SA, для яких дана абонентська станція авторизована; Privacy and Key Management Protocol; Extensible Authentication Protocol (EAP,розширюваний протокол аутентификации)
2. Шифрування даних	AES-CBC зі 128-бітним ключем; 3DES-CBC з 3x64 бітним ключем	DES, AES
3. Протоколи управління безпекою	Encapsulating security payload; ESP	PKM (privacy and key management protocol)

Незважаючи на значну насиченість систем захисту мереж 4-го покоління, вони мають і деякі свої вразливості. Тому необхідно запропонувати удосконалення, що дозволять їх нівелювати.

Таким чином, концептуально систему забезпечення кібербезпеки можна представити наступним чином (рис. 2).

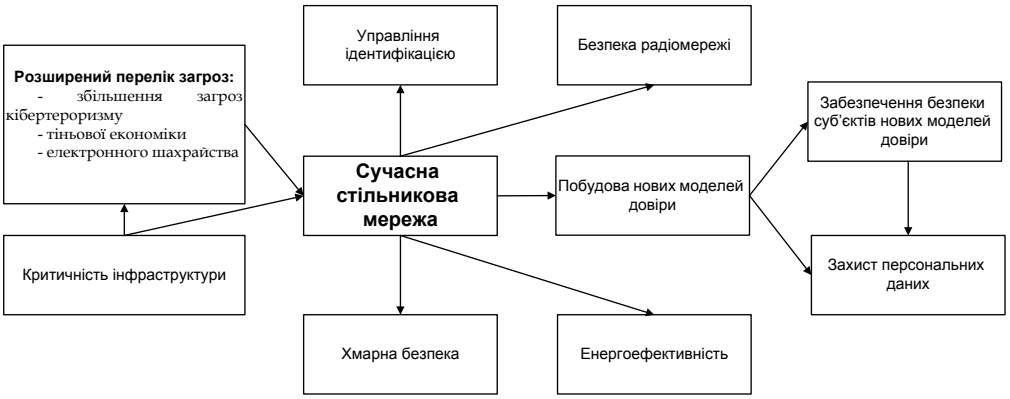

Рис. 2. Концепція забезпечення кібербезпеки сучасних стільникових мереж

Розглянемо окремі частини Концепції забезпечення кібербезпеки сучасних стільникових мереж.

Розширений перелік загроз та критичність інфраструктури. Мережі 4G та 5G відігравати-муть ще більш центральну роль в якості критичної інфраструктури, оскільки будуть здатні надавати можливість забезпечення зв'язку для вкрай чутливих додатків. Також великі проблеми, такі як збільшення загроз кібертероризму, тіньової економіки, електронного шахрайства створюються за рахунок нових можливостей стільникових мереж. Тому за рахунок цього буде здійснюватись постійний негативний вплив на стільникову інфраструктуру та її користувачів.

Нові моделі довіри. Цільові моделі постійно змінюються із плином часу. Для сучасних мобільних систем, модель довіри досить проста: вона містить 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 та захист персональних даних користувачів, як індивідуальних, так і корпоративних.

Безпека для нових моделей надання послуг. Звісно необхідно буде забезпечувати гарантований рівень безпеки для нових моделей довіри, що дозволить абонентам спокійно користуватися ресурсами стільникових мереж, збільшуючи їх дохід.

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. Серйозний інтерес прикутий до цієї проблеми і в Україні. Так, наприклад, до захисту персональних даних під час електронного декларування статків держслужбовців [12]. Як варіант доступу до цих ресурсів в майбутньому може бути використаний більш гнучкий та мобільний варіант доступу через стільникову мережу, який на той час повинен бути не менш надійний та захищений, ніж проводові системи доступу до мережі Інтернет.

Управління ідентифікацією. Розглядаючи нові шляхи для встановлення ідентичності пристроїв/абонентів, можна стверджувати, що вони є ключовим фактором який безперечно має увійти до нових моделей довіри як для сучасних версій 4G, так і майбутнього 5G.

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

Безпека радіомережі. У зв'язку із розширеною кількістю загроз і нових технологій, що забезпечує користувачам альтернативне програмування своїх власних пристроїв (навіть на рівні радіодоступу), захист від атак на радіомережі повинен бути більш чітко вираженим в новій архітектурі мереж, що має враховувати захист від загроз, таких як DoS (відмова в обслуговуванні) [13] через потенційно некоректно працюючі пристрої і додаючи заходів з пом'якшення наслідків нового дизайну радіопротоколу.

Енергоефективність. У той час, як сервіси забезпечення безпеки пов'язані із витратами, це не більше не є 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 [14]. Тим не менш, для найбільш енергонезалежних пристроїв з необхідним тривалим часом роботи, може виникнути необхідність розглянути ще менш енерговитратні рішення.

Хмарна безпека. Тема забезпечення хмарної безпеки вже стала надзвичайно гарячою, і, безперечно, буде додана до списку проблем сучасних стільникових мереж. Наведемо тільки короткий перелік пріоритетів для забезпечення хмарної безпеки в контексті майбутніх мереж 5G, керуючись вище викладеним матеріалом:

– розробка гіпервізорів і віртуалізації мережі з високим рівнем гарантії ізоляції. Як уже згадувалося, інвестиції в цій області можуть окупитися, так як це значно спростити 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.

Таким чином, у відповідності до концепції (рис. 2), щоб стільникова мережа була здатна забезпечувати ефективну передачу даних із гарантованим рівнем забезпечення кібербезпеки операторам стільникового зв'язку та розробникам обладнання до них необхідно розробляти нові, більш ефективні засоби забезпечення безпеки, до яких безперечно необхідно віднести нові алгоритми шифрування радіо інтерфейсу та відносно новий механізм відстеження кіберінцедентів в будь-якій мережі – CERT (Computer Emergency Response Team) [15]. Розглянемо їх більш детально.

Як було продемонстровано в табл. 2 та інших джерелах [11] для шифрування даних в мережах 4G використовується загальновідомий AES, який є розробкою NIST (National Institute of Standards and Technology), із різною довжиною ключа. Цей стандарт являється одним із найпоширеніших і використовується в пристроях більшості виробників обладнання. Проте, як відзначається в багатьох відкритих джерелах, наприклад в [16], Сполучені Штати Америки залишили, так званий backdoor, з можливістю дешифрування даних і їх використання в своїх інтересах, що зовсім не відповідає концепції забезпечення кібербезпеки, а тому й вимагає заміни. Тому на основі проведеного аналізу були виявлені вітчизняні аналоги розглядуваного шифру. Так в роботі [17] запропоновано нові алгоритми шифрування інформації для підвищення ефективності захисту електронних інформаційних ресурсів. Окрім високої криптостійкості, результати експериментального дослідження алгоритми Luna та Neptun показали, що ці алгоритми мінімум в 2 рази швидші за наш національний стандарт шифрування ДСТУ ГОСТ 28147-2009 та алгоритм AES. Крім того, вони пройшли комплексний контроль за методикою NIST STS і показали кращі результати, ніж генератори на основі інших алгоритмів шифрування. Також показано, що запропоновані алгоритми практично стійкі до лінійного та диференційного криптоаналізу.

Іншим нововведенням до архітектури сучасних стільникових мереж є MO CERT (Mobile operator Computer Emergency Response Team) (рис. 3).

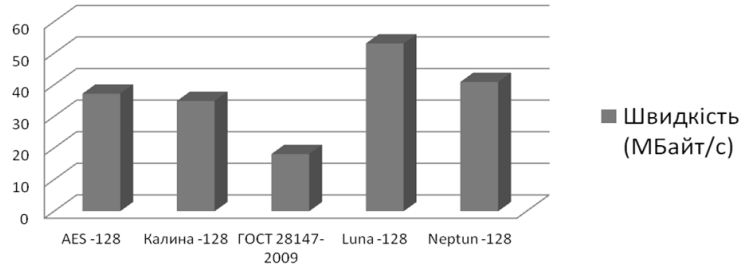

Рис. 3. Порівняльна характеристика швидкісних характеристик алгоритмів шифрування

Основне завдання MO CERT – зниження рівня загроз інформаційної безпеки для користувачів стільникової мережі. MO CERT здійснює збір, зберігання і обробку статистичних даних, пов'язаних з поширенням шкідливих програм і мережевих атак на підконтрольній території. До компетенції служби входить обробка наступних комп'ютерних інцидентів з метою їх виявлення та нейтралізації:

– атаки на вузли мережевої інфраструктури і серверні ресурси, з метою порушення їх працездат-

ності (DoS (відмова в обслуговуванні) і DDoS) і конфіденційності інформації;

– несанкціонований доступ до інформаційних ресурсів;

– поширення шкідливого програмного забезпечення, незатребуваної кореспонденції (спам);

– сканування національних інформаційних мереж і хостів;

– підбір та захоплення паролів і іншої аутентификационной інформації;

– злом систем захисту інформаційних мереж, в тому числі з використанням шкідливих програм (снифферів, руткітів, кілоггерів і т.д.).

Розглянутий короткий перелік нововведень зовсім не є вичерпним та має на меті демонстрацію можливостей та необхідності у генеруванні нових технічних рішень для концепції забезпечення кібербезпеки сучасних стільникових мереж.

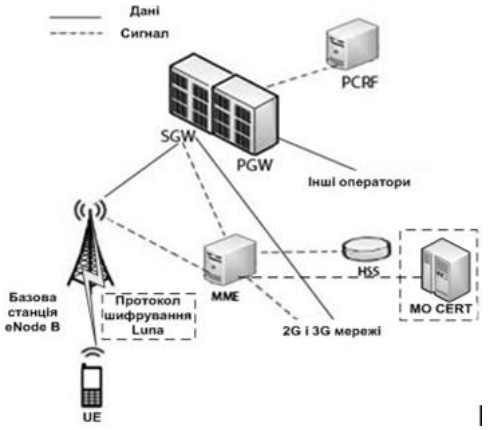

Рис. 4. Спрощена архітектура мережі LTE

Висновки

Розглянутий розвиток стільникових мереж зв'язку як в Україні, так і в світі дав змогу обґрунтувати необхідність дослідження сучасних стільникових мереж, а також були проаналізовані системи безпеки цих мереж. Проте, незважаючи 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 стільникові мережі відіграватимуть в майбутньому 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. З огляду на це були сформульовані концептуальні засади забезпечення кібербезпеки у сучасних стільникових мережах, що дозволило обґрунтувати необхідність проведення подальших досліджень, пов'язаних із оптимізацією захисту даного типу мереж, в тому числі і на шляху розвитку до 5G.

Література

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

[2] Одарченко Р.С. Стратегії розвитку операторів стільникового зв'язку в Україні // Наукоємні технології Том 26, № 2 (2015). – С. 141-48.

[3] Національний проект «Відкритий світ» - це проект освіти майбутнього, що стає реальністю для України вже сьогодні [Електронний ресурс]. – Режим доступу: http://www.educom.ua/uk-ua/about/.

[4] Global mobile suppliers association [Електронний ресурс]. – Режим доступу: http://www.gsacom.com/downloads/pdf/GSA_Evolution_to_LTE_report_060514.php4.

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

[6] 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.

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

[8] 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.

[9] Одарченко Р., Беженар Ю., Ксендзенко А. Аналіз вразливостей систем захисту інформації в мережах Wi-Max та методів їх усунення // Защита информации. Сб. научных трудов.- Киев: НАУ, 2011. - Выпуск № 18.- С. 39-44.

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

[11] 3G security; Network Domain Security (NDS); IP network layer security [Електр. ресурс]. – Режим доступу: http://www.3gpp.org/ftp/Specs/htmlinfo/33210.htm.

[12] У Держспецзв'язку відмовилися атестат відповідності системі електронного декларування [Електронний ресурс]. – Режим доступу: http://dt.ua/UKRAINE/u-derzhspeczv-yazku-vidmovilisya-vidavati-atestat-vidpovidnosti-sistemi-elektronnogo-deklaruvannya-216173_.html.

[13] Raymond D. R., Midkiff S. F. (2008). Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. IEEE Pervasive Computing, January-March 2008, pp 74-81.

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

[15] Computer Emergency Response Team of Ukraine [Електронний ресурс]. – Режим доступу: http://cert.gov.ua/

[16] Encryption AES - is there really a backdoor [Електронний ресурс]. – Режим доступу: https://forums.hak5.org/index.php?/topic/13355-encryption-aes-is-there-really-a-backdoor/

[17] Кінзерявий В., Гнатюк С., Кінзерявий О. Нові ефективні алгоритми шифрування інформації // Захист інформації. – №4 (57). – 2015. – С. 132-142.

УДК 621.396: 621.395: 007.681 (045)

Одарченко Р.С., Гнатюк В.А. Концептуальные основы повышения уровня кибербезопасности современных сотовых сетей

Аннотация. *В данной работе проанализирована эволюция сотовых сетей связи от 1-го до 5-го поколений. Кроме этого, были проанализированы системы безопасности этих сетей и также была показана их эволюция. Более подробно были рассмотрены возможные технические решения для систем безопасности современных в настоящее время сетей LTE. В результате проведенных исследований стало ясно, что эти сети и сети 5G сиграют в будущем наиболее значимую роль в формировании электронного общества, будут использованы для обеспечения потребностей и требований критической инфраструктуры и тому подобное. На основе проведенных исследований была предложена концепция построения системы кибербезопасности сотовых сетей, при этом указаны ключевые направления совершенствования современных систем безопасности: управление идентификацией, безопасность радиосети, повышение энергоэффективности, гибкая и масштабируемая архитектура, безопасность облачных сервисов. 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 данного типа сетей, в том числе и 5-го поколения. Также были предложены технические усовершенствования архитектуры и технологий сотовых сетей LTE учитывающие новейшие разработки в этой области.*

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

Odarchenko R., Gnatyuk V. Conceptual framework of modern cellular network cybersecurity rising

Abstract. *This paper analyzes the evolution of mobile networks from 1st to 5th generations. In addition, analyzed security of these networks was also examined their evolution. More details were discussed possible technical solutions for the most advanced security systems currently LTE Networks. As a result of the research it became clear that the 5G network will play in the future, the most important role in the formation of e-society used to meet the needs and requirements of critical infrastructure and so on. On the basis of the research was proposed concept of cellular networks cybersecurity systems building, while outlining key areas of improvement of modern systems of security, identity management, security, network, energy efficiency, flexible and scalable architecture, security, cloud services and more. 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 this type of network, including the 5th generation. There were also proposed technical improvements to the architecture and technology of LTE cellular networks in view of the latest developments in this field.*

Key words: *security of information, information security, LTE, 5G, cellular networks, trust model, confidentiality, threat, authentication management, radio network, encryption protocols, conception.*

Отримано *16 травня 2016 року*, затверджено редколегією *31 травня 2016 року*