Вінницький національний технічний університет
Факультет інфокомунікацій, радіоелектроніки та наносистем
Кафедра телекомунікаційних систем та телебачення

Пояснювальна записка

до магістерської кваліфікаційної роботи
за освітньо-кваліфікаційним рівнем «магістр»
на тему:
ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМ МОБІЛЬНОГО ЗВ'ЯЗКУ
08-34.МКР.002.00.000 ПЗ

Виконав: студент 2-го курсу,
групи ТТК-18м
спеціальності 172 – Телекомунікації та радіотехніка

_____ Вітюк М. О.

Керівник: к.т.н., доцент каф. ТКСТБ

_____ Семенова О.О.

«____» _____ 2019 р.

Рецензент: к.т.н., доцент каф.

.

«____» _____ 2019 р.

ВНТУ ФІРЕН ТКСТБ МКР 2019

Вінниця ВНТУ - 2019 рік

Вінницький національний технічний університет
Факультет інфокомунікацій, радіоелектроніки та наносистем
Кафедра телекомунікаційних систем та телебачення
Освітньо-кваліфікаційний рівень магістр
Галузь знань 17– Електроніка та телекомунікації
(шифр і назва)
Спеціальність 172 – Телекомунікації та радіотехніка
(шифр і назва)
Освітня програма Технології та засоби телекомунікацій

ЗАТВЕРДЖУЮ
Завідувач кафедри ТКСТБ
к.т.н., проф Г.Г. Бортник

"___" _____2019 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Вітюку Максиму Олеговичу
(прізвище, ім'я, по батькові)

1. Тема роботи Підвищення інформаційної безпеки систем мобільного зв'язку

керівник роботи Семенова Олена Олександрівна, к. т. н, доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від "02" 10 2019 року № 254
2. Строк подання студентом роботи 02 грудня 2019 року

3. Вихідні дані до роботи: діапазон частот: 1920...2175 МГц, довжина коду 20 і 50, швидкість коду ½, ймовірність імітонав'язування не більше 10^{-9}, ймовірності прийому всього виклику не менше 0,95, відношення сигнал/завада не менше 1,8дБ, періодичність передачі пакету 100мс і 500мс, розмір пакету 512 байт.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) вступ; техніко – економічне обґрунтування тематики; особливості захисту інформації у мережах 3G; забезпечення безпеки в мережах 4G; система ідентифікації користувача на базі нейронної мережі; розроблення приймача; економічна частина; охорона праці та безпека в надзвичайних ситуаціях; висновки; література; додатки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
1) Схема моніторингу загроз. Плакат
2) Генератор псевдовипадкової бітової послідовності. Структурна схема
3) Система ідентифікації. Схема структурна
4) Нейронна мережа. Структурна схема
5) Дискретно-неперервний канал. Схема структурна.
6) Дослідження пропускної здатності. Плакат
6. Консультанти розділів роботи

ВНТУ ФІРЕН ТКСТБ МгР 2019

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Технічна частина	Семенова О.О., доцент каф. ТКСТБ		
Економічна частина	Адлер О.О. доцент каф. ЕПВМ		
Охорона праці та безпека в надзвичайних ситуаціях	Березюк О.В., доцент каф. БЖДПБ		

7. Дата видачі завдання 02 вересня 2019 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Розробка технічного завдання	06.09.2019р.	
2.	Техніко-економічне обґрунтування розробки	13.09.2019р.	
3.	Дослідження особливостей захисту інформації	04.10.2019р.	
4.	Розроблення системи ідентифікації користувача	25.10.2019р.	
5.	Дослідження впливу завад	08.11.2019р.	
6.	Аналіз економічної ефективності розробки	15.11.2019р.	
7.	Аналіз безпеки життєдіяльності, цивільний захист	22.11.2019р.	
8.	Оформлення пояснювальної записки та графічної частини	29.11.2019р.	
9.	Нормоконтроль МКР	02.12.2019р.	
10.	Попередній захист МКР, рецензування МКР	06.12. 2019р.	
11.	Захист МКР ДЕК	09.12. 2019р.	

Студент _____ Вітюк М. О.
(підпис)

Керівник роботи _____ Семенова О.О.
(підпис)

ВІТУ ФПЕН ТКСТБ МКР 2019

РЕФЕРАТ

УДК 621.396

Вітюк Максим Олегович. Підвищення інформаційної безпеки систем мобільного зв’язку. Магістерська кваліфікаційна робота. – Вінниця: ВНТУ, 2019. – 95с.

На українській мові. Бібліогр.: 29 назв; Рис.:32; Табл.: 23.

Магістерська робота присвячена розробленню та дослідженню методів підвищення ефективності захисту інформації у системах стільникового зв’язку. У роботі проаналізовано сучасні методи підвищення інформаційної безпеки у системах стільникового зв’язку третього та четвертого поколінь. Розраховано економічний ефект. Розглянуті питання безпеки життєдіяльності та охорони праці. Отримані результати задовольняють вимогам технічного завдання.

Ключові слова: мобільний, захист, атака.

ВНТУ ФІРЕН ТКСТБ МКР 2019

ABSTRACT

UDK 621.396

Vitiuk Maksym Olehovych. Increasing of information security in mobile communication systems. Master thesis. – Vinnytsya: VNTU, 2019. – 95pp.

In Ukrainian language. Refs.: 29 titles; figs.: 32; tables: 23.

The master thesis is dedicated to developing and researching the methods of infofmation security efficiency increasingin cellular systems. In this thesis modern methods of information security efficiency increasing in the third and fourth generation mobile systems have been analyzed. The economic gain has been calculated. Problems of industrial and occupational safety have been considered. The obtained results satisfy preliminary specifications.

Keywords: mobile, protection, attack.

ВНТУ ФІРЕН
ТКСТБ МКР 2019

ЗМІСТ

ВІТУ ФЛРЕН ТКСТБ МКР 2019

ВНТУ ФІРЕН ТКСТБ МКР 2019

ВСТУП

Актуальність теми. Сучасні мережі мобільного зв'язку мають багато прогалин у своїх системах безпеки. Так, розглянемо основні проблемні місця у технології LTE [1]. Першою очевидною загрозою безпеки можна вважати так звані атаки DoS (Denial of Service) на комунікаційну мережу. Хоча ємність радіоканалу у системі LTE є досить великою, все ж таки вона має певні обмеження. Всі мережеві ресурси базової станції розподіляються між користувачами, і хоча існують певні обмеження проти монополізації смуги одним користувачем, атака на відмову у обслуговуванні мережі є цілком ймовірною. Зникнення RNC привело до того факту, що доступ до ядра системи LTE є можливий безпосередньо із базової станції.

Іншою загрозою є вірусні атаки. Схильними до таких атак є пристрої, а не мережа в цілому, але технологія LTE підвищує швидкість розповсюдження шкідливих програм, та як стандарт LTE є високошвидкісним. Крім того, оплата за користування послугами систем четвертого покоління не залежить від обсягу трафіку, тарифи є або безлімітними, або із обмеженнями за смугою пропускання. Саме тому абоненти не можуть швидко помітити трафік, котрий породжує шкідлива програма. Це означає, що розробники вірусів мають більше розробок: починаючи від стеження за конкретною людиною і закінчуючи одноразовими паролями у системах банківського обслуговування. Третьою небезпекою є атаки на так звані додаткові сервіси. Взагалі, технологія LTE була розроблена не лише для забезпечення абонентам доступу до мережі Інтернету, а скоріше у якості платформи для впровадження новітніх послуг, до яких належать відео та ігри. Такі сервіси є вразливими для атак різних видів, які можуть надходити або з Інтернету, або з мобільної мережі. Також можливо, що після атаки сервісу, зловмисник впровадити у абонентські пристрої шкідливу програму.

Загроза для користувачів системи LTE може надходити також від сервісів подвійного призначення. Оператор мобільного зв'язку мають багато цінної інформації про користувачів, і рано чи пізно можуть захотіти монетизувати її.

ВНТУ ФІРЕН ТКСТБ МКР 2019

LBS-сервіси є типовим прикладом такої ситуації. З однієї сторони їх можна застосувати, наприклад, для контролю переміщення вантажу, визначення місцезнаходження неповнолітніх дітей, оповіщення населення про надзвичайні ситуації. З іншої сторони їх можна застосувати для незаконного стеження за абонентом. З розповсюдженням смарт-пристроїв кількість потенційно небезпечних сервісів буде лише збільшуватись. Такий сервіс дозволяє зловмиснику одержати доступ до інформації провайдера та побудувати нову схеми здійснення злочинів або незаконного одержання коштів. І це є далеко не повним переліком нових загроз, що пов'язані із впровадженням LTE. Окрім того, є певні проблеми і з власне стандартом. Досить гостро стоїть питання взаємодії із недовіреними мережами. Якщо трафік між устаткуванням користувача та eNB шифрується і загроза порушення конфіденційності є неактуальною, то у такому випадку, взаємодія eNB із радіоконтроллер мережі третього покоління є не захищеною за замовчуванням, а отже, з боку зловмисників можлива атака. Так само як відсутність обов'язкової аутентифікації між eNB і ядром мережі, цю опцію оператор мобільного зв'язку може або використовувати, або не використовувати з метою зниження своїї витрати з розгортання мережі стандарту LTE.

До останнього часу основним чинником для еволюції мереж мобільного зв'язку було підвищення пропускної здатності та зменшення затримки, що забезпечує оптимальний доступ до Інтернету. А от мережі наступних поколінь вимагають принципово нову модель для забезпечення безпеки інформації, так як вони володіють суттєво розширеним функціоналом. По-перше, вони сконструйовані не тільки для забезпечення потреб суспільства, а й для об'єднання цілих індустрій.

Основні чинники розвитку мереж мобільного зв'язку можна згрупувати у характеристики, кожна з яких чинить вплив на формування вимог для забезпечення інформаційної безпеки та недоторканності приватного життя людей. До цих характеристик належать: нові моделі служби доставки, нові моделі довіри, збільшення рівня конфіденційності, розширений перелік загроз. Таким чином,

ВНТУ ФРЕН ТКСТБ МКР 2019

вказані характеристики впливають на підходи до формування вимог до систем забезпечення безпеки та конфіденційності у системах мобільного зв'язку.

Аналіз останніх досліджень. Таким чином, задача забезпечення інформаційної безпеки в мережах мобільного зв'язку є актуальною, і рішення її можливо із використанням нових технологій в області систем зв'язку. Питання підвищення безпеки зв'язку досліджували вчені: Одарченко Р.С., Яковлєв В.А., Коржик В. І., Бакаєв М.В., Ковайкін Ю.В., U. Maurer, S. Wolf, J. Wallace, R. Sharma, T. Aono та ін [1-10].

Мета та задачі дослідження. Метою даної магістерської кваліфікаційної роботи є дослідження механізмів забезпечення безпеки інформації у мережах мобільного зв'язку.

Для досягнення мети необхідно розв'язати такі задачі:

- огляд механізмів забезпечення інформаційної безпеки у мережах мобільного зв'язку;
- аналіз проблемних місць у забезпеченні безпеки та способи їх подолання;
- розроблення методів підвищення інформаційної безпеки.

Об'єктом дослідження є фізичні процеси у пристроях мобільного зв'язку.

Предметом дослідження є пристрої системи мобільного зв'язку.

Методи дослідження. Для рішення поставлених завдань були використані методи теорії інформації та передавання сигналів, методи теорії телетрафіку, методи комп'ютерного моделювання та оптимізації.

Наукова новизна одержаних результатів полягає у наступному:

- запропоновано алгоритм ідентифікації користувача на базі нейронної мережі;
- досліджено стійкість запропонованої системи ідентифікації користувача на базі нейронної мережі.

Практичне значення роботи полягає у розроблені схеми нейронної мережі для ідентифікації користувача.

Особистий внесок здобувача: розроблено рекомендації до підвищення

ВНТУ ФІРЕН ТКСТБ МКР 2019

інформаційної безпеки мереж мобільного зв’язку.

Апробація результатів роботи. Основні ідеї роботи доповідались і обговорювались на І-й міжнародній науково-технічній конференції «Сучасні проблеми інфокомунікацій, радіоелектроніки та наносистем» СПІРН-2019.

ВНТУ ФІРЕН
ТКСТБ МКР 2019

1 ТЕХНІКО – ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ТЕМАТИКИ РОБОТИ

1.1 Стан проблеми

Наразі є велика кількість літературних джерел, що присвячені проблемам забезпечення інформаційної безпеки у інфокомунікаційних мережах та системах. Задачі створення, організації і дослідження процесів розроблення, функціонування та розвитку різноманітних систем захисту інформації в знайшли відображення у працях зарубіжних та вітчизняних вчених, серед яких Е.С. Вентцель, В.А. Галатенко, В.Ю. Гайкович, В.І. Гарбарчук, В.А. Герасименко, Ю.В.Демченко, В.К. Задиракa, В.І. Завгородній, В.В. Лебедєва, А.Г. Карпова, В.В. Мельникова, А.С. Олексюк, А.Н. Назаров, А.З. Пєскозуб, А.Ю. Першин, А.П.Пятібратова, С.П. Расторгуєва, В.К. Размахнін, Ю.А. Самохіна та інші [8-11]. Праці [12,13] присвячені оцінюванню систем безпеки мереж мобільного зв’язку. Однак, питання розроблення вимог до системи захисту інформації мереж мобільного зв’язку нового покоління було розроблене вітчизняними науковцями досить слабко, а тому воно представляє великий інтерес та обґрунтовує актуальність тематики дослідження. Як відомо, в даний час безпека є однією з основних проблемних точок комунікаційної мережі. Розгортання комунікаційної мережі не може реалізовуватися без забезпечення безпеки передачі інформації для усіх зацікавлених сторін, до яких належать абоненти, постачальники послуг, віртуальні оператори, провайдери інфраструктури. Отже, постає науково-технічна задача виявлення недоліків існуючих систем захисту стільникових мереж попередніх поколінь і формування вимог до безпеки мереж четвертого та п’ятого поколінь як у цілому так і для їхніх окремих компонентів.

1.2 Аналіз шляхів рішення проблеми

У той час, коли було розроблено та впроваджено системи GSM, було стандартизовано і функції безпеки, котрі враховували недоліки, якими характери-

ВНТУ ФІРЕН ТКСТБ МКР 2019

зувалися попередні аналогові системи, і були налаштовані на боротьбу з можливими загрозами. По-перше, була введена процедура шифрування радіоінтерфейса, так як з'явилася можливість прослуховування переговорів абонентів. По-друге, з'явився ризик шахрайства, що могло становити серйозну проблему. Все це призвело до застосування додаткових заходів безпеки, тобто SIM-карт, котрі дали змогу додати сильніший механізм аутентифікації. Потім, при переході до систем третього покоління, були впроваджені подальші покращення системи безпеки. Прикладами подібних удосконалень є взаємна аутентифікація для зниження таких загроз як підміна базових станцій, і передавання операції шифрування вглиб самої мережі. Коли ж були запущені мережі четвертого покоління, то одним із основних заходів безпеки стало повернення шифрування даних користувача до базової станції. Окрім того, були введені складніші ключі керування з метою захисту від можливих фізичних зломів у базовій станції.

Взагалі, архітектура системи безпеки у мережі стандарту LTE представляє собою підсистему мережі стільникового зв'язку стандарту LTE, що описано в технічних специфікаціях 3GPP TS 33.401 [14] та 3GPP TS 33.402 [15], котрі містять набір методів, які дають можливість забезпечити безпечний зв'язок між окремими вузлами мобільної мережі, а також конфіденційність та цілісність даних абонента. Ця архітектура була запропонована в 2008 році консорціумом 3GPP [15]. Вимоги до забезпечення безпеки системи LTE характеризуються так [17]:

- забезпечити рівень безпеки не нижче, ніж як і у мережах 3G;
- забезпечити захист від Інтернет-атак;
- механізм безпеки не повинен створювати проблем при переході зі стандарту 3G на стандарт 4G;
- забезпечити можливість використання модуля USIM, що представляє собою універсальну сім-карту.

Загалом, механізми безпеки, пропоновані технологією LTE дуже схожі на заходи мереж захисту 3G проте посилені, хоча мають і свої особливості. Розмірковуючи про необхідність забезпечення безпеки мереж поколінь 2G-4G, мож-

ВНТУ ФІРЕН ТКСТБ МКР 2019

на додати, що для них системи безпеки були впроваджені в основному з метою захисту саме основних послуг, до яких належали спочатку передача голосу, а потім і пакетних даних для того, аби забезпечити довіру абонентів, а також для захисту екосистеми за умов правильної взаємодії всіх учасників процесу. Слід зазначити, що вказаний підхід дуже добре функціонував. Хоча деякі спроби здійснення нападу на системи безпеки GSM-мереж і відбулися протягом останніх років, це були малоефективні та поодинокі випадки. Тобто, цілі, для яких і було розроблено систему безпеки мережі GSM, були виконані та перевиконані. Все це стосується й нових та більш прогресивних мереж третього й четвертого поколінь.

1.3 Вибір оптимального варіанта рішення проблеми

Через розширений перелік кількістю загроз та впровадження нових технологій, котрі забезпечують споживачам можливість альтернативного програмування своїх власних пристроїв, механізми захисту від атак на радіо мережі мають бути більш чітко вираженими у новій архітектурі мереж стільникового зв'язку, яка повинна враховувати захист від різних загроз таких як, наприклад DoS, через пристрої, що потенційно некоректно працюють, та додавати заходи із пом'якшення можливих наслідків радіопротокола за новим дизайном. Не зважаючи на те, що радіомережі стандарту LTE характеризуються дуже хорошим захистом від криптографічного підслуховування, не існує жодного захисту проти змінювання чи ін'єкцій трафіку у площині користувача. Саме тому цей напрям досліджень також заслуговує на увагу, особливо якщо зважати на можливе застосування мереж п'ятого покоління.

Зважаючи на можливість віртуалізації та більш динамічну конфігурацію, що типові для мереж п'ятої генерації, доцільно розглянути більш динамічну та гнучку архітектуру системи безпеки для них. Безпека для деяких синхронних аспектів, до яких належить, наприклад, сигналізація RAN, може розташовуватися поряд із доступом із високим ступенем незалежності від асинхронних ас-

ВНТУ ФІРЕН ТКСТБ МКР 2019

пектів безпеки, наприклад таких, які пов’язані з площиною користувача. Це дає змогу більш ефективно забезпечувати безпеку передачі інформації, а також обмежити можливі загрози інформації користувача. Нові проекти безпеки із високим рівнем гнучкості також можуть краще слугувати для розв’язання непотрібних конфліктів між безпекою та зручністю.

1.4 Постановка задач дослідження

Отже, для розв’язання проблеми підвищення інформаційної безпеки, яка виникла на сучасному етапі розвитку науки і техніки, потрібно розв’язати наступні задачі:

- огляд механізмів забезпечення інформаційної безпеки у мережах мобільного зв’язку;
- аналіз проблемних місць у забезпеченні безпеки та способи їх подолання;
- розроблення методів підвищення інформаційної безпеки.

ВНТУ ФІРЕН ТКСТБ МКР 2019

2 ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ У МЕРЕЖАХ 3G

2.1 Проблеми безпеки інформації

Для визначення можливих загроз безпеки мережі третього покоління потрібно оцінити її інфраструктуру. Як видно на рис. 2.1, мережа 3G складається з двох частин, а саме

- радіомережа доступу (Radio Access Network);
- базова мережа (Core Networ).

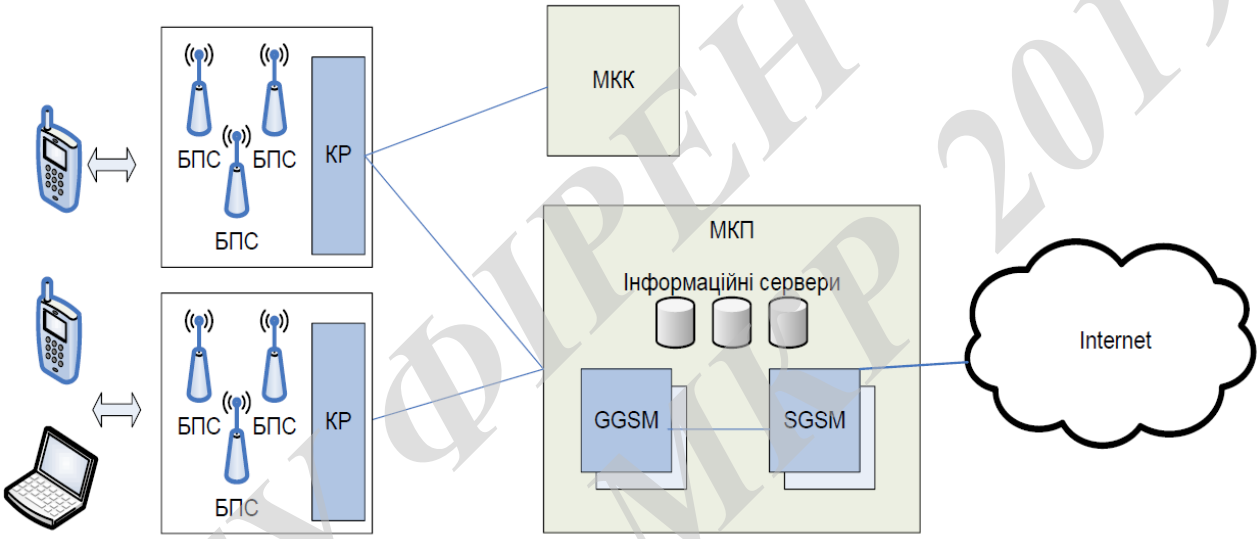


Рисунок 2.1 – Архітектура радіомережі 3G

Радіомережа доступу складається з двох мереж: існуючої мережі GPRS/GSM, до якої підключена мережа із пакетною комутацією (МКП) та мережі із канальною комутацією (МКК). Для реалізації повного переходу до мереж третього покоління МКП з'єднується з системою UTRAN (Universal Terrestrial Radio Access Network), котра UTRAN складається з підсистеми, що в свою чергу містить входить контролер радіомережі (КР), до якого під'єднуються декілька базових передавальних станцій (БПС).

Згідно рис.2.1 базова радіомережа складається із мереж КП та КК. Мережа КП містить сервери SGSM (Serving GPRS Support Node) та GGSM (GPRS Gateway Service Node). Кожен сервер SGSN з'єднує кілька КР із мережею КП.

ВНТУ ФІРЕН ТКСТБ МІР 2019

До функцій серверу відносять керування мобільністю, маршрутом, доступом, а також сповіщеннями. GGSM є логічним шлюзом для з'єднання із Інтернетом. Інформаційні сервери виконують різноманітні функції, такі як визначення місця розташування користувача і аутентифікація користувача. Крім того, існують сервери DNS, DHCP та RADIUS, котрі взаємодіють із SGSN/GGSN і реалізують функції керування і контролю.

Отже, інфраструктура 3G мережі є досить масивною та складною із великою кількістю об'єктів, що взаємодіють між собою. Тому важливою проблемою є забезпечення безпеки інофрмації у кожному каналі зв'язку.

Деякі обмеження висувають д стільникових мереж на відміну від проводових:

1. Безпроводового середовище є відкритим, оскільки дані передаються по радіоефірі, то немає фізичного бар'єра, який завадив би зловмиснику одержати доступ.

2. Пропускна здатність є обмеженою, хоча пропускна здатність безпроводових мереж все збільшується, вона все одно є нижчою за пропускну здатність проводових технологій.

3. Безпроводові системи характеризуються підвищеною складністю через необхідність забезпечення мобільності, а також їхньою здатність ефективно використати канал передачі.

4. Обчислювальна потужність є обмеженою, оскільки процесори, котрі встановлюють на безпроводових пристроях, не володіють достатньою потужними, щоби обробляти інформації із потрібною інтенсивністю.

5. З'єднання із мережею є ненадійним, оскільки під час передавання сигналу по каналу зв'язку на нього чинять вплив значно більше завад ніж це відбувається у проводових мережах.

Розглянемо основні недоліки стільникової мережі, котрі враховують при розгортанні стільникової інфраструктури.

Завдяки виконанню операції аутентифікації оператор має змогу впевнитися, що суб'єкт дійсно є тим, за кого він себе видає. За значної кількості або-

ВІТУ ФІРЕН ТКСТБ МКР 2019

нентів операторові треба впевнитися, що від надає послуги саме тим користувачам, котрі мають на це право.

Так як наразі більшість телефонів мають операційні системами, котрі володіють такими ж самими можливостями, як і персональні комп'ютери, то тому актуальною проблемою є мобільні операційні системи, так як у них можуть виявитися недоліки, якими можуть скористатися зловмисники.

Веб-сервіс представляє собою є компонент, який забезпечує функціональність доступа через мобільну мережу, у цьому випадку застосовується HTTP протокол. Саме це і робить стільникові телефони вразливим до таких загроз як віруси, переповнення буфера, та атаки типу «відмова у обслуговуванні».

Оскільки у мережі мобільного зв'язку визначити місце розташування абонентів можна досить легко, то таку інформацію треба приховувати.

У випадку, коли стільниковий телефон втрачено, він має бути захищеним від несанкціонованого використання, аби неможливо було одержати доступ до персональної інформації користувача.

Існують такі види атак на мережу мобільного зв'язку (рис. 2.2):

- Найпотужнішою атакою є атака типу «відмова у обслуговуванні» (DoS), яка може призвести до неробочого стану всієї мережевої інфраструктури. Така атака може бути реалізована при надмірному передаванні даних у безпровідній мережі, оскільки це це призводить до неможливості використання сервісів окремими користувачами.
- При здійсненні атаки «розподілена відмова у обслуговуванні» (DDoS) задіюється велика кількість вузлів.
- При несанкціонованому доступі належним чином не використовується аутентифікація. Це означає, що зловмисники можуть отримати доступ до безпровідної мережі і нелегально використовувати її послуги.
- При підслуховуванні зловмисники мають можливість підслуховувати і перехоплювати конфіденційну інформації.

ВНТУ ФІРЕН ТКСТБ МКР 2019

- При підробленні повідомлень зловмисники фальсифікують дані у випадку, які предаються через незахищений канал передачі, та передають їх далі у мережу.
- При здійсненні атаки «Відтворення повідомлення –Навіть, коли канал передачі безпечний, зловмисник може перехоплювати зашифровану інформацію та відправити її користувачу.
- Hijack атака, тобто коли зловмисники підключаються до мережі працюють як законна базова станція

В основі безпеки 3G технологій лежать такі функції забезпечення безпеки:

- аутентифікація користувачів;
- шифрування даних для передавання по інтерфейсу;
- тимчасова ідентифікація.

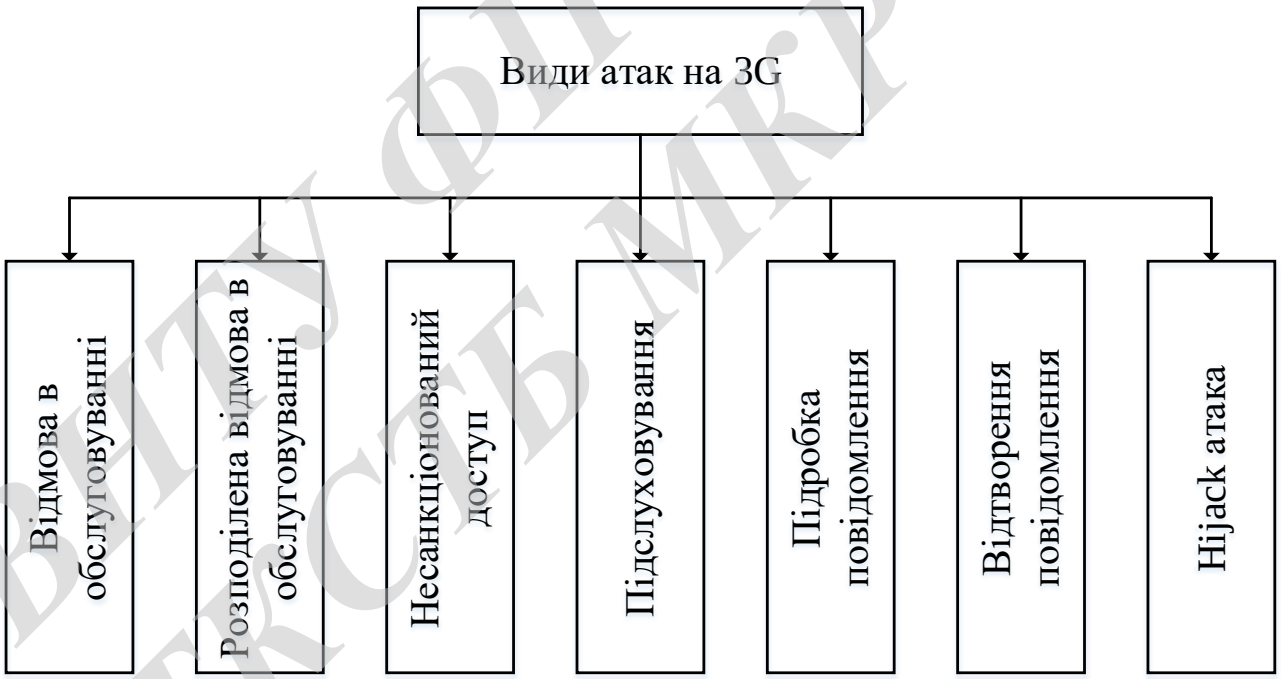


Рисунок 2.2 – Види атак

Аутентифікація абонента у 3G технології здійснюється шляхом шифрування за протоколом типу «запит-відгук» із загальним ключем. При

ВНТУ ФІРЕН ТКСТБ МКР 2019

здійсненні аутентифікації мережі можливість вибору алгоритму надається оператору [16].

Алгоритми аутентіфікації в технології 3G можна поділити на дві групи – з блоковим симетричним шифруванням та без шифрування. До першої групи відносять використання блокового шифрування в режимі CBC. При цьому, останній зашифрований блок призначений для формування аутентифікаційного кода блокового симетричного шифрування. Прикладом другої групи є алгоритм формування аутентифікаційного коду за HMAC протоколом.

Для реалізації передачі даних у технології 3G застосовують функцію шифрування f8 та функцію f9, котра відповідає за цілісність даних. Функція f8 базується на так званому алгоритмі KASUMI, котрий був розроблений групою SAGE (Security Algorithms Group of Experts).

Також технологія 3G реалізує:

- взаємну аутентифікацію, це означає, що для усунення можливості атаки із застосуванням помилкової базової станції абонент в свою чергу аутентифікує мережу;
- взаємне підтвердження ключів аутентифікації ы шифрування між користувачами та мережею;
- захист цілісності даних, при якому для забезпечення цілісності застосовуються удосконалені алгоритми;
- мережеву безпеку, тобто шифрування реалізується всередині мережі та між різними мережами;
- безпеку додатків та сервісів, для цього було удосконалено механізми для забезпечення надійності.

Також вищенаведені принципи та методи забезпечення безпеки інформації у технології 3G можуть протидіяти загрозам, котрі мали місце у мережах 2G:

- підключення фальшивої базової станції;
- викрадення каналу зв’язку під час сесії;
- перехоплення ключів аутентифікації та шифрування;

ВНТУ ФІРЕН ТКСТБ МКР 2019

- загроза порушення цілісності даних;
- складність у впровадженні новітніх механізмів інформаційного захисту.

2.2 Алгоритми забезпечення безпеки

Існують такі основні алгоритми забезпечення безпеки у системах зв'язку третього покоління:

f0 – функція генерування параметрів виклику ;

f1 – функція аутентифікації мережі;

f2 – функція аутентифікації абонента;

f3 – функція генерування ключа шифрування;

f4 – функція генерування ключа перевірки цілісності;

f5 – функція генерування ключа анонімності.

У технології 3G реалізується схема взаємної аутентифікації рухомої станції та мережі (рис. 2.3). Після отримання від рухомої станції запиту на обслуговування, стільникова мережа ініціює процедуру аутентифікації абонента.

Центр аутентифікації стільникових мереж третьог покоління генерує випадкове число RAND використовуючи функції f_0, а потім генерує параметр аутентифікації AUTN, застосовуючи функцію f_1. Для цього крім числа RAND застосовується довгостроковий попередньо розподілений секретний ключ K та номер переданої послідовності даних SQN. З метою ускладнення операції визначення місцяположення користувача номер переданої послідовності даних SQN підсумується за модулем 2 з ключем анонімності KA, котрий генерується функцією f_5. Потім параметри RAND, SQN, KA та AUTN передаються на рухому станцію.

У технології 3G процедура аутентифікації абоеннтської станції мережею подібна до процедури у мережах мобільного зв'язку другого покоління. абонентська станція обчислює число RES використовуючи функцію f_2. На вхід станції поступають ключ K і RAND. Потім число RES передається у мережу, котра

ВНТУ ФІРЕН ТКСТБ МКР 2019

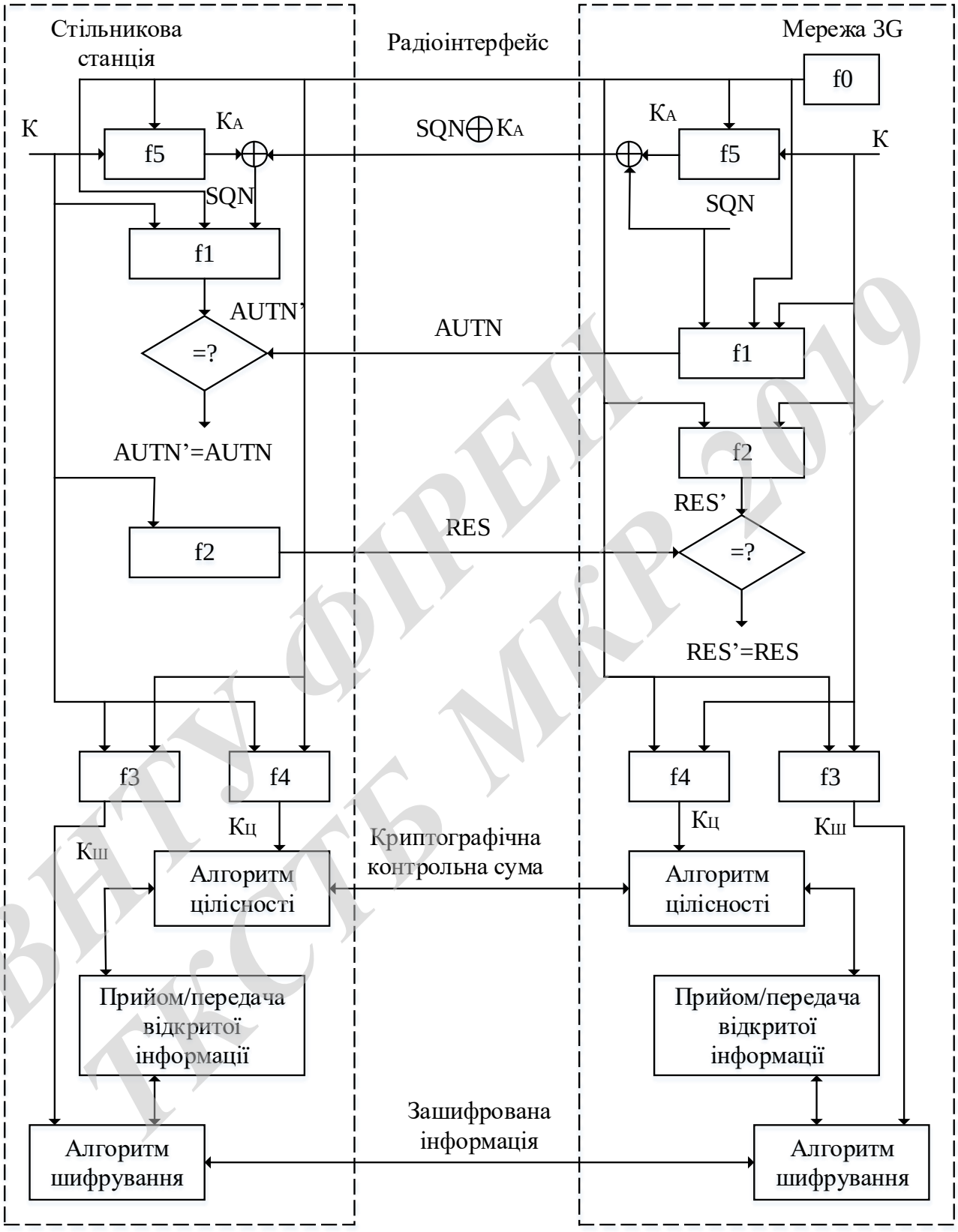
виконує такі ж самі обчислення, одержує число RES’ та порівнює його із RES. Якщо ці числа співпадають, то мережа "визнає" абонентську станцію. Отже, у системах 3G передбачені процедури підтвердження дійсності як станції, так і мережі. При розробленні архітектури доступу у технології 3G значна увага приділяється зворотній сумісності із мережами 2G , оскільки сумісність із системою, котра має набагато слабший захист, є небажаною.

З метою реалізації криптографічного захисту каналів зв’язку і мережа і станція повинні генерувати ключі шифрування та перевірки цілісності, застосовуючи при цьому функції f3 і f4 відповідно. Кожен з цих ключів має довжину 128 біт, вхідними параметрами є K та RAND. Потім реалізується потокове шифрування інформації з обох сторін. Зокрема, формування криптографічних контрольних сум дозволяє перевіряти та контролювати цілісність повідомлень у системі.

Процес шифрації даних, котрі передають через мережу (рис. 2.4) реалізується досить просто, але шифрація має місце на другому рівні, а пристрій має декілька передавальних інтерфейсів, кожен з який застосовує власний лічильник. При застосуванні лічильників, котрі мають досить короткий період маска шифрування, видана блоком, зможе на них повторюватися. Все це призводить до повторення вхідних даних функції f8, а також до різкого зниження крипостійкості мережі мобільного зв’язку. Для цього застосовується додатковий лічильник, який має більш довгий період, котрий називається Hiperframe Number і збільшується кожен раз, коли лічильник інтерфейсу переповнюється. На вхід COUNT-C подається конкатенація значень цих двох лічильників. Функція f8 визначена в стандарт, єдина та заснована на блоковому шифруванні KASUMI (специфікація 3GPP TS 35.202).

Як показано на рис.2.5, операція забезпечення цілісності майже аналогічна операції забезпечення шифрування. Так, зашифроване повідомлення пропускається через функцію f9. Лічильник COUNT-I має те ж саме значення, що і лічильник, котрий використовується для шифрування інформації. Новим тут є лише параметр FRESH.

ВНТУ ФІРЕН ТКСТБ МКР 2019



ВНТУ ФІРЕН ТКСТБ МКР 2019

Рисунок 3.3 – Схема ідентифікації та криптозахисту

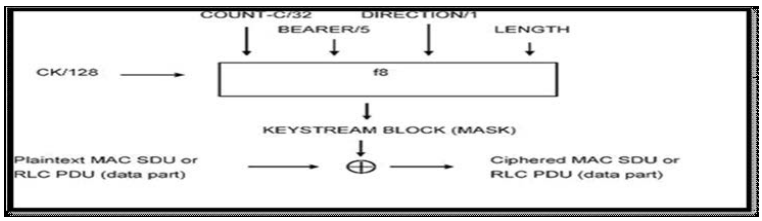


Рисунок 2.4 – Процес шифрування

Нехай перед початком з'єднання модуль ідентифікації абонента USIM повідомляє мережу про своє HFN. Якщо ключ не зміниться, тобто якщо не відбулася нова процедура аутентифікації, то зловмисник може передати на станцію інформацію з дуже малим HFN, котра була перехоплена раніше. Саме тому обслуговуюча, має призначити випадковий параметр FRESH при кожному з'єднанні. BEARER – ідентифікатор інтерфейса – уже зашифровано в самому повідомленні, тбто його не порібно враховувати, а для іншого інтерфейсу дані вже не є правильними.

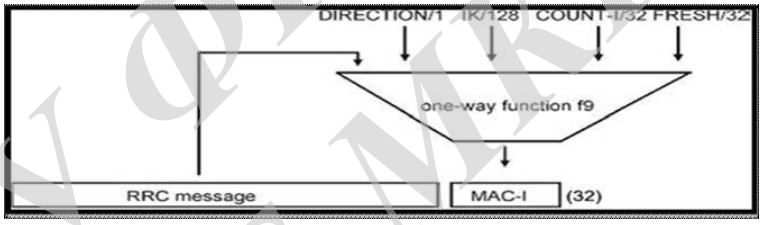


Рисунок 2.5 – Забезпечення цілісності даних

При розробленні механізмів забезпечення безпеки однією із головних проблем стає незаконність її забезпечення у ряді країн. Тому технології 3G є механізми забезпечення перехоплення з'єднань та фільтрації потрібних даних від непотрібний шляхом завдяки застосуванню спеціального обладнання. Шляхом використання пристрою «Positioning System» досягається потрібна точність позиціювання.

Перед початком процедур обміну даними між станціюєю та мережею, кожна сторона переконується в тому, що спілкуватиметься не із зловмисником (рис. 2.7). Для використовуються алгоритми аутентифікації та узгодження ключів. Модулі AuC та USIM зберігають копії основного ключа користувача,

ВНТУ ФІРЕН ТКСТБ МКР 2019

котрий призначений для взаємодії користувача із мережею. Центр аутентифікації AuC після запиту мережі створює n-компонентну таблицю аутентифікаційних векторів, компонентами яких є:

- RAND – випадкове число
- XRES – очікувана відповідь
- CK – ключ шифрування
- IK – ключ цілісності
- AUTN – маркер аутентифікації.

Із значень RAND, K та порядкового номеру SQN вектора одержуються останні чотири компонента.

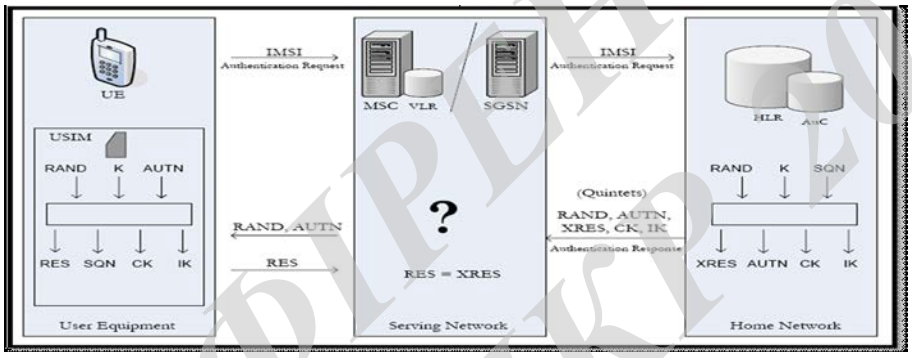


Рисунок 2.6 – Аутентифікація абонента

Регістр VLR обслуговуючої мережі обирає наступний k-тий аутентифікаційний вектор із впорядкованої таблиці. Потім він надсилає абоненту RAND(k) та AUTN(k). Далі, USIM перевіряє, чи є AUTN(k) дійсним маркером аутентифікації. У випадку, якщо це так, то генерується відповідь RES(k).

Для передавання даних у технології 3G визначені функції шифрування f8 та f9, котрі відповідають відповідно за шифрування та цілісність. Для фукнцій f8 та f9 визначають наступні такі вимоги:

- f8 – поточний шифр;
- f9 – функція множення/підсумовування;
- обидві функції мають бути реалізовані на чіпах невеликих розмірів, які характеризуються низьким енергоспоживанням;
- не має бути обмежень по заміни функцій на обладнанні користувача.

ВНТУ ФІРЕН ТКСТЗ МКР 2019

Функція f9 являє собою послідовну функція множення-накопичення, котра у ядрі має KASUMI. До кожного переданого повідомлення прикріплюється MAC-I, що представляє собою 32-х бітовий псевдовипадковий рядок. Це вихідне значення функції f9. Приймальна сторона обчислює такий же рядок. Вихідне значення функції f9 залежить майже непередбачувано від вхідних параметрів, це означає, що лише правильне поєднання ІК та лічильника забезпечує достовірність переданого повідомлення.

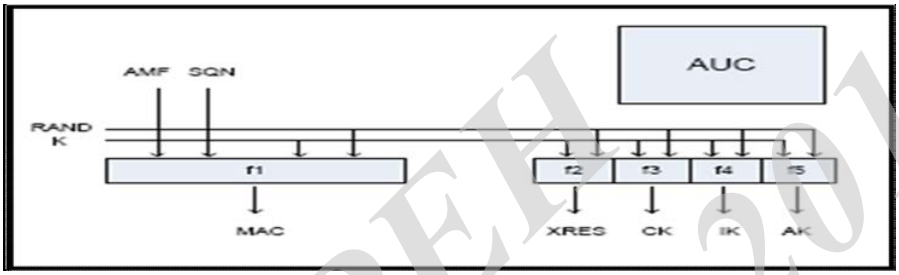


Рисунок 2.7 – Аутентифікаційні вектори

2.3 Алгоритм KASUMI

KASUMI є блоковим шифром, призначеним для мереж мобільного зв'язку третього покоління. KASUMI було розроблено на базі існуючого алгоритму MISTY1, котрий було оптимізовано для систем стільникового зв'язку.

KASUMI представляє собою блок у 64-біт та 128-бітовий ключ у схемі Фейстеля, котра складає 8 раундів. При цьому, у кожному раунді застосовується 128-бітний раундовий ключ, котрий складається із 8 16-бітових підключів, які одежрують із вихідного ключа за фіксованої процедурою генерації підключів. В непарних раундах, на відміну від парними, додатково виконується операція FL, що також реалізується і по завершенню останнього раунда. Число раундів становить 8.

Отже, при реалізації операції FL вхідне значення, котре становить 32 біти, розділяють на два блоки по 16 бітів у кожному. Потім, над вказаними блоками здійснюю операції додавання по модулю два та побітові логічні операції,

ВНТУ ФІРЕН ТКСТВ МКР 2019

причому у них беруть участь частки розширеного ключа шифрування K_{L1} і K_{L2}.

Операція FO є дещо складнішою. Так, у ній 32-бітове вхідне значення також розділяється на три 16-бітових фрагменти, один з яких обробляють за допомогою операції додавання по модулю 2 із частиною ключа для операції $FO(K_{Ox})$ та операції FI, яка на відміну від операцій FL та FO, оброблює 16-бітові блоки даних. Потім значення даних в блоках додають по модулю 2 та міняють місцями.

Трираундова мережа Фейстеля обробляє 7-бітовий та 9-бітовий блоки, над якими здійснюються наступні операції:

- табличні заміни S7 і S9 над 7 - та 9-бітовим блоками;

- додавання блоків по модулю 2 між собою; у першому та ву третьому раундах 7-бітовий блок доповнюється нулями, результатом додавання є 9-бітовий блок; в другому раунді при додаванні відкидаються два лівих біти 9-бітового блоку, а і результатом додавання є 7-бітовий блок;

- додавання за модулем 2 блоків із 7- та 9-бітовими частками розширеного ключа шифрування K_{L1} і K_{L2}, котрі реалізують у другому раунді;

Кожен раунд KASUMI генерюються ключі з загального ключа шифрування K:

- 128-бітовий ключ K ділиться на 8 ключів $K = K_1 \square K_2 \square ... \square K_8$;

- розраховується другий масив за формулою $K_{j'} = K_j \oplus C_j$.

- для кожного раунда розраховуються ключі.

У стандартах третього покоління шифр KASUMI здійснюється функцією безпеки f_8. Він функціонує у режимі зворотного зв'язку, а f_8 застосовується для генерації блоків ключового потоку, котрі побітово додаються до блоків відкритого тексту по модулю 2.

Атаки на KASUMI методом «бумерангу» зламують його швидше, ніж метод повного перебору. Але складність такої атаки становить 2^{76}, що у порівнян-

ВНТУ ФІРЕН ТКСТБ МКР 2019

ні з алгоритмом А5/1 зі складністю атаки 2^{40}, більше на 10-ки порядків. Отже, шифр KASUMI є найбільш криптостійким і його можна вважати є оптимальним вибором для шифрування даних у мережах стільникового зв'язку.

Симетричний блочний алгоритм шифрування KASUMI в алгоритмах забезпечення конфіденційності (UIA1) та цілісності (UEA1).

Криптостійкість алгоритму шифрування визначає його надійність. Необхідно відрізняти поняття теоретичної криптографічної стійкості, котра вказується розробником шифру як кількість можливих варіантів значень ключа, що можуть бути отримані методом повного перебору від поняття практичної криптографічної стійкості алгоритму шифрування, котра визначається на основі застосування ефективніших методів. Так, для алгоритма KASUMI теоретична криптостійкість становить 2128, а практична криптостійкість визначається сендвіч-атакою з пов'язаними ключами, яка є найефективнішою криптоаналітичною атакою. Цей метод не реалізований відносно реальної системи передавання даних, так як він потребує великого обсягу вхідних даних. Вищеописані методи криптоаналізу мають теоретичний характер, при цьому оцінювати їх складність потрібно практично. Тому важливо реалізувати розроблені криптоаналітичні методи на відповідних обчислювальних засобах.

2.4 Аналіз криптоалгоритму

Сендвіч-атака належить до атак так званого диференціального типу. Вона базується на «бумеранг-атаці», котра розглядає шифр в якості каскаду двох субшифрів. Сендвіч-атака розглядає алгоритм в якості каскаду трьох субшифрів.

У сендвіч-атаці реалізовано поділ шифру на три субшифри, $E=E_1+M+E_0$. Припущення тут такі як і у бумеранг-атаці: нехай є диференціал пов'язаних ключів $\alpha \rightarrow \beta$ для E_0, котрий має різницю ключів ΔK_{ab} із ймовірністю появи p, а також диференціал пов'язаних ключів $\gamma \rightarrow \delta$ для E_1, котрий має різницю ΔK_{ac} із ймовірністю появи q. Алгоритм атаки є таким же як і у базовій атаці, тобто цен-

ВНТУ ФІРЕН ТКСТБ МКР 2019

тральний субшифр M ігнорується. Але, при цьому аналіз є більш детальним та потребує уваги при розгляді залежності між різними розподілами.

Основною ідеєю сендвіч-атаки є перехід середини. У алгоритмі бумеранг-атаки, у випадку, якщо пара (P_a, P_b) є правильною парою відносно першого диференціалу, а також обидві пари ($C_в$, C_c) і (C_b, C_d) є правильними парами відносно другого диференціалу, виходить залежність:

$$(X_a \oplus X_b = \beta) \wedge (X_a \oplus X_c = \gamma) \wedge (X_b \oplus X_d = \gamma),$$

де X_i – проміжне значення шифрування Pi.

Маємо

$$X_c \oplus X_d = (X_c \oplus X_a) \oplus (X_a \oplus X_b) \oplus (X_b \oplus X_d) = \beta \oplus \gamma \oplus \gamma = \beta.$$

Результатом є $P_c \oplus P_d = \alpha$ із ймовірністю p (рис. 2.8, 2.9).

У випадку сендвіч-атаки:

$$(Xa \oplus Xb = \beta) \wedge (Ya \oplus Yc = \gamma) \wedge (Yb \oplus Yd = \gamma).$$

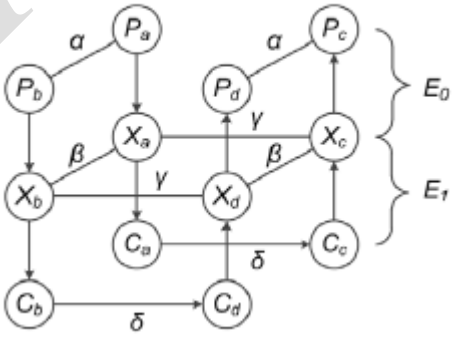


Рисунок 2.8 – Конструкція квартетів «бумеранг» та «сендвіч»

ВНТУ ФІРЕН ТКСТЬ МКР 2019

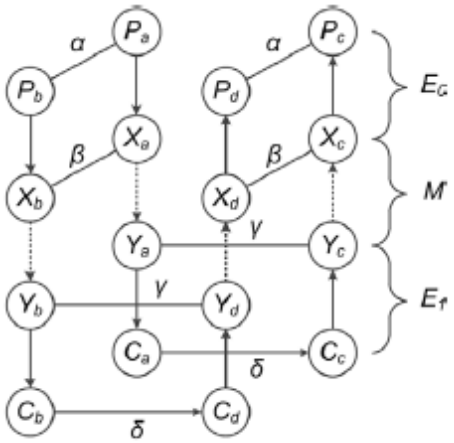


Рисунок 2.9 – Конструкція «сендвіч»

Алгоритм «сендвіч-атака» із пов’язаними ключами на алгоритм KASUMI складається з 4-х етапів.

Перший етап алгоритму – це планування пов’язаних ключів. Така процедура не займає багато часу, її можна пропустити при оцінюванні.

Другий етап алгоритму представляє собою це збір даних. При цьому вхідні дані генеруються та аналізуються. Квартети генерування та аналізування одержують при реалізації операцій шифрування й дешифрування із пов’язаними ключами. У такому випадку сасова складність – 2^{26}, тобто 2^{25} витрачається на знаходження C_b із C_a, і 2^{25} витрачається на знаходження C_d із C_c. Дані зберігаються у асоціативних структурах, що дає змогу виконати швидкий пошук.

Третій етап – це аналіз квартетів. Застосовуючи допущені значення частини ключа і правильні квартети, можна знайти інші частки вихідного ключа.

Четвертий етапавляє собою повний перебір 32 бітів ключа, а часова складність – 2^{32}.

Отже, загальна часова складність складає $2^{26} + 2^{32}$. Так як 2^{26} набагато менше ніж 2^{32}, можна твердити, що для алгоритмів криптоаналізу мають часову складність 2^{32}.

ВНТУ ФІРЕН
ТКСТБ МКР 2019

Враховувати обсяг пам’яті для вихідних даних та для оперування потрібно при оцінці вимог до пам’яті. Визначальним є обсяг пам’яті для вихідних даних, складність даних складає 226.

Тоді необхідний обсяг пам’яті становитиме 230 байт, це 226 пар відкритих текстів та шифротекстів, кожна пара займає 16 байт.

2.5 Реалізації криптоаналітичної системи

Вищенаведений алгоритм криптоаналізу реалізують використовза допомогою технологі’ MPI і OpenMP. Він орієнтований на впровадження у системах з розподіленою пам’яттю.

При виборі технології програмування основними критеріями є доступність обчислювальних засобів, а також універсальність технології програмування, що дає змогу використати розроблене алгоритмічне забезпечення на звичайних Beowulf-кластерах.

Згідно результатів проведених експериментів [12], для здійснення криптоаналізу часозатрати знижуються. При застосуванні технології OpenMP й типового набору вхідних даних, ідентифікування правильних квартетів реалізовується з ймовірністю 0,76, а при застосуванні MPI й збільшенні набору вхідних даних – із ймовірністю 0,94.

Рішення задачі показало, що для здійснення криптоаналізу алгоритму шифрування KASUMI за методом сендвіч-атака потрібен час близько 30-40хв для одного тестового набору вхідних даних. При цьому кластер опрацьовує майже 100 наборів вхідних даних.

Програмне забезпечення зорієнтовано на кластерні системи. Воно може бути ефективно впроваджено у мета-кластерних системах. Більшої ефективності можна досягнути шляхом застосування технології GPGPU, її особливістю є простота розробки і невисока вартість.

Не лише спеціалізовані плати, наприклад, nVidia Tesla GPU Modules характеризуються обчислювальними можливостями, а й звичні відеокарти nVidia,

ВІТУ ФІРЕН ТКСТБ МКР 2019

котрі можна застосовувати в якості пристроїв для обчислень. Окрім того, такі плати мають вбудовану високошвидкісну пам’ять та високошвидкісну шину для обміну даними між ядрами графічних процесорів.

Альтернативою технології GPGPU з погляду швидкодії є застосування програмованих логічних інтегральних схем (ПЛІС). Їх основною перевагою порівняно із технологією GPGPU є висока швидкодія при обробленні великих потоків даних. Окрім того, застосування ПЛІС дозволяє змінити архітектуру обчислювальної системи і залежно від поставленої задачі, що в GPGPU зробити неможливо. Але засоби GPGPU є дешевшими, ніж аналогічні ПЛІС. Якщо ж не передбачається апаратна реалізація поставленої задачі у вигляді окремого пристрою, то значно дешевшим застосування є графічних процесорів порівняно з ПЛІС.

Завдяки паралельному програмному забезпеченню можна дослідити надійність криптографічних компонентів, котрі забезпечують цілісність та конфіденційність даних, переданих при застосуванні алгоритму KASUMI. Крім того, розпаралелення обчислювальної задачі криптоаналізу дає змогу підвищити її ефективність та достовірність.

При розробленні систем криптоаналізу варто проводити порівняльний аналіз різноманітних програмно-апаратних засобів і паралельних і розподілених систем з метою виявлення найефективніших на різних етапах атаки. Такий аналіз дасть змогу розробити ефективні криптоаналітичні алгоритми для симетричних блочних шифрів.

ВНТУ ФІРЕН ТКСТБ МКР 2019

3 ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В МЕРЕЖАХ 4G

Безпека в мережах LTE реалізується у виглядц таких процедур :

- Захист абонентів.
- Захист переданих повідомлень.
- Шифрування повідомлень.
- Аутентифікація і абонента, і мережі.

Захист абонента полягає в тому, що в процесі обслуговування його приховують тимчасовими ідентифікаторами.

Для закриття даних в мережах LTE використовується потокове шифрування методом накладення на відкриту інформацію псевдовипадкової послідовності (ПВП) за допомогою оператора XOR (виключне АБО). У цих мережах для забезпечення безпеки всередині мережі застосовується принцип тунелювання з'єднань. Шифруванню можна піддавати пакети S1 і X2 за допомогою IPsec ESP, також піддаються шифруванню сигнальні повідомлення цих інтерфейсів.

3.1 Аутентифікацій в мережі

У момент підключення або активізації абонентського обладнання (UE) в мережі, мережа запускає процедуру аутентифікації і угоди про ключі AKA (Authentication and Key Agreement). Метою цієї процедури є взаємна аутентифікація абонента і мережі та вироблення проміжного ключа KASME. Робота механізму AKA займає частки секунди, які необхідні для вироблення ключа в додатку USIM і для підтримання зв'язку з центром реєстрації (HSS). Внаслідок цього, для досягнення швидкості передачі даних мереж LTE необхідно додати функцію оновлення ключової інформації без ініціалізації механізму AKA. Для вирішення цієї проблеми в мережах LTE пропонується використовувати ієрархічну ключову інфраструктуру. Тут також, як і в мережах 3G, додаток USIM та центр аутентифікації (AuC) здійснюють попередній розподіл ключів. Коли ме-

ВНТУ ФІРЕН ТКСТБ МКР 2019

ханізм AKA ініціюється для здійснення двосторонньої аутентифікації користувача і мережі, генеруються ключ шифрування CK і ключ загального захисту, які потім передаються з USIM в мобільне обладнання (ME) і з ментру аутентифікації в ментр реєстрації (HSS). ME і HSS, використовуючи ключову пару (CK; IK) і ID використовуваної мережі, виробляють ключ KASME. Встановивши залежність ключа від ID мережі, центр реєстрації гарантує можливість використання ключа тільки в рамках цієї мережі. Далі KASME передається з центру реєстрації в пристрій мобільного управління (MME) поточної мережі, де він використовується в якості майстер-ключа. На підставі KASME виробляється ключ Knas-enc, який необхідний для шифрування даних протоколу NAS між мобільним пристроєм (UE) і MME, і Knas-int, необхідний для захисту цілісності. Коли UE підключається до мережі, MME генерує ключ KeNB і передає його базовим станціям. У свою чергу, з ключа KeNB виробляється ключ Kup-enc, який використовується для шифрування даних користувача протоколу U-Plane, ключ Krrc-enc для протоколу RRC (Radio Resource Control – протокол взаємодії між мобільними пристроями і базовими станціями) і ключ Krrc-int, призначений для захисту цілісності.

Алгоритм аутентифікації і генерації ключа представлений на рис. 3.1:

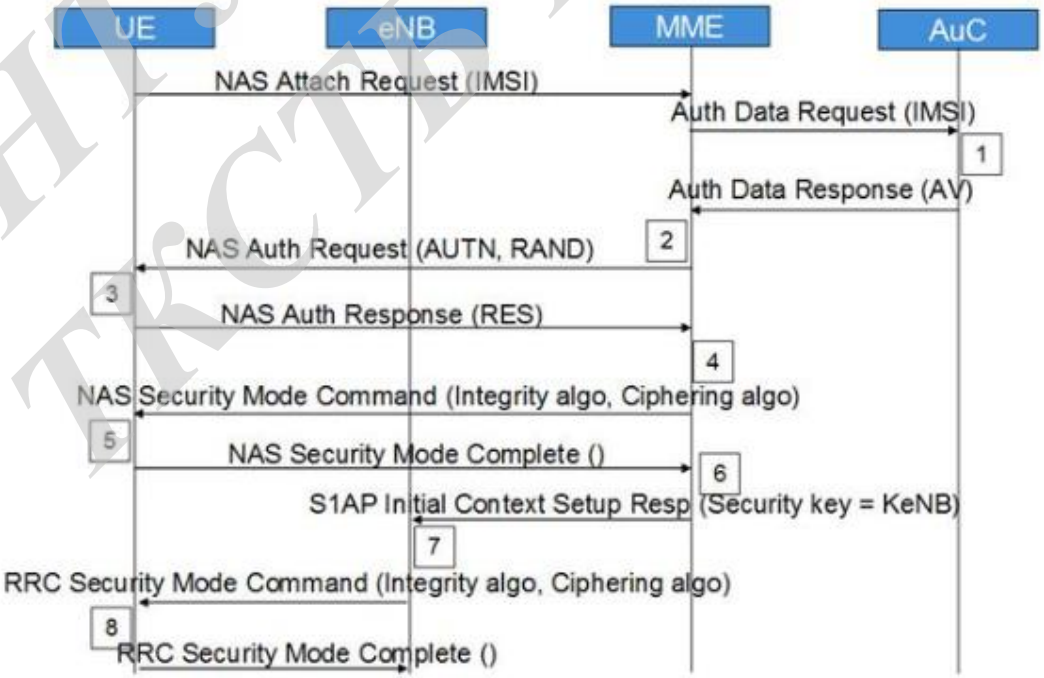


Рисунок 3.1 – Діаграма аутентифікації та генерації ключа

ВНТУ ФІРЕН ТКСТБ МКР 2019

Вказана процедура складається з таких кроків.

Крок 1. Запит про підключення до мережі від мобільної станції (UE). MME запитує аутентифікаційні дані, що відносяться до конкретного IMSI, відправляючи Authentication Data Request. AuC/HSS вибирає PSK, що відноситься до конкретного IMSI і обчислює аутентифікаційні дані по PSK. AuC/HSS відправляє назад AV с Authentication Data Response.

Крок 2. MME отримує IK, CK, XRES, RAND і AUTH з AV. MME відправляє AUTH і RAND за допомогою Authentication Request до UE.

Крок 3. UE аутентифікує NW, перевіряючи отриманий AUTH. Після чого обчислює IK, CK, RES, XMAC зі свого ключа захисту, AMF, (OP), AUTH і RAND. Вона відправляє RES з Authentication response.

Крок 4. Після отримання RES, MME порівнює його з XRES і якщо вони збігаються, то аутентифікація пройшла успішно, в іншому випадку, MME відправляє збій аутентифікації (Authentication failure) до UE. MME скидає лічильник DL NAS. Розраховує KASME, KeNB, Knas-int, Knas-enc. Відправляє NAS команду режиму безпеки (алгоритм цілісності, алгоритм шифрування, NAS набір ключів ID, функцію безпеки UE) з цілісністю не зашифрованих, використовуючи Knas-inc.

Крок 5. Після отримання NAS команди режиму безпеки, UE обчислює KASME, KeNB, Knas-int, Knas-enc. UE відправляє NAS режиму безпеки.

Крок 6. Після отримання NAS команди режиму безпеки від UE, MME відправляє KeNB в eNB з S1AP первісну установку початкового контексту (ключ захисту).

Крок 7. Після отримання KeNB, eNB обчислює Krrc-int, Krrc-enc, Kup-enc. Потім він відправляє RRC ключ захисту команду з AS цілісністю алгоритму і AS шифрує алгоритм.

Крок 8. Після отримання RRC команди ключа захисту UE обчислює Krrc-int, Krrc-enc, Kup-enc. UE відправляє RRC виконаний ключ шифрування на eNB.

ВНТУ ФІРЕН ІКСТБ МКР 2019

Після всіх описаних дій, всі NAS і AS повідомлення будуть надійно захищені і зашифровані, на відміну від призначених для користувача даних, які будуть тільки шифруватися. [2]

Архітектура безпеки LTE визначає механізм безпеки і для рівня NAS і для рівня AS (рис.3.2).

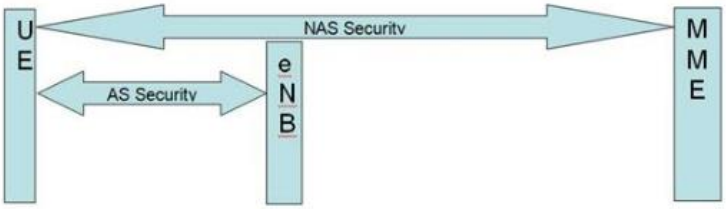


Рисунок 3.2 – Шари безпеки

Безпека NAS (Non-Access Stratum – шару без доступу) виконана для NAS повідомлень і належить області UE і MME.

У цьому випадку необхідною при передачі повідомлень NAS між UE і MME є цілісність, захищена і зашифрована з додатковим заголовком безпеки NAS.

Безпека AS (Access Stratum – шару з доступом) Виконана для RRC і площини призначених для користувача даних, що належать області UE і eNB. Рівень PDCP на сторонах UE і eNB відповідає за шифрування і захист цілісності.

RRC повідомлення захищені цілісністю і зашифровані, проте дані U-Plane тільки зашифровані.

3.2 Генерація векторів аутентифікації

Для генерації векторів аутентифікації використовується криптографічний алгоритм з допомогою односпрямованих функцій (f1, f2, f3, f4, f5), коли прямий результат одержується шляхом простих обчислень, а зворотний результат не може бути отриманий зворотним шляхом, тобто не існує ефективного алгоритму отримання зворотного результату. Для цього алгоритму використовується випадкове 128-бітове випадкове число RAND, майстер-ключ K абонента, також 128 біт і порядковий номер процедури SQN (Sequence Number). Лічильник SQN

ВНТУ ФІРЕН ТКСТБ МКР 2019

змінює своє значення при кожній генерації вектора аутентифікації. Схожий лічильник SQN працює і в USIM. Такий метод дозволяє генерувати кожен раз новий вектор аутентифікації, не повторюючи попередній вже використаний вектор аутентифікації.

Крім цих трьох вихідних величин: SQN, RAND і K в алгоритмі f1 бере участь поле управління аутентифікацією Authentication Management Field (AMF), а в алгоритмах f2-f5 вихідні параметри – RAND і K, що і продемонстровано на рис. 3.3, 3.4. На виходах відповідних функцій отримують Message Authentication Code (MAC) – 64 біта; XRES – eXpected Response, результат роботи алгоритму аутентифікації <32 - 128 біт>; ключ шифрування CK, що генерується з використанням вхідних (K, RAND) -> f3-> CK; ключ цілісності IK, згенерований з використанням вхідних (K, RAND) -> f4-> IK; і проміжний ключ Anonymity Key (AK), що генерується за допомогою (K, RAND) -> f5-> AK – 64 біта.

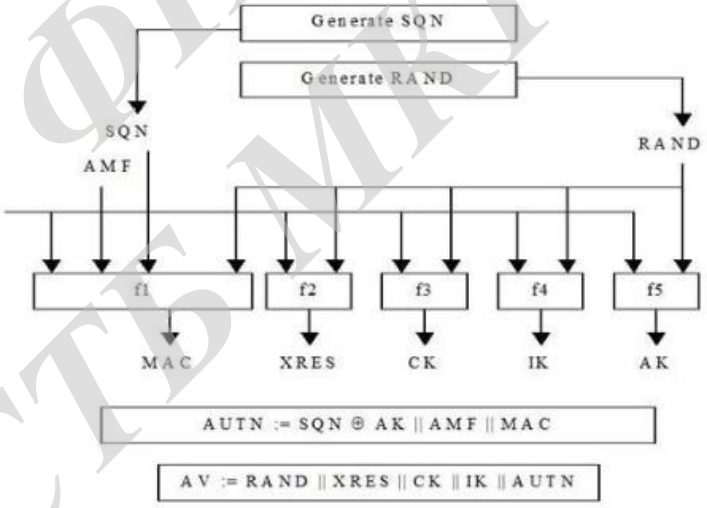


Рисунок 3.3 – Створення векторів на передавальній стороні

При обслуговуванні абонента мережею LTE ключі CK і IK в відкритому вигляді в ядрі мережі залишають поза передачею. В цьому випадку HSS генерує KASME за допомогою алгоритму KDF (Key Derivation Function), для якого вихідними параметрами є CK і IK, а також ідентифікатор обслуговуючої мережі і SQNAAK. Вектор аутентифікації містить RAND, XRES, AUTN і KASME, на

ВНТУ ФІРЕН ТКСТБМКР 2019

основі якого відбувається генерація ключів шифрування і цілісності, які використовуються у відповідному алгоритмах.

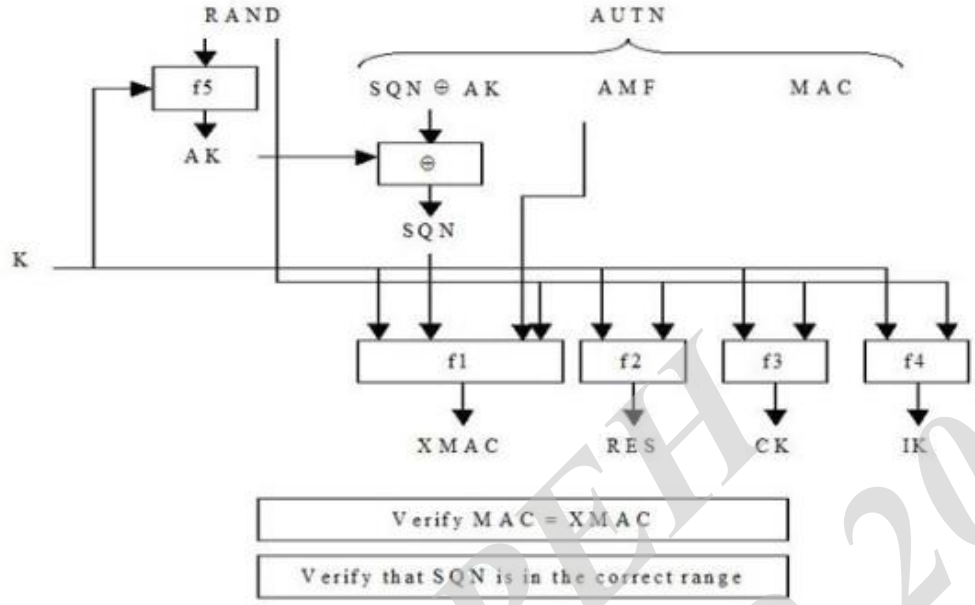


Рисунок 3.4 – Перетворення векторів на приймальній стороні

Мобільна станція отримує з ядра мережі три параметра (RAND, AUTN і KSIASME, де KSI – Key Set Identifier, індикатор встановленого ключа, однозначно пов’язаний з KASME в мобільної станції). Після чого використовуючи RAND і AUTN, USIM на основі алгоритмів безпеки, що зберігаються і в HSS, здійснює обчислення XMAC, RES, CK і IK.

Потім у відповіді RES UE передає в MME обчислене RES, яке має збігтися з XRES, отриманим з HSS. Так мережа аутентифікує абонента. Обчисливши XMAC, UE порівнює його з MAC, отриманим нею в AUTN. При успішній аутентифікації абонентом мережі (MAC = XMAC) UE повідомляє про це у відповіді RES. Якщо аутентифікація мережі не вдалася (MAC ≠ XMAC), то UE направляє в MME відповідь CAUSE, де вказує причину невдачі аутентифікації.

При успішному завершенні попереднього етапу MME, eNB і UE здійснюють генерацію ключів, використовуваних для шифрування і перевірки цілісності одержуваних повідомлень. У LTE є ієрархія ключів, яка приведена на рис.3.5.

ВНТУ ФІРЕНТ ТКСТБ МКР 2019

Вектори аутентифікації є такими:

- Ключі IK і CK генеруються і в центрі аутентифікації, і в USIM;
- Ключ AK генерується тільки в центрі аутентифікації;
- Відповідь XRES генерується тільки в центрі аутентифікації, а RES генерується в USIM;
- Код MAC генерується тільки в центрі аутентифікації, а відповідний йому параметр XMAC генерується в USIM;
- Маркер AUTH генерується тільки в центрі аутентифікації.

Вихідним ключем для всієї ланки є KASME (256 біт). При передачі в радіоканалі захист забезпечують для сигнального трафіку (Control Plane) і для призначених для користувача пакетів (User Plane). При цьому всі повідомлення сигналізації поділяють на наскрізні сигнальні повідомлення між UE і MME протоколів MM і SM (NAS – Non Access Stratum) і сигнальні повідомлення між eNB протоколу RRC (AS – Access Stratum).

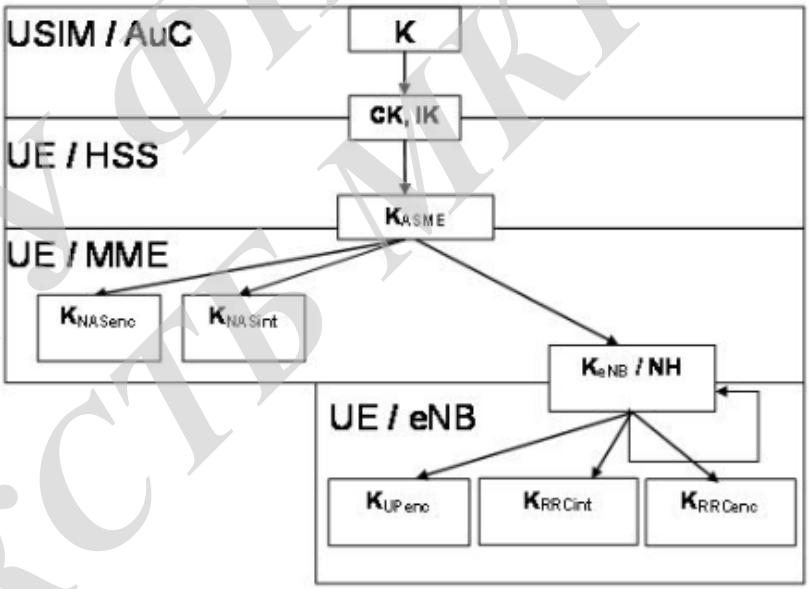


Рисунок 3.5 – Ієрархія ключів

Для шифрування і захисту цілісності можна використовувати різні базові алгоритми: UEA2 (UMTS Encryption Algorithm 2) і UIA2 (UMTS Integrity Algorithm 2); розроблені для стандартів 3G, AES (Advanced Encryption Standard).

ВНТУ ФІРЕН ТКСТБ МКР 2019

3.3 Захист повідомлень протоколу RRC

Сигнальні повідомлення протоколу RRC (AS) також шифрують і забезпечують їх цілісність. Пакети трафіку тільки шифрують. Ці операції проводять в обслуговуючій eNB і UE. Схема отримання ключів шифрування і цілісності для AS і UP трафіку відрізняється від попереднього випадку тим, що вихідним параметром тут служить вторинний проміжний ключ KeNB (256 біт). Цей ключ генерують, також використовуючи KDF, де вхідними параметрами є: KASME, лічильник сигнальних повідомлень NAS вгору, колишнє значення KeNB, ідентифікатор стільники і номер частотного каналу в напрямку вгору. Отже, за будь-якої періодичної локалізації UE відбувається зміна KeNB.

Також KeNB змінюється і при хендовері; при цьому в алгоритмі генерації нового KeNB можна використовувати додатковий параметр NH (Next Hop), фактично лічильник числа базових станцій, по ланці обслуговуючих абонента. Алгоритм шифрування і дешифрування повідомлень представлений на рис. 3.6.

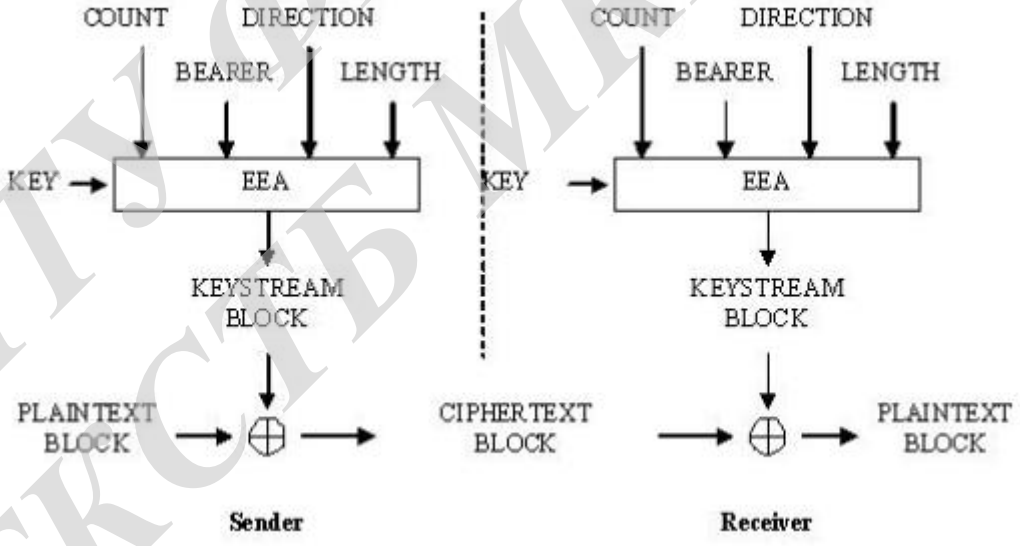


Рисунок 3.6 – Алгоритм шифрування

Вихідними параметрами в цьому алгоритмі є шифрує ключ KEY (128 біт), лічильник пакетів (блоків) COUNT (32 біта), ідентифікатор наскрізного каналу BEARER (5 біт), покажчик напрямку передачі DIRECTION (1 біт) і довжина шифрувального ключа LENGTH. Відповідно до обраного алгоритму шифрування EEA (EPS Encryption Algorithm) виробляється шифрувальне число

ВНТУ ФІРЕН ТКСТБ МКР 2019

KEYSTREAM BLOCK, яке при передачі складають по модулю два з зашифрованих вихідним текстом блоку PLAINTEXT BLOCK. При дешифрування на приймальному кінці повторно роблять цю ж операцію.

Процедура захисту цілісності повідомлення складається в генерації "хвоста" MAC (Message Authentication Code) (32 біта), що приєднується до переданого пакету. Алгоритм генерації MAC і перевірки цілісності отриманого пакета шляхом порівняння XMAC з MAC відображено на рис. 3.7.

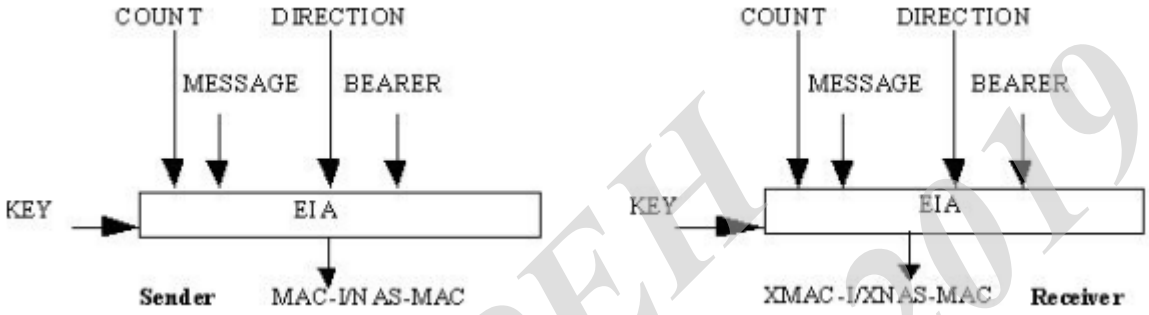


Рисунок 3.7 – Алгоритмперевірки цілісності

В алгоритмі EIA (EPS Integrity Algorithm) використано ключ цілісності KEY (128 біт), лічильник повідомлень COUNT (32 біта), ідентифікатор наскрізного каналу BEARER (5 біт), покажчик напрямку передачі DIRECTION (1 біт) і саме повідомлення MESSAGE.

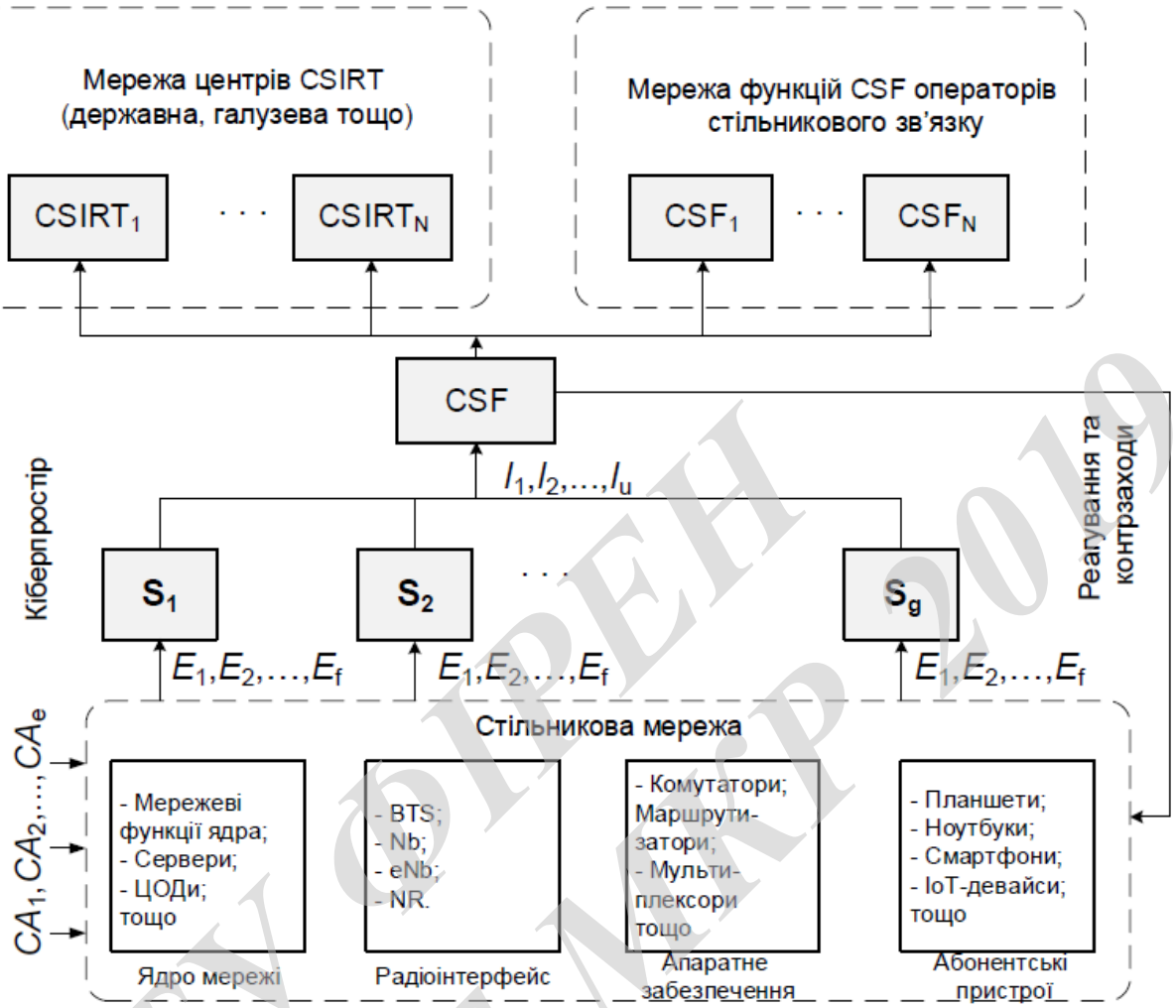
3.4 Моніторинг загроз

Наразі є єдиний центр для абонентів національних інформаційних систем та сегмента Інтернет мережі для реагування на комп'ютерні кіберінциденти CERT (Computer Emergency Response Team). Вказана служба відповідає за збір і аналіз інформації про комп’ютерні інциденти, надає консультативну та технічну підтримку абонентам по запобіганню загроз безпеки.

Ці функції CERT варто перенести в область мереж мобільного зв’язку, що дасть змогу операторам не лише підвищити рівень кібербезпеки та зменшити збитки від вчинених кіберзлочинів, а й впровадити додаткові сервіси забез-

ВНТУ ФІРЕН ТКСТБ МКР 2019

печення безпеки. Схема реалізації моніторингу кіберінцедентами в стільниковій мережі подана на рис. 3.8.



Рсунок 3.7 – Схема моніторингу кіберінцедентів в стільниковій мережі

3.5 Використання генератора псевдовипадкової послідовності

З метою протидії злочинам потрібно коректно обирати заходи і засоби забезпечення захисту інформації в телекомунікаційних мережах. Зокрема, широкого поширення набули криптографічні засоби, складовою частиною яких, є генератори псевдовипадкової бітової послідовності. Вони застосовуються для генерації ключів, у потокових шифрах, для формування цифрового підпису. Також генератори псевдовипадкової бітової послідовності широко застосовуються у сфері захисту інформації для придушення електромагнітного ви-

ВНТУ ФІРЕН ТКСТБ МКР 2019

промінювання, для зашумлення приміщень, при проектуванні генераторів шуму, скремблерів. Окрім того, вони є складовими елементами захисту у мобільному зв'язку. Відомо багато способів формування псевдовипадкової послідовності, розроблено багтао генераторів із різними характеристиками, головними з яких є: статистичні характеристики, криптостійкість, швидкодія, технологічність апаратної реалізації. Підвищитирівень криптостійкості генератора псевдовипадкової послідовності можна, використавши за основу модифікований адитивний генератор Фібоначчі. У роботі [5] розглядалися модифіковані адитивні генератори Фібоначчі та варіанти покращення їх статистичних характеристик. Такі генератори не є криптостійкими, так як окрім початкових установок регістрів не мають інших засобів для її забезпечення. Підвищити криптографічну стійкість модифікованого адитивного генератора Фібоначчі можна ускладнивши схему його побудови та доповнивши її додатковими елементами. На рис. 3.8 представлена структурна схема генератора псевдовипадкової бітової послідовності на основі модифікованого адитивного генератора Фібоначчі з підвищеною крипостійкістю.

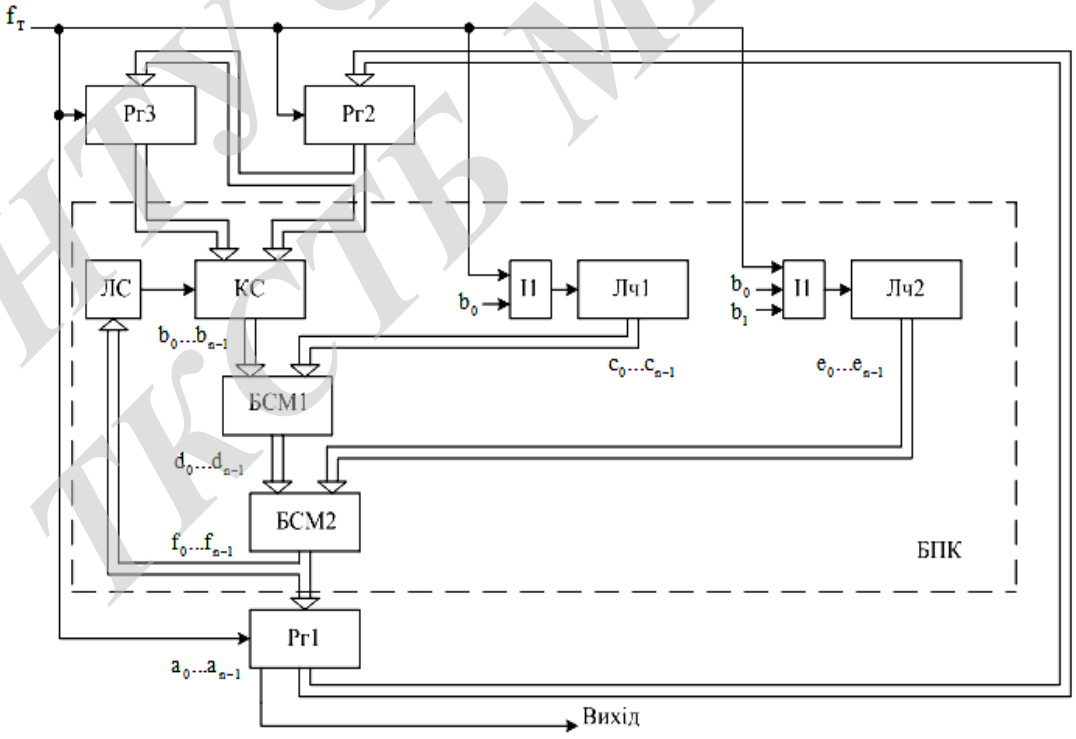


Рисунок 3.4 – Структурна схема генератора псевдовипадкової бітової послідовності на основі модифікованого адитивного генератора Фібоначчі

ВНТУ ФІРЕН ТКСТБ МКР 2019

4 СИСТЕМА ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА НА БАЗІ НЕЙРОННОЇ МЕРЕЖІ

4.1 Структура системи ідентифікації

В пропонованій системі як хеш-значення застосовано вектор вагових коефіцієнтів нейронної мережі. Для його збереження та відтворення використовуються блоки, подані на рис.4.1.

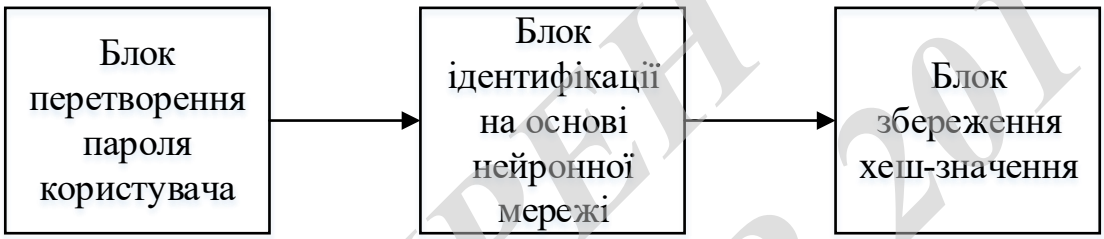


Рисунок 4.1 – Струкутра системи ідентифікації користувача

Блок перетворення пароля формує вхідні дані для штучної нейронної мережі. Однією із головних умов побудови працездатної нейронної мережі є правильно обрана навчальна вибірка. Навчальною вибіркою називають множину $\{P_n\}$, елементи якої представляють собою пари вхідних і вихідних векторів $P_i = (X_i, Y_i)$, одержаних із початкових даних. У даному випадку початковими даними для навчальної вибірки є пароль S^0, який задає користувач. Для того, щоб одержати навчальну вибірку застосовуємо алгоритм перетворення двійкової послідовності у множину навчальних прикладів. Алгоритм має відповідати таким вимогам:

1) Створена множина $\{P_n^i\}$ має бути унікальною для будь-якого вхідного пароля S^i, що можна подати у вигляді умови:

$$\{P_n^i\} \neq \{P_n^j\} \text{ при } S^i \neq S^j, i \neq j, S^i, S^j \in \{S^k\}.$$

ВІТУ ФІРЕН ТКСТЬ МКР 2019

2) Однакові елементи P_i повинні бути відсутні, також не повинно бути елементів із однаковими складовими, тобто всі елементи навчальної вибірки повинні відповідати умовам функціональності.

Алгоритм А1 відповідає вищезазначеним вимогам та забезпечує перетворення двійкової послідовності $\{U_m\}$ у множину дійсних чисел $\{P_n\}$:

1) Створюємо розширену двійкову послідовність $\{U_m^*\}$ додавання N-1 перших біт у послідовність $\{U_m\}$. Тут N – довжина пароля.

2) З метою побудови послідовності дійсних чисел $\{V_m\}$ використаємо метод, який полягає у застосуванні вікна розміром 16 біт, котре може пересуватися вздовж розширеної двійкової послідовності із певним кроком. Біти, що знаходяться всередині вікна, подаються як N-розрядне двійкове число a_i, де i – це поточна позиція вікна. I-й елемент послідовності дійсних чисел $\{V_m\}$ визначається так:

$$v_i = \frac{a_i}{2^N - 1},$$

де $i = 0,...,m-1$.

3) З послідовності $\{V_m\}$ одержуються N вхідних векторів, що позначаються X* .

4) Вихідні значення Y_j^* можна знайти за виразом:

$$Y_j^* = \frac{\sum_{i=0}^{j} b_i}{\sum_{k=0}^{N-1} c_k},$$

де $j = 0,...,N-1,$

ВНТУ ФІРЕН ТКСТБ МКР 2019

b_i – це вікно розміру N, що пересувається по двійковій послідовності із кроком N-1;

c_k – це вікно розміру N, що пересувається по двійковій послідовності із кроком N.

Блок ідентифікації, побудований на базі штучної нейронної мережі прямого поширення (рис.4.2), є основним елементом системи.

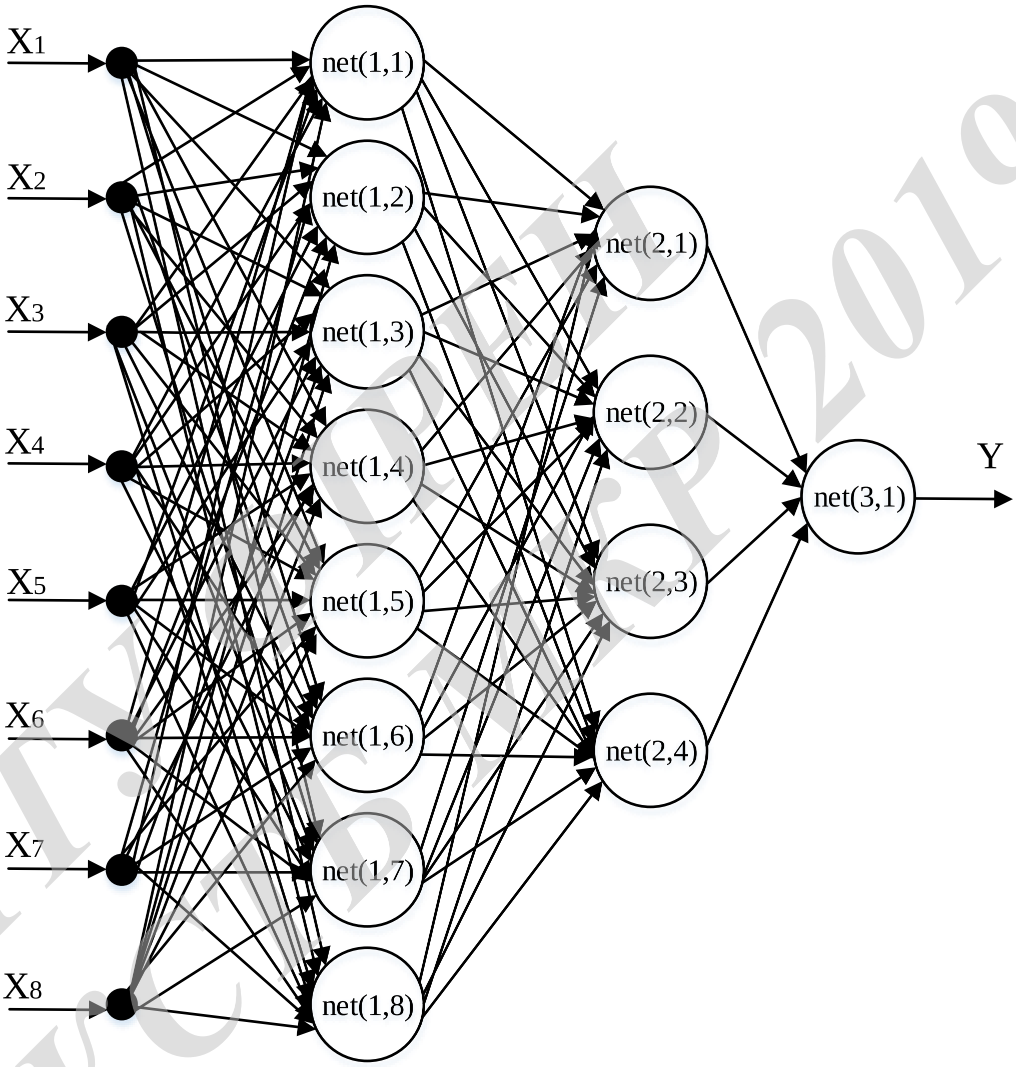


Рисунок 4.2 – Структура нейронної мережі

Нейронна мережа є тришаровою, нейрони в ній утворюють пірамідальну структуру. Вихідний шар нейронної мережі складається із одного нейрона. Число нейронів вхідного шару дорівнює числу бітів, котрі визначають одну літеру пароля. Подана нейронна мережа здатна забезпечити мінімум 100 змінних параметрів. Будемо вважати, що така розмірність хеш-значень є достатньою.

ВНТУ ЛРНІ ТКСТБ МКР 2019

У процесі функціонування штучної нейронної мережі вхідний вектор X перетворюється у вихідний вектор Y. Для нейронної мережі, яка складається з M-шарів, вихідний вектор описується рівнянням [5]:

$$Y = \psi^{(M)}(\omega_0^{(M)} + W^{(M)}\psi^{(M-1)}(\omega_0^{(M-1)} + W^{(M-1)}\psi^{(M-2)} \times$$
$$\times(...(\omega_0^{(2)} + W^{(2)}\psi^{(1)}(\omega_0^{(1)} + W^{(1)}X))...))),$$

де $\omega_0^{(M)}$ – вектор порогових вагових коефіцієнтів,

$W^{(M)}$ – матриця вагових коефіцієнтів,

$\psi^{(M)}$ – оператор, що перетворює вхідний вектор відповідно до функції активації нейрона.

Штучна нейронна мережа реалізує функцію вектору X, котра залежить від вектору вагових коефіцієнтів W. Для знаходження вектору вагових коефіцієнтів застосовують алгоритми навчання, що представляють собою процес знаходження значень вагових коефіцієнтів при яких нейронна мережа відповідає навчальній вибірці з похибкою ξ, що виражає міру наближення отриманих вихідних значень до бажаних [5]. Як алгоритм навчання можна застосовувати детерміновані ітераційні алгоритми, що забезпечують потрібну швидкість роботи системи.

З метою підвищення надійності роботи системи ідентифікації застосовується алгоритм перемішування вагових коефіцієнтів на базі генератора випадкових чисел. Генератор ініціюється значенням на основі пароля, що дозволяє забезпечити для різних паролей унікальні перестановки.

4.2 Аналіз стійкості системи

Хеш-функції визначає надійність системи ідентифікації. В той же час, якість хеш-функції визначається стійкістю до можливих криптографічних атак,

ВНТУ ФІРЕН ТКСТБ МКР 2019

які здійснюються із метою розкриття пароля, якщо хеш-значення є відомим. Найбільш ефективними видами атак є такі:

1) Атака на однобічність, що представляє собою знаходження вхідного значення x за значеннями h(x) і h;
2) Атака на колізії, тобто знаходження значення x' так, що h(x')=h(x).

Атаки на однобічність можуть буди прямими або непрямими [2]. При прямій атаці визначається обернена залежність або знаходиться алгоритм одержання невідомого вхідного значення. Але пряма атака може бути успішною лише у деяких випадках, в той час як непряма атака часто є успішною. Вона представляє собою огляд деякої множини вхідних значень, які обираються або випадковим чином або за певним алгоритмом, та порівняння значень хеш-функції, обчислених для кожного елементу, із шуканими.

Хеш-значення – це невпорядкований вектор вагових коефіцієнтів. Він одержується після процесу навчання нейронної мережі за допомогою навчальної вибірки. Тобто, потрібно розв’язати дві задачі за допомогою прямої атаки на однобічність:

1) Відновити вірне розташування вагових коефіцієнтів;
2) Визначити входи мережі, задіяні при навчанні.

Для розв’язання першої задачі потрібно переглянути множину усіх можливих векторів вагових коефіцієнтів. Зменшити цю множину можна, застосовуючи правила:

1) Значення вагових коефіцієнтів наступних шарів, як правило вище за відповідні значення попередніх шарів.
2) Для одного нейронна сума значень вагових коефіцієнтів прямує до нуля.

Для перевірки достовірності вектору вагових коефіцієнтів потрібно розв’язати другу задачу, яка полягає у наступному:

1) Для всіх вхідних значень X_i потрібно визначити відповідні вихідні значення Y_i.

ВНТУ ФІРЕН ТКСТБ МКР 2019

2) Визначити елементи одержаної множини, які могли застосовуватися при навчанні, враховуючи особливості алгоритму.

Не зважаючи на простоту реалізації, пряма атака дуже рідко завершується успішно, так як у загальному випадку для кожного елементу множини векторів вагових коефіцієнтів потрібно виконати перегляд множини вхідних значень, що має розмірність 2^{8N}.

Непряма атака на однобічність побудованої на основі нейронної мережі хеш-функції ускладняється через те, що розрахунок хеш-значення вимагає багато часу. Атака на колізії також вимагає великої кількості обчислень хеш-значень, а також пам'яті великого обсягу для зберігання усіх отриманих значень.

Наступні особливості на основі нейронної мережі хеш-функції, які чинять суттєвий вплив на стійкість мережі до криптографічної атаки:

1) Розмірність хеш-значення набагато більша за розмірність пароля.
2) Хеш-значення мають високу варіативність.
3) Немає кореляції між отриманим хеш-значенням та паролем.

Навчання штучної нейронної мережі є тривалим ітераційним процесом, протягом якого можлива непередбачувана зміна вагових коефіцієнтів. Так зміна одного біта пароля може привести до одержання різних вагових коефіцієнтів, що зменшує ймовірність виникнення колізії.

ВНТУ ФІРЕН ТКСТБ МКР 2019

5 ДОСЛІДЖЕННЯ ВПЛИВУ ЗАВАД

Детальний аналіз пропускної здатності каналу зв'язку за умовах впливу флуктуаційного шуму та навмисних завад від одної станції було виконано у роботах [8-10]. Постає задача аналізу пропускної здатності каналів систем мобільного зв'язку із технологією MIMO-OFDM в умовах впливу флуктуаційного шуму і навмисних завад.

Взагалі, технологія MIMO подібна принципу рознесеного прийому, тобто коли у системі зв'язку створюються кілька некорельованих копій сигналу на приймальній стороні. У таких системах реалізується просторове мультиплексування: потік даних на перевальній стороні розбивається на два чи більше потоків, які передаються одночасно за допомогою різних антен. Технологія MIMO поєднує просторово-часові методи прийому із використанням адаптивних антен та методи просторово-часового кодування і просторово-часового рознесення сигналів [12, 33].

Розглянемо систему MIMO M×L, подану на рис.5.1, де ППД – це перетворювач потоку даних, $Пд_i$ – це передавач і-ого каналу, $Пр_i$ – це приймач і-ого каналу.

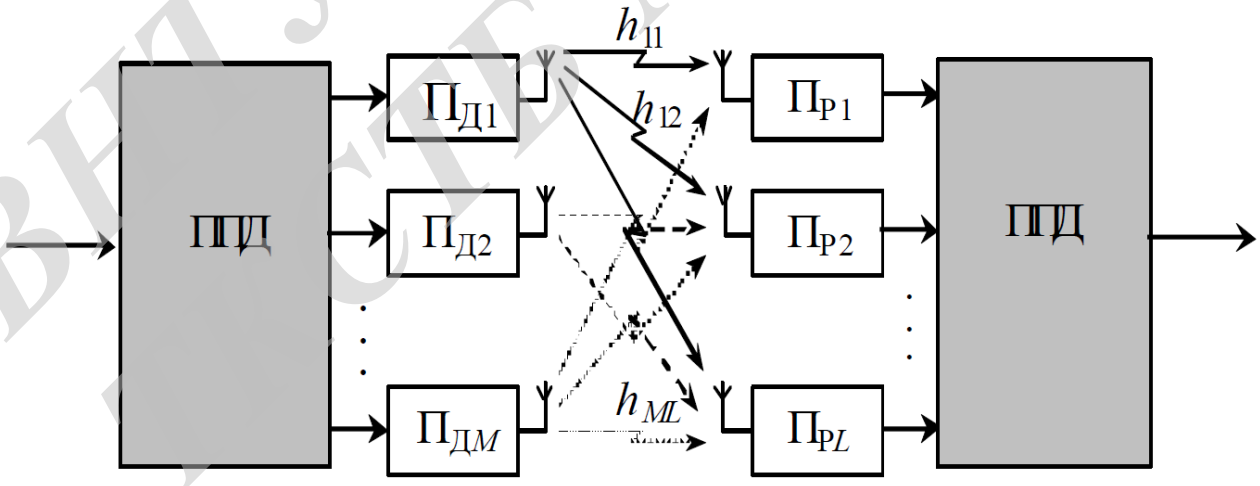


Рисунок 5.1 – Структурна схема системи MIMO

ВНТУ ФІРЕН
КСТБ МКР 2019

Спочатку високошвидкісний потік даних розділяється на M окремих послідовностей, які мають швидкості 1/M , а потім передаються одночасно із кількох антен, при цьому використовуючи тільки 1/M їх смуги частот.

На передавальному кінці лінії зв'язку перетворювач потоку даних перетворює послідовний потік даних у паралельний, а на приймальному кінці здійснюється зворотне перетворення.

На рис. 5.2 подано структурну схему формування сигналів OFDM-системи MIMO, вплив флуктуаційного шуму, навмисних завад на кожен канал, а також демодуляція сигналів у кожному каналі. Дискретно-неперервний канал виділений пунктирною лінією.

Субканал модулятора сигналів подано на рис. 5.3. Субканал демодулятора сигналів подано на рис. 5.4.

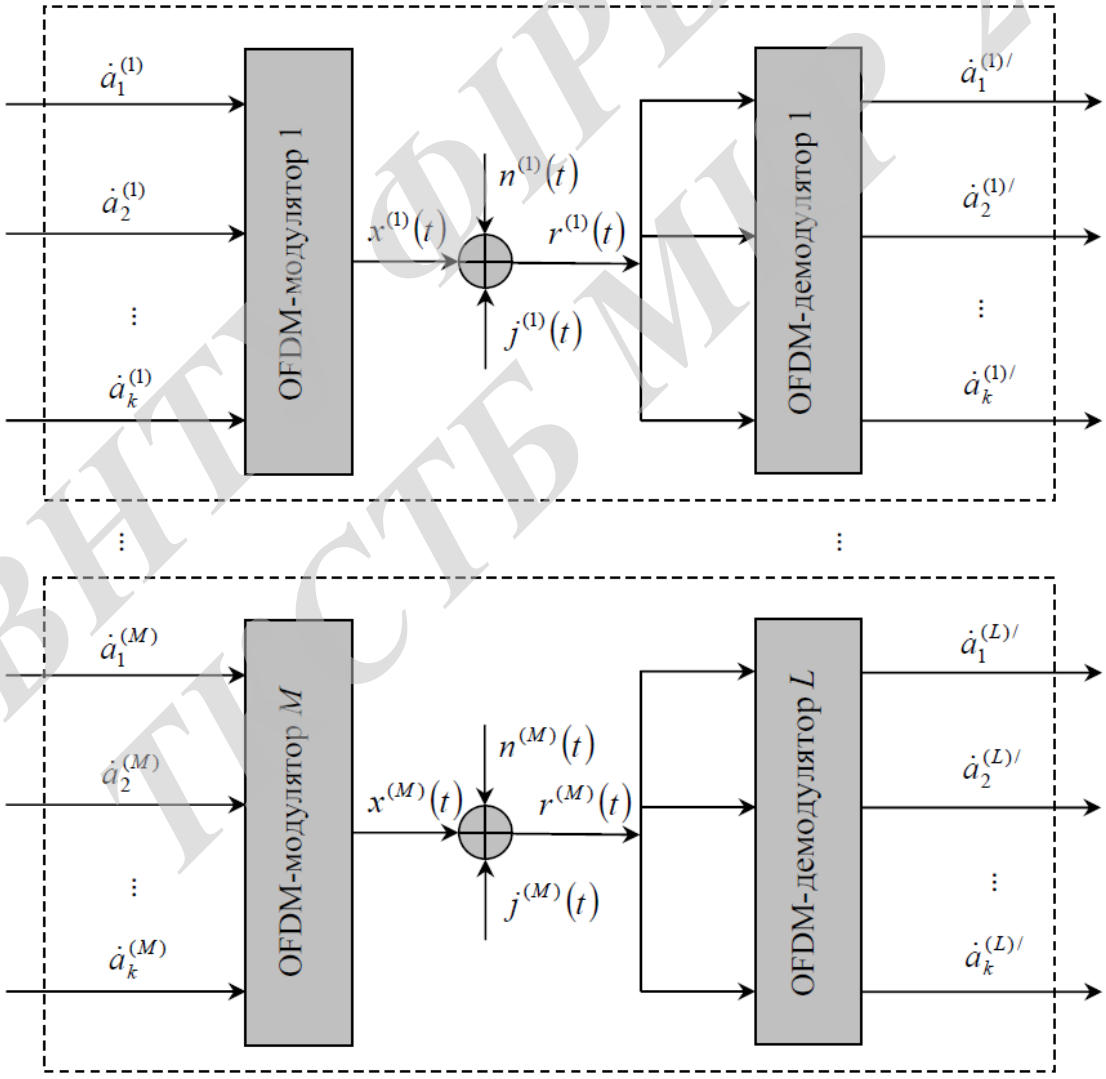


Рисунок 5.2 – Структурна схема дискретно-неперервного каналу

ВНТУ ФІРЕН ТКСТБ МКР 2019

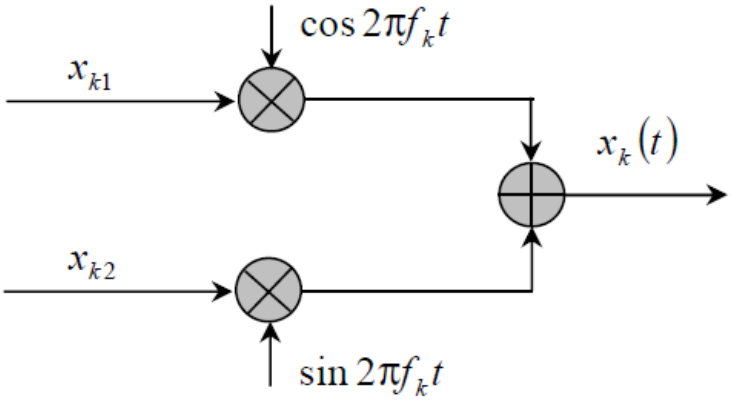


Рисунок 5.3 – Субканал модулятора

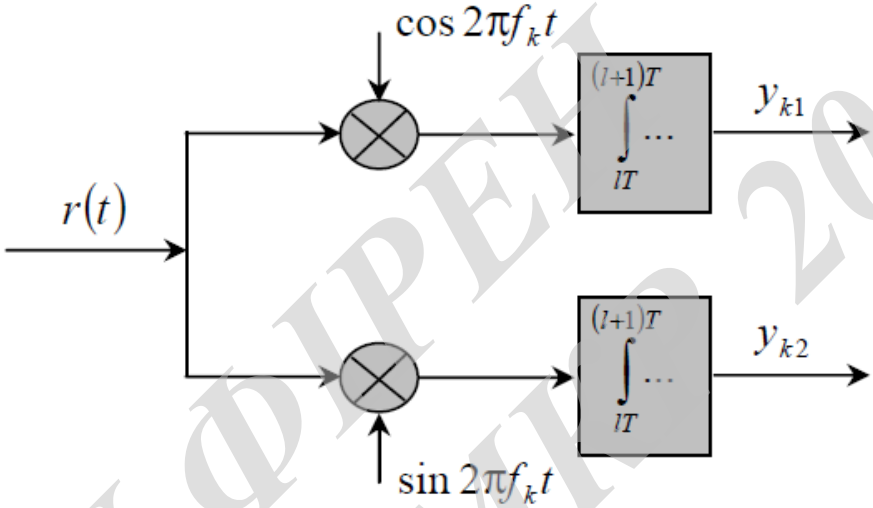


Рисунок 5.4 – Субканал демодулятора

Тепер розглянемо g-й канал MIMO.

Набір сигналів $\{x_k(t)\}$, $k=\overline{1,N}$ можна виразити як лінійну комбінацією N ортогональних сигналів $\psi_{k1}(t),\psi_{k2}(t),...,\psi_{kN}(t)$ [12]:

$$x_k(t)=\sum_{n=1}^{N} x_{kn}\psi_{kn}(t),$$

де x_{kn} – це коефіцієнти при $\psi_{kn}(t)$ розкладу сигналів по базисних функціях.

На вхід модулятора сигналів надходять M-рівневі відліки синфазної та квадратурної складових сигналів. Оскільки в каналі зв'язку виконується додавання до синфазної і квадратурної складових сигналів випадкових синфазних та

ВНТУ ФІРЕН ТКСТБ МІКС 2019

квадратурних складових завади та шуму, які розподілені за Гаусовим законом, сигнали на виході субканалів демодулятора є випадковими величинами, розподіленими за Гаусовим законом.

Замінимо *g*-й дискретно-неперервний канал, векторною моделлю (рис. 5.5).

Проаналізуємо пропускну здатність цього каналу при умові впливу флуктуаційного шуму разом з так званою шумовою загороджувальною завадою, а також шумовою завадою в частині смуги і завадою у відповідь [13].

Спочатку розглянемо k-й субканал OFDM.

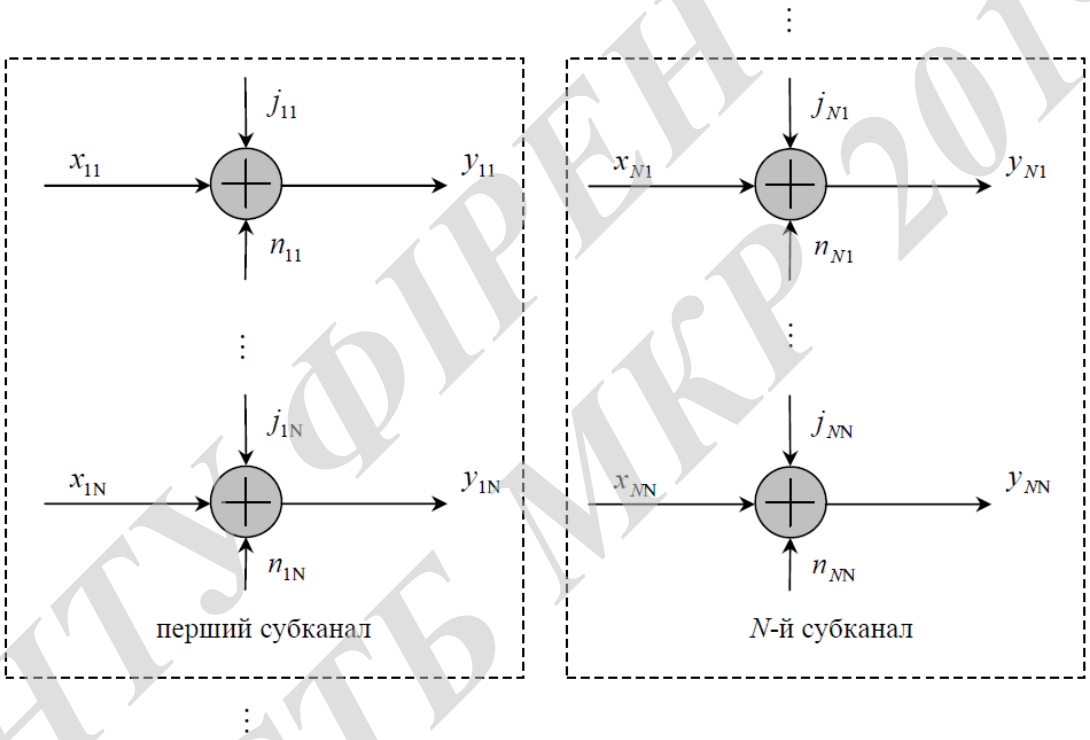


Рисунок 5.5 – Структурна схема спрощеної моделі
g-го дискретно-неперервного каналу

Коефіцієнти шумового процесу $\{n_{kn}\}$, $k=\overline{1,N}$, $n=\overline{1,N}$ – гаусові випадкові величинами з нульовим математичним сподіванням і дисперсіями $G_{k0}/2$.

Функції густини розподілу ймовірності для кожного коефіцієнта обчислюються так [12]

ВНТУ ФІРЕН ТКСТБ МКР 2019

$$w_k(n_{kn}) = \xi\left(0, \frac{G_{k0}}{2}\right) = \frac{1}{\sqrt{\pi G_{k0}}} \exp\left(-\frac{(n_{kn})^2}{G_{k0}}\right).$$

Коефіцієнти процесу навмисної завади $\{j_{kn}\}$, $k = \overline{1,N}$, $n = \overline{1,N}$ також представляють собою гаусівські випадкові величини із нульовим математичним сподіванням і дисперсіями $G_{kj}/2$.

Для навмисних завад функції густини розподілу ймовірності для кожного коефіцієнта визначаються так

$$w_k(n_{kn}) = \xi\left(0, \frac{G_{k0}}{2}\right) = \frac{1}{\sqrt{\pi G_{k0}}} \exp\left(-\frac{(n_{kn})^2}{G_{k0}}\right).$$

Пропускна здатність k-го дискретно-неперервного субканалу, обчислена на один вхідний символ, визначається максимумом кількості інформації, що була передана по каналу, по всіма можливими розподілами вхідного сигналу x_m:

$$C_k = \max J_k(x_{km}, y_k).$$

Пропускна здатність g-го каналу для системи MIMO розраховується так

$$C_g = \sum_{k=1}^{N} C_k .$$

Пропускна здатність каналу зв'язку системи з технологією MIMO-OFDM розраховується так

$$C = \sum_{g=1}^{L} \sum_{k=1}^{N} C_k .$$

ВНТУ ФІРЕН ТКСТБ МКР 2019

У якості прикладу розглянемо радіостанцію із OFDM-сигналами та систему MIMO 2×2, на яку надсилаються завади від трьох станцій. Перша станція випромінює шумову загороджувальну заваду та чинить вплив на смугу частот OFDM- сигналу, котра відповідає субканалам з 1 по 10 першого каналу системи MIMO. Друга станція випромінює шумову заваду в частині смуги з коефіцієнтом 0,7 та чинить впливає на смугу частот OFDM-сигналу, котра відповідає субканалам з 1 по 6 другого каналу. Третя станція завад випромінює шумову заваду в частині смуги з коефіцієнтом 0,8 та чинить вплив на смугу частот OFDM сигналу, котра відповідає з 10 по 16 субканалам другого каналу.

З першого по шістнадцятий субканал першого каналу системи MIMO застосовується модуляція типу ФМ-4. З першого по дев'ятий субканал другого каналу системи MIMO застосовується модуляція типу ФМ-2, а з десятого по шістнадцятий – ФМ-8. Залежність пропускної здатності системи MIMO-OFDM від співвідношення сигнал-шум в каналі показана на рис. 5.6

Перша крива відповідає випадку впливу навмисних завад і флуктуаційного шуму на систему із MIMO 2×2 та сигналами OFDM-16. А Друга характеристика відповідає впливу тільки флуктуаційного шуму на систему MIMO 2×2 з сигналом OFDM. Третя залежність відображає вплив флуктуаційного шуму на систему MIMO 2×2 з сигналами ФМ-2.

Нехай на станцію, яка використовує OFDM сигнали та систему MIMO 2×2, чинять впливають три станції завад. У такому випадку пропускну здатність системи можна підвищити, якщо збільшити кількість каналів системи MIMO. Обираємо систему MIMO 4×4 та приймаємо, що навмисні завади не впливають на третій та четвертий канали системи MIMO 4×4. З першого по шістнадцятий субканал третього каналу MIMO 4×4 застосовується модуляція ФМ-4, а з першого по шістнадцятий субканал четвертого каналу MIMO 4×4 застосовується модуляція ФМ-8. Відповідна залежність пропускної здатності системи MIMO-OFDM від співвідношення сигнал/шум в каналі показана на рис. 5.7.

ВНТУ ФІРЕН ТКСТБ МКР 2019

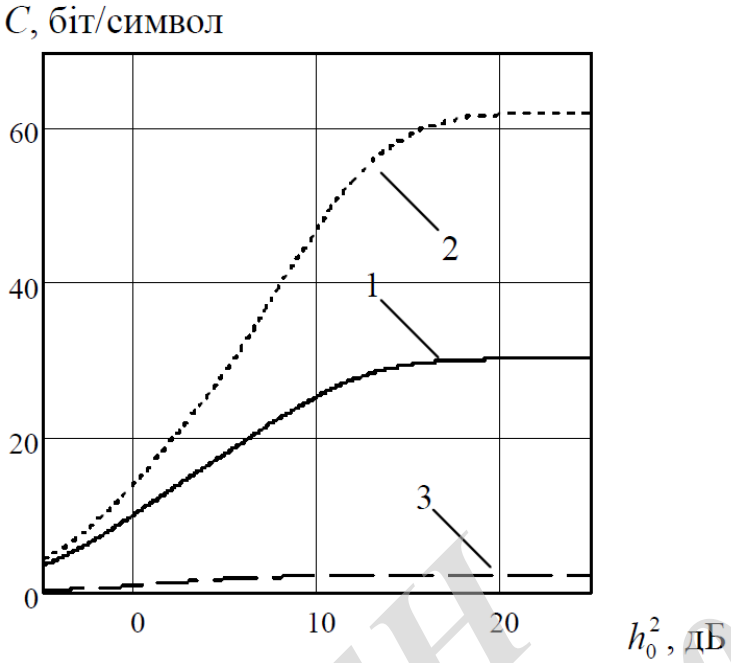


Рисунок 5.6 – Залежність пропускної здатності каналу від співвідношення сигнал/шум при впливі шумової завади в частині смуги та шуму на систему MIMO-OFDM (крива 1), при впливі лише шуму на систему MIMO-OFDM (крива2) та на систему MIMO із сигналами ФМ-2 (крива 3)

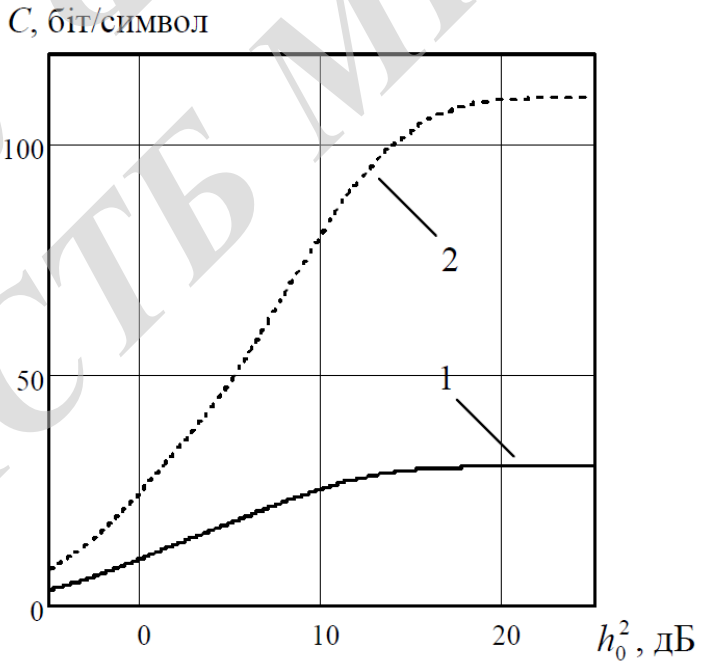


Рисунок 5.7 – Залежність пропускної здатності каналу від співвідношення сигнал/шум при впливі шумової завади в частині смуги та шуму на систему OFDM -MIMO 2×2 (крива1) та OFDM MIMO 4×4 (крива 2)

ВНТУ ФРЕН ТКСТБ МКР 2019

6 ЕКОНОМІЧНА ЧАСТИНА

6.1 Аналіз комерційного потенціалу досліджень з підвищення інформаційної безпеки систем мобільного зв'язку

6.1.1 Визначення рівня комерційного потенціалу досліджень з підвищення інформаційної безпеки систем мобільного зв'язку

Метою проведення технологічного аудиту є оцінювання комерційного потенціалу досліджень з підвищення інформаційної безпеки систем мобільного зв'язку, створеної в результаті науково-технічної діяльності. В результаті оцінювання можна буде зробити висновок щодо напрямів (особливостей) організації подальшого її впровадження з врахуванням встановленого рейтингу.

Для проведення технологічного аудиту залучимо 3-х незалежних експертів. У нашому випадку такими експертами будуть керівник магістерської роботи та провідні викладачі випускової та споріднених кафедр.

Оцінювання комерційного потенціалу досліджень з підвищення інформаційної безпеки систем мобільного зв'язку будемо здійснювати за 12-ю критеріями згідно рекомендацій.

Результати оцінювання комерційного потенціалу досліджень з підвищення інформаційної безпеки систем мобільного зв'язку заносимо до табл. 6.1. За даними табл. 6.1 робимо висновок щодо рівня комерційного потенціалу досліджень з підвищення інформаційної безпеки систем мобільного зв'язку. При цьому користуємося рекомендаціями, наведеними в табл. 6.2.

Таким чином, робимо висновок, щодо рівня комерційного потенціалу досліджень з підвищення інформаційної безпеки систем мобільного зв'язку – середній.

ВНТУ ФІРЕН ТКСТБ МКР 2019

Таблиця 6.1 – Результати оцінювання комерційного успіху досліджень з підвищення інформаційної безпеки систем мобільного зв’язку

Критерії	Експерти		
	Семенова О.О., к.т.н., доцент	Михалевський Д.В., к.т.н., доцент	Барась С.Т., к.т.н., професор
	Бали, виставлені експертами		
1	2	2	2
2	3	1	3
3	2	2	3
4	3	1	2
5	3	2	3
6	2	2	2
7	3	2	3
8	2	2	2
9	3	2	1
10	3	3	3
11	2	2	3
12	3	3	2
Сума балів	31	24	29
Середньоарифметична сума балів, СБ	28		

Таблиця 6.2 – Рівні комерційного потенціалу досліджень з

Середньоарифметична сума балів, розрахована на основі висновків експертів	Рівень комерційного потенціалу досліджень з
0 – 10	Низький
11 – 20	Нижче середнього
21 – 30	Середній
31 – 40	Вище середнього
41 – 50	Високий

ВНТУ ФІРЕН ТКСТБ МКР 2019

6.2 Прогнозування витрат на виконання науково-дослідної, дослідно-конструкторської та конструкторсько-технологічної роботи

6.2.1 Розрахунок витрат, що стосуються виконавців досліджень з підвищення інформаційної безпеки систем мобільного зв'язку

Основна заробітна плата кожного із розробників (дослідників) Зо, якщо вони працюють в наукових установах бюджетної сфери:

$$Зо = \frac{М}{Тр} \cdot t, \qquad (6.1)$$

де М – місячний посадовий оклад конкретного розробника (інженера, дослідника, науковця тощо), грн. У 2019 році величини окладів (разом з встановленими доплатами і надбавками) рекомендується брати в межах (5000…10000) грн. за місяць;

Тр – число робочих днів в місяці; приблизно Тр = (21…23) дні;

t – число робочих днів роботи розробника (дослідника).

Зроблені розрахунки зводимо до табл. 6.3.

Таблиця 6.3 – Заробітна плата розробників

Посада	Місячний посадовий оклад, грн.	Оплата за робочий день, грн.	Число днів роботи	Витрати на заробітну плату, грн.
Керівник	8000	381	10	3810
Програміст	7000	333	5	1665
Консультант	4500	214	2	428
Всього:				5903

ВНТУ ФІРЕН ТКСТБ МКР 2019

Додаткова заробітна плата Зд всіх розробників та робітників, які брали участь у виконанні даного етапу роботи, розраховується як (10…12)% від суми основної заробітної плати всіх розробників та робітників, тобто:

$$Зд = 0{,}1 \cdot (Зр + Зо) = 0{,}1 \cdot (5115) = 590{,}3 \quad грн. \tag{6.2}$$

Нарахування на заробітну плату Нзп розробників та робітників, які брали участь у виконанні даного етапу роботи, розраховуються за формулою:

$$Нзп = 0{,}22 \cdot (Зр + Зо + Зд) = 0{,}22 \cdot (5903 + 590{,}3) = \\ = 1429 \text{ грн.} \tag{6.3}$$

де Зо – основна заробітна плата розробників, грн.;

Зр – основна заробітна плата робітників, грн.;

Зд – додаткова заробітна плата всіх розробників та робітників, грн.;

β – ставка єдиного внеску на загальнообов'язкове державне соціальне страхування, % (приймаємо для 1-го класу професійності ризику 22%).

Амортизація обладнання, комп'ютерів та приміщень А, які використовувались під час (чи для) виконання даного етапу роботи.

Дані відрахування розраховують по кожному виду обладнання, приміщенням тощо.

У спрощеному вигляді амортизаційні відрахування А в цілому бути розраховані за формулою:

$$А = \frac{Ц \cdot На}{100} \cdot \frac{Т}{12},$$

де Ц – загальна балансова вартість всього обладнання, комп'ютерів, приміщень тощо, що використовувались для виконання даного етапу роботи, грн.;

На – річна норма амортизаційних відрахувань. Для нашого випадку можна прийняти, що На = (10...25)%;

ВНТУ ФЛЕН ТКСТБ МКР 2019

Т – термін, використання обладнання, приміщень тощо, місяці.

Таблиця 6.4 – Амортизаційні відрахування

Найменування	Ціна, грн.	Норма амортизації, %	Термін використання, м.	Сума амортизації
Основні засоби, обладнання, комп'ютери тощо	15000	20	2	500
Приміщення кафедри та факультету	150000	10	2	2500
Всього	3000			

Витрати на комплектуючі К, що були використані під час виконання даного етапу роботи, розраховуються за формулою:

$$К = \sum_1^n Ні \cdot Ці \cdot Кі, грн$$

де Ні – кількість комплектуючих і-го виду, шт.;

Ці – ціна комплектуючих і-го виду, грн.;

Кі – коефіцієнт транспортних витрат, Кі = (1,1…1,15);

n – кількість видів комплектуючих.

Витрати на силову електроенергію Ве, якщо ця стаття має суттєве значення для виконання даного етапу роботи, розраховуються за формулою:

$$Ве = В \cdot П \cdot Ф \cdot Кп, грн$$

В – вартість 1 кВт-год. електроенергії, в 2019 р. В ≈ 8,45 грн./кВт;

П – установлена потужність обладнання, кВт;

Ф – фактична кількість годин роботи обладнання, годин,

ВНТУ ФІРЕН ТКСТЬ МКР 2019

Кп – коефіцієнт використання потужності; Кп < 1.

Таблиця 6.5 – Комплектуючі, що використані на розробку

Найменування матеріалу	Ціна за одиницю, грн.	Витрачено	Вартість, грн.
Компакт диск	20	1	20
Заправка картриджа	50	1	50
Ручка	10	1	10
Папір	100	2	200
Папки	30	1	30
Файли	5	2	10
Всього, з урахуванням коефіцієнта транспортних витрат	352		

Потужність обладнання складає – 0,5 кВт.

Кількість годин роботи складає – 100 годин.

Коефіцієнт викор. потужності -0,9.

Ве=380 грн.

Інші витрати Він охоплюють: витрати на управління організацією, оплата службових відряджень, витрати на утримання, ремонт та експлуатацію основних засобів, витрати на опалення, освітлення, водопостачання, охорону праці тощо.

Інші витрати Ів можна прийняти як (100…300)% від суми основної заробітної плати розробників та робітників, які були виконували дану роботу, тобто:

$$Ів = 1 \cdot (Зо + Зр) = 1 \cdot (5903) = 5903 \text{ грн.} \quad (6.4)$$

Сума всіх попередніх статей витрат дає витрати на виконання даної частини (розділу, етапу) роботи – В.

ВНТУ ФІРЕН ТКСТЬ МКР 2019

$$В = 17557 \text{ грн.}$$

6.2.2 Розрахунок загальних витрат на дослідження з підвищення інформаційної безпеки систем мобільного зв'язку

Загальна вартість всієї наукової роботи визначається за Взаг формулою:

$$Взаг = \frac{Iв}{\alpha} = \frac{5903}{0,6} = 9830 \text{ грн}, \quad (6.5)$$

де α – частка витрат, які безпосередньо здійснює виконавець даного етапу роботи, у відн. одиницях.

6.2.3 Прогнозування витрат на виконання та впровадження досліджень з підвищення інформаційної безпеки систем мобільного зв'язку

Прогнозування загальних витрат ЗВ на виконання та впровадження досліджень з підвищення інформаційної безпеки систем мобільного зв'язку здійснюється за формулою:

$$ЗВ = \frac{Взаг}{\beta} = \frac{9830}{0,1} = 98300 \text{ грн}, \quad (6.6)$$

де β – коефіцієнт, який характеризує етап (стадію) виконання даної роботи.

Так, якщо розробка знаходиться: на стадії науково-дослідних робіт, то β ≈ 0,1; на стадії технічного проектування, то β ≈ 0,2; на стадії досліджень з конструкторської документації, то β ≈ 0,3; на стадії досліджень з технологій, то β ≈ 0,4; на стадії досліджень з дослідного зразка, то β ≈ 0,5; на стадії досліджень з промислового зразка, β ≈ 0,7; на стадії впровадження, то β ≈ 0,9.

ВНТУ ФІРЕН ТКСТБ МКР 2019

6.3 Прогнозування комерційних ефектів від реалізації досліджень з підвищення інформаційної безпеки систем мобільного зв'язку

З метою прогнозування комерційних ефектів від реалізації досліджень з підвищення інформаційної безпеки систем мобільного зв'язку складемо таблицю вихідних показників, за рахунок яких і відбуватиметься отримання комерційного ефекту.

Таблиця 6.6 – Вихідні дані для прогнозування комерційного ефекту від реалізації досліджень з підвищення інформаційної безпеки систем мобільного зв'язку

Рік реалізації досліджень	1
Кількість од. реалізації, шт.	1

Збільшення чистого прибутку підприємства Пі для кожного із років, протягом яких очікується отримання позитивних результатів від впровадження досліджень з, розраховується за формулою:

$$\Delta Пi = \sum_1^n (\Delta Ц0 \cdot N + Ц0 \cdot \Delta N)i \cdot \rho \cdot \gamma \cdot (1 - \frac{v}{100}) \quad (6.7)$$

де ΔПо – покращення основного оціночного показника від впровадження результатів досліджень у даному році. Зазвичай таким показником може бути ціна одиниці нового дослідження;

N – основний кількісний показник, який визначає діяльність підприємства у даному році до впровадження результатів наукового дослідження;

ΔN – покращення основного кількісного показника діяльності підприємства від впровадження результатів досліджень;

Цо – основний оціночний показник, який визначає діяльність підприємства у даному році після впровадження результатів наукових досліджень;

ВНТУ ФІРЕН ТКСТБ МКР 2019

n – кількість років, протягом яких очікується отримання позитивних результатів від впровадження досліджень;

λ – коефіцієнт, який враховує сплату податку на додану вартість. У 2018 р. ставка податку на додану вартість дорівнює 20%, а коефіцієнт – 0,8333. З 2014 року ставка податку на додану вартість встановлена на рівні 17%, а коефіцієнт – 0,8547;

ρ – коефіцієнт, який враховує рентабельність продукту. Рекомендується приймати – 0,2…0,3;

υ – ставка податку на прибуток. У 2018 році – 21%, у 2013 році – 19%, а з 2014 року – 16%.

Збільшення чистого прибутку підприємства Пі протягом першого року складе: 42186 грн.

6.4 Розрахунок ефективності вкладених інвестицій та період їх окупності

6.4.1 Визначення абсолютної ефективності вкладених інвестицій у дослідження з підвищення інформаційної безпеки систем мобільного зв'язку

Для цього користуються формулою:

$$Еабс = (ПП - PV), \quad (6.8)$$

де ПП – приведена вартість всіх чистих прибутків, що їх отримає підприємство (організація) від реалізації результатів наукових досліджень, грн.;

PV – теперішня вартість інвестицій PV = ЗВ, грн.

У свою чергу, приведена вартість всіх чистих прибутків ПП розраховується за формулою:

$$ПП = \sum_1^\tau \frac{\Delta Пі}{(1+\tau)^t} \quad (6.9)$$

ВНТУ ФІРЕН ТКСТБ МКР 2019

де ΔПі– збільшення чистого прибутку у кожному із років, протягом яких виявляються результати виконаної та впровадженої НДДКР, грн.;

т – період часу, протягом якого виявляються результати впровадженої НДДКР, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні; для України цей показник знаходиться на рівні 0,1;

t – період часу (в роках) від моменту отримання чистого прибутку до точки „0”.

$$ПП = 421860 \text{ грн.},$$

$$Еабс = 421860 - 98300 = 323560 \text{ грн.}$$

Оскільки Еабс > 0, то результат від проведення наукових досліджень та їх впровадження принесе прибуток, але це також ще не свідчить про те, що інвестор буде зацікавлений у фінансуванні досліджень з підвищення інформаційної безпеки систем мобільного зв’язку.

6.4.2 Розрахунок відносної ефективності вкладених коштів в НДДКР з досліджень підвищення інформаційної безпеки систем мобільного зв’язку

Для цього користуються формулою:

$$Ев = \sqrt[т]{1 + \frac{Еабс}{PV}} - 1 \qquad (6.10)$$

де Еабс – абсолютна ефективність вкладених інвестицій, грн..;

PV – теперішня вартість інвестицій PV = ЗВ, грн.;

Тж – життєвий цикл наукових досліджень, роки.

$$Ев = 1{,}21$$

ВНТУ ФІРЕН ТКСТБ МКР 2019

Далі, розрахована величина Ев порівнюється з мінімальною (бар'єрною) ставкою дисконтування, що дорівнює:

$$\tau = d + f, \tag{6.11}$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; в 2018 році в Україні d = (0,14...0,2);

f – показник, що характеризує ризикованість вкладень; зазвичай, величина f = (0,05...0,1), але може бути і значно більше.

$$Ев = 1{,}21 \geq \tau = 0{,}2 + 0{,}1 = 0{,}3.$$

Оскільки величина Ев > τмін, то інвестор може бути зацікавлений у фінансуванні даного наукового дослідження.

6.4.3 Розрахунок терміну окупності коштів, вкладених в наукові дослідження з підвищення інформаційної безпеки систем мобільного зв’язку

Термін окупності вкладених у реалізацію наукового проекту інвестицій Ток можна розрахувати за формулою:

$$Ток = \frac{1}{Ев} = \frac{1}{1{,}21} = 0{,}82 \text{ роки}. \tag{6.12}$$

Оскільки Ток < 3…5-ти років, то фінансування даних наукових досліджень з підвищення інформаційної безпеки систем мобільного зв’язку є доцільним.

ВНТУ ФІРЕН ТКСТБ МКР 2019

7 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Забезпечення захисту працівників під час трудового процесу від небезпечних та шкідливих виробничих факторів, які справляють негативний вплив на здоров'я, життя та працездатність людини, забезпечення належних умов праці є важливими завданнями безпеки життєдіяльності у виробничому середовищі.

У даному розділі наводиться розгляд шкідливих, небезпечних [17] та уражаючих для людини і навколишнього довкілля факторів, що виникають при проведенні дослідження інформаційної безпеки систем мобільного зв'язку. Тут розглядаються, в тому числі, технічні рішення з гігієни праці та виробничої санітарії, визначення радіусу дроту сітчастого екрану для послаблення ЕМВ, технічні рішення з промислової та пожежної безпеки під час проведення дослідження, безпека в надзвичайних ситуаціях.

7.1 Гігієна праці та виробнича санітарія

7.1.1 Склад повітря робочої зони та мікроклімат

Вибираємо для приміщення для проведення дослідження інформаційної безпеки систем мобільного зв'язку, категорію важкості робіт за фізичним навантаженням – легка Іа.

Згідно із [18] допустимі показники мікроклімату у робочій зоні для теплого та холодного періодів року наведені в табл.7.1.

Для опромінення менше 25% поверхні тіла людини, допустима інтенсивність теплового опромінення – 100 Вт/м^2.

Вміст шкідливих речовин в повітрі робочої зони не повинен перевищувати гранично допустимих концентрацій (ГДК) у повітрі робочої зони та підлягає систематичному контролю з метою запобігання можливості перевищення ГДК, значення яких для роботи з ЕОМ наведено в табл. 7.2.

ВНТУ ФІРЕН ТКСТБ МКР 2019

При використанні ЕОМ джерелом забруднення повітря є також іонізація молекул речовин, що містяться у повітрі. Рівні додатних та від'ємних іонів повинні відповідати [20] та наведені в табл. 7.3.

Таблиця 7.1 – Нормовані допустимі параметри мікроклімату

Період року	Категорія робіт	Температура повітря, °С для робочих місць		Відносна вологість повітря, %	Швидкість руху повітря, м/с
		постійних	непостійних		
Холодний	Ia	21-25	18-26	75	≤0,1
Теплий		22-28	20-30	55 при 28°С	0,1-0,2

Таблиця 7.2 – Гранично допустимі концентрації шкідливих речовин [21]

Назва речовини	ГДК, мг/м^3	Агрегатний стан	Клас небезпеки
Озон	0,1	Пара	4
Оксиди азоту	5	Пара	2
Пил	4	Аерозоль	2

Таблиця 7.3 – Кількість іонів в 1 см^3 повітря приміщення при роботі на ЕОМ

Рівні	Мінімально необхідні	Оптимальні	Максимально допустимі
позитивний	400	1500-3000	50000
негативний	600	3000-5000	50000

З метою встановлення нормованих показників мікроклімату та складу повітря робочої зони запропоновано:

1) в приміщенні має бути встановлена система кондиціонування для теплого і опалення для холодного періодів року;

ВНТУ ФІРЕН ТКСТБ МКР 2019

2) припливно-витяжна система вентиляції, а при несприятливих погодних умовах кондиціонування.

7.1.2 Виробниче освітлення

Для забезпечення гігієнічних раціональних умов на робочих місцях великі вимоги висуваються до кількісних та якісних показників освітлення.

З точки зору задач зорової роботи в приміщенні, де проводиться робота з дослідження інформаційної безпеки систем мобільного зв'язку, відповідно до [19] знаходимо, що вони відносяться до IV розряду зорових робіт. Приймаємо контраст об'єкта з фоном – середній, а характеристику фону – середню, яким відповідає підрозряд *в*.

Нормовані значення коефіцієнта природного освітлення (КПО) і мінімальні значення освітленості для штучного освітлення приведені в табл. 7.4.

Таблиця 7.4 – Нормовані значення коефіцієнта природного освітлення та мінімальні освітленості для штучного освітлення

Характеристика зорової роботи	Найменший розмір об'єкта розрізнення, мм	Розряд зорової роботи	Підрозряд зорової роботи	Контраст об'єкта розрізнення з фоном	Характеристика фону	Освітленість при штучному освітленні, лк			КПО для бокового освітлення, %	
						комбіноване		загальне	Природного	Суміщеного
						всього	у т. ч. від загального			
Середньої точності	0,5-1	IV	в	середній	середній	400	200	200	1,5	0,9

Так як приміщення знаходиться у м. Вінниця (друга група забезпеченості природним світлом), а вікна орієнтовані за азимутом 0°, то для таких умов КЕО визначатиметься за формулою [19, 20].

ВНТУ ФІРЕН ТКСТБ МКР 2019

$$e_N = e_н m_N \, [\%], \qquad (7.1)$$

де $e_н$ – табличне значення КЕО для бокового освітлення, %;

m_N – коефіцієнт світлового клімату;

N – порядковий номер групи забезпеченості природним світлом.

Підставляючи відомі значення одержимо нормовані значення КПО для бокового та суміщеного освітлення:

$$e_{N.б} = 1{,}5 \cdot 0{,}9 = 1{,}4 \ (\%);$$

$$e_{N.с} = 0{,}9 \cdot 0{,}9 = 0{,}8 \ (\%).$$

З метою забезпечення нормативних значень параметрів освітлення передбачено такі заходи:

1) при недостатньому природному освітлені в світлу пору доби доповнення штучним за допомогою газорозрядних ламп з утворенням системи суміщеного освітлення;

2) застосування загального штучного освітлення в темну пору доби.

7.1.3 Виробничі віброакустичні коливання

Зважаючи на те, що при експлуатації пристроїв крім усього іншого обладнання використовується устаткування, робота якого генерує шум та вібрацію, необхідно передбачити захист від шуму та вібрації.

Визначено, що приміщення, де проводиться робота з дослідження інформаційної безпеки систем мобільного зв’язку може мати робочі місця із шумом та вібрацією, що створюється рухомими елементами ЕОМ.

Для попередження травмування працюючих від дії шуму він підпадає під нормування. Основним документом стосовно промислового шуму, що діє в нашій країні, є [21], згідно з яким допустимі рівні звукового тиску, рівні звуку і

ВНТУ ФІРЕН ТКСТБ МКР 2019

еквівалентні рівні шуму на робочих місцях у виробничих приміщеннях не повинні перевищувати значень, які приведені у табл. 7.5. Норми виробничих вібрацій наведені в табл. 7.6 для локальної вібрації.

Таблиця 7.5 – Допустимі рівні шуму і еквівалентні рівні звуку

Рівні звукового тиску в дБ в октавних полосах з середньо-геометричними частотами, Гц									Рівні звуку та еквівалентні рівні звуку, дБА
31,5	63	125	250	500	1000	2000	4000	8000	
86	71	61	54	49	45	42	40	38	50

Таблиця 7.6 – Нормовані рівні віброприскорення [22]

Гранично допустимі рівні віброприскорення, дБ, в октавних полосах з середньо-геометричними частотами, Гц								Коректовані рівні віброприскорення, дБА
8	16	31,5	63	125	250	500	1000	
73	73	79	85	91	97	103	109	76

Для покращення віброакустичного клімату у приміщенні передбачено такі заходи:

1) періодичне змащування підшипників вентиляторів блоку живлення комп’ютера та кулерів мікропроцесора та відеоадаптера;

2) передбачено використовувати в приміщені штори із щільної тканини.

7.1.4 Виробничі випромінювання

Значення напруженості електромагнітного поля на робочих місцях з персональними комп'ютерами мають не перевищувати граничнодопустимі, які складають 20 кВ/м.

Експозиційна доза рентгенівського випромінювання на відстані 0,05 м від екрана до корпуса монітора при будь-яких положеннях регулювальних при-

ВНТУ ФІВЕН ТКСТБ МКР 2019

строїв не повинні перевищувати $7{,}74 \cdot 10^{-12}$ Кл/кг, що відповідає потужності еквівалентної дози 0,1 мБер/год (100 мкР/год) згідно [31].

З метою забезпечення захисту та досягнення нормативних рівнів випромінювань необхідно застосовувати приекранні фільтри, локальні світлофільтри та інші засоби захисту, що пройшли випробування в акредитованих лабораторіях і мають щорічний гігієнічний сертифікат.

Визначимо радіус дроту стального сітчастого екрану, якщо послаблення електромагнітного випромінювання L = 32 дБ, довжина хвилі λ = 52 мм, крок сітки d = 12 мм.

Крок сітки стального сітчастого екрану можна визначити з формули

$$L = 10\lg \frac{4\left(\frac{d}{\lambda}\ln\frac{d}{2\pi r_0}\right)^2}{1+4\left(\frac{d}{\lambda}\ln\frac{d}{2\pi r_0}\right)^2} \text{ [дБ]}, \qquad (7.2)$$

звідки після значних математичних перетворень отримаємо таку формулу

$$r_0 = \frac{d}{2\pi e^{\frac{\lambda}{2d\sqrt{1-10^{L/10}}}}} \text{ [мм]}, \qquad (7.3)$$

де L – послаблення електромагнітного випромінювання, дБ;

λ – довжина хвилі, мм;

d – крок сітки сітчастого екрану, мм.

Після підстановки відомих значень у формулу (7.3), одержимо:

$$r_0 = \frac{12}{2 \cdot 3{,}14 \cdot e^{\frac{52}{2 \cdot 12\sqrt{1-10^{32/10}}}}} = 1{,}91 \text{ (мм)}.$$

ВНТУ ФІЕН ТКСТБ МКР 2019

7.2 Промислова та пожежна безпека під час проведення дослідження

Сучасний етап розвитку техніки, автоматизації розробок та досліджень характеризується широким використанням на робочому місці ЕОМ. Велика кількість прикладних програм перетворює ЕОМ на основне знаряддя праці радіоінженера.

7.2.1 Безпека щодо організації робочих місць

Розташування робочих місць, оснащених ЕОМ виконується у приміщеннях з однобічним розміщенням вікон, які неодмінно мають бути оснащені сонцезахисним засобами: жалюзями та шторами [23]. При розміщенні робочих місць у приміщеннях з джерелами шкідливих та небезпечних виробничих чинників, вони зобов’язані розміщатись у абсолютно відокремлених кабінетах з природним освітленням та організованим повітрообміном. Площа, на якій розташовується одне робоче місце для обслуговуючого персоналу, повинна становити не менше 6,0 м^2, об'єм – не менше ніж 20 м^3, а висота – не менше 3,2 м [24]. Поверхня підлоги повинна бути гладкою, без вибоїн, не слизькою, зручною для вологого прибирання, мати антистатичні властивості. Не дозволяється використовувати для оздоблення інтер'єру полімерні матеріали, що виділяють у повітря шкідливі речовини.

7.2.2 Електробезпека

Основними причинами ураження електричним струмом в даному приміщенні можуть бути: робота під напругою при ремонтних роботах, несправність устаткування, випадкове торкання до металевих частин, які опинилися під напругою чи струмоведучих частин. Згідно [25] дане приміщення належить до приміщень із підвищеною небезпекою ураження електричним струмом в наслідок наявності значної (більше 75 %) відносної вологості. Тому

ВНТУ ФІРЕН ТКСТБ МКР 2019

безпека використання електрообладнання має гарантуватись комплексом заходів, що включають застосування ізоляції струмовідних частин, захисних блокувань, захисного заземлення тощо [26].

Таблиця 7.7 – Значення мінімальних меж вогнестійкості приміщення [28]

Ступінь вогнестійкості будівлі	Стіни				Колони	Східчасті майданчики	Плити та інші несучі конструкції	Елементи покриття	
	Несучі та східчасті клітки	Самонесучі	Зовнішні несучі	Перегородки				Плити, прогони	Балки, ферми
2	REI 120 M0	REI 60 M0	E 15 M0	EI 15 M0	R 120 M0	R 60 M0	REI 45 M0	REI 15 M0	R 30 M0

Примітка. R – втрати несучої здатності; E – втрати цілісності; I – втрати теплоізолювальної спроможності; M – показник здатності будівельної конструкції поширювати вогонь (межа поширення вогню); M0 – межа поширення вогню дорівнює 0 см; M1 – M ≤ 25 см – для горизонтальних конструкцій; M ≤ 40 см – для вертикальних і похилих конструкцій; M2 – M > 25 см – для горизонтальних конструкцій; M > 40 см – для вертикальних і похилих конструкцій, нн – не нормується.

Таблиця 7.8 – Протипожежні норми проектування будівель і споруд [29]

Об’єм приміщення, тис. м	Категорія пожежної небезпеки	Ступінь вогнестійкості	Відстань, м, при щільності людського потоку в загальному проході, осіб/м^2			Кількість людей на 1 м ширини евакуаційного виходу	Протипожежні розриви, м, при ступені їх вогнестійкості			Найбільша кількість поверхів	Максимально допустима площа поверху, м^2, для числа поверхів		
			до 1	2-3	4-5		I,II	III	IV,V		1	2	3 і більше
до 15	Б	2	40	25	15	45	9	9	12	6	н.о.	–	–

Примітки: н.о. – не обмежується, н.н. – не нормується.

ВНТУ ФРЕН ГКСТБ МКР 2019

7.2.3 Пожежна безпека

Відповідно до [27] приміщення, в якому проводиться робота з дослідження інформаційної безпеки систем мобільного зв’язку, відноситься до категорії пожежної небезпеки Б. Дане приміщення відноситься до 2-го ступеня вогнестійкості, в якому приміщення знаходяться в будівлі з несучими та огороджувальними конструкціями з природних або штучних кам’яних матеріалів, бетону, залізобетону із застосуванням листових і плитних негорючих матеріалів.

Мінімальні межі вогнестійкості будівельних конструкцій приміщення, що розглядається наведені в табл. 7.7. В табл. 7.8 наведено протипожежні норми проектування будівель і споруд.

Встановлюємо, що приміщення, де проводиться робота з дослідження, має бути обладнане двома вогнегасниками, пожежним щитом, ємністю з піском [27].

7.3 Дослідження безпеки роботи системи мобільного зв’язку в умовах дії загрозливих факторів надзвичайних ситуацій

Загрозливі фактори надзвичайних ситуацій (НС) можуть негативно впливати на безпеку роботи системи мобільного зв’язку, спрямованої на забезпечення послугами цифрового безпровідного зв'язку. При цьому найбільшу небезпеку серед НС для даної системи становлять іонізуючі випромінювання та електромагнітний імпульс.

Вплив іонізуючих випромінювань приводить як до оборотних, так і необоротних змін електричних властивостей твердотільних приладів та інтегральних схем. Оскільки такі зміни можуть приводити до відмов електронних підсистем, вагомі зусилля останнім часом скеровуються на розробку методів, які дозволяють уникнути погіршення параметрів радіоелектронної апаратури (РЕА) при опроміненні.

ВНТУ ФІРЕН ТКСТБ МКР 2019

Електромагнітний імпульс (ЕМІ) ушкоджує напівпровідникові прилади, резистори, конденсатори та ін. Це являє значну небезпеку для апаратури, добре захищеної від впливу інших загрозливих чинників. Тому слід пам'ятати про те, що захист РЕА від механічних пошкоджень ушкоджень не оберігає від дії ЕМІ. Апаратура може втратити працездатність, перебуваючи у безпечних захисних спорудах.

Для запобігання цього проводяться розрахунки безпеки роботи системи мобільного зв’язку в умовах дії іонізуючих випромінювань, електромагнітного імпульсу та приймаються рішення щодо захисту елементів РЕА.

7.3.1 Дослідження безпеки роботи системи мобільного зв’язку в умовах дії іонізуючих випромінювань

Приймаючи до уваги елементну базу, що використовується при реалізації системи мобільного зв’язку, складемо таблицю потужностей експозиційної дози опромінення для кожного елемента $P_{зв.і}$, які спричиняють початок зворотних змін (табл. 7.9).

Знаходимо елемент, який найбільшою мірою піддається впливу випромінювання, тобто елемент із найменшим значенням $P_{зв.min} = 10^4$ Р.

Розраховуємо граничне значення потужності експозиційної дози:

$$P_{гр} = K_{над} \cdot P_{в.min} \cdot K_{посл} \text{ [Р/год]}; \quad (7.4)$$

$$P_{гр} = 0{,}95 \cdot 10^4 \cdot 2 = 19000 \text{ (Р/год)},$$

де $K_{над}$ – коефіцієнт надійності (приймається $K_{над} = 0{,}95$);

$P_{зв}$ – потужність експозиційної дози, яка відповідає початку зворотних змін в елементах;

$K_{посл}$ – коефіцієнт послаблення радіації (приймається $K_{посл} = 2$).

ВНТУ ФІРЕН ТКСТБ МКР 2019

Таблиця 7.9 – Потужності експозиційної дози кожного компонента

№	Елементи системи мобільного зв'язку	$P_{зв.i}$, Р/год	$P_{зв.min}$, Р/год
1	Транзистори серії КП	10^4	10^4
2	Діоди 1N4004	10^4	
3	Конденсатори СР-13.020	10^7	
4	Мікросхеми МС4000	10^5	
5	Резистори МЛТ	10^8	

Таким чином, безпечне функціонування системи мобільного зв'язку в умовах впливу іонізуючих випромінювань забезпечується при $P_{зв} <$ 19000 Р/год, а допустимий час його безвідмовної роботи може скласти:

$$t_{доп} = \left(\frac{Д_{гр} K_{посл}}{2P_1} + \sqrt{t_n} \right)^2 \text{ [год];} \qquad (7.5)$$

$$t_{доп} = \left(\frac{10^6 \cdot 2}{2 \cdot 19000} + \sqrt{1} \right)^2 = 2876{,}35 \text{ (год).}$$

7.3.2 Дослідження безпеки роботи системи мобільного зв'язку в умовах дії електромагнітного імпульсу

Початкові дані: напруга живлення $U_{ж}$ = 220 ± 5% В; максимальна довжина горизонтальної струмопровідної частини електричної принципової схеми l_B = 0,3 м.

Як критерій безпеки роботи радіоелектронних систем до дії електромагнітного імпульсу приймаємо коефіцієнт безпеки:

$$K_в = 20 \lg \frac{U_д}{U_{в(г)}} \geq 40 \text{ [дБ],} \qquad (7.6)$$

ВНТУ ФІРЕН ТКСТБ МКР 2019

де $U_д$ – допустимі коливання напруги живлення, В;

$U_{в(г)}$ – напруга наведення за рахунок електромагнітного імпульсу в вертикальних (горизонтальних) струмопровідних частинах, В.

Визначаємо спочатку допустиме коливання напруги живлення:

$$U_д = U_ж + \frac{U_ж}{100} N \text{ [В]}, \tag{7.7}$$

де $U_ж$ – робоча напруга живлення, В;

N – допустимі коливання напруги, %.

Визначаємо максимально очікувану напруга в горизонтальних лініях:

$$U_в = \frac{U_д}{10^{K/20}} \text{ [В]}. \tag{7.8}$$

де K – коефіцієнт безпеки (K = 40 дБ).

Розраховуємо горизонтальну складову напруженості електромагнітного поля за формулою:

$$E_г = \frac{U_в}{l_в} \text{ [В/м]}. \tag{7.9}$$

Визначаємо горизонтальну складову напруженості електромагнітного поля за формулою

$$E_в = 10^3 E_г \text{ [В/м]}, \tag{7.10}$$

Після підстановки відомих значень у формули (7.7, …, 7.10) отримаємо

ВНТУ ФІРЕН ТКСТБ МКР 2019

$$U_{\partial} = 220 + \frac{220}{100} \cdot 5 = 231 \text{ (В)};$$

$$U_{в} = \frac{231}{10^{40/20}} = 2{,}31 \text{ (В)};$$

$$E_{г} = \frac{2{,}31}{0{,}3} = 7{,}7 \text{ (В/м)};$$

$$E_{в} = 10^{3} \cdot 7{,}7 = 7700 \text{ (В/м)}.$$

Згідно з виконаними розрахунками безпека роботи системи мобільного зв'язку в умовах впливу електромагнітного імпульсу можлива для значення напруженості вертикальної складової електричного поля $E_{в} < 7700$ В/м.

7.3.3 Розробка превентивних заходів по підвищенню безпеки роботи системи мобільного зв'язку в умовах надзвичайних ситуацій

З метою зменшення негативної дії на РЕА системи мобільного зв'язку можна використати наступні методи.

Для захисту системи мобільного зв'язку від дії іонізуючих випромінювань можна використати алюмінієві сплави, леговані елементами з високим атомним номером (лантаноїдами і рідкоземельними елементами), сплави на основі рідкоземельних і тугоплавких елементів, а також багатошарові матеріали.

З метою захисту від впливу електромагнітного імпульсу потрібно використати захищене металічним екраном приміщення, в якому розташована радіоелектронна апаратура.

Товщину захисного екрану знаходимо за формулою:

ВНТУ ФІРЕН ТКСТЬ МКР 2019

$$t = \frac{A}{k\sqrt{f}} \text{ [см];} \qquad (7.11)$$

$$t = \frac{15}{5{,}2 \cdot \sqrt{15000}} = 0{,}024 \text{ (см)} = 0{,}24 \text{ (мм)},$$

де A – перехідне затухання енергії електричного поля стальним екраном (A = 15 дБ);

k – коефіцієнт, який для стального екрана дорівнює 5,2;

f – найбільш характерна частота (f = 15000 Гц).

7.4 Висновки до розділу

Під час виконання цього розділу було розглянуто такі питання охорони праці та безпеки в надзвичайних ситуаціях, як технічні рішення з гігієни праці та виробничої санітарії, визначення радіусу дроту сітчастого екрану для послаблення ЕМВ, технічні рішення з промислової та пожежної безпеки під час проведення дослідження інформаційної безпеки систем мобільного зв'язку, безпека в надзвичайних ситуаціях. Також в цьому розділі досліджено безпеку роботи системи мобільного зв'язку в умовах дії загрозливих чинників НС. Встановлено, що безпечне функціонування системи мобільного зв'язку в умовах впливу іонізуючих випромінювань забезпечується при потужності експозиційної дози опромінення менше 19000 Р/год, а допустимий час його безвідмовної роботи може скласти 2876,35 год. Запропоновано превентивні заходи із покращення безпеки роботи системи мобільного зв'язку в умовах нідзвичайних ситуацій. Визначено, що екранування стальним екраном товщиною 0,24 мм захищає систему мобільного зв'язку від дії електромагнітного імпульсу для перехідного затухання енергії електричного поля в 15 дБ.

ВНТУ ФІРЕН ТКСТБ МКР 2019

ВИСНОВКИ

Таким чином, розглянувши сучасний розвиток мереж стільникового зв'язку як в Україні, так і у світі, можна обґрунтувати необхідність подальшого дослідження мобільних мереж п'ятого покоління, підкресливши їхні основні переваги. Окрім того, було проаналізовано відомі системи безпеки стільникових мереж. Однак, не дивлячись на усі переваги систем безпеки вже існуючих мереж.

У роботі було проведено аналіз проблемних місць у моделі системної безпеки, а також розглянуто основні способи їх подолання.

Були розглянуті підходи до аутентифікації викликів користувачів при затосуванні псевдовипадкових послідовностей Касамі та Голда, що дає змогу забезпечити необхідну захищеність від процедури нав'язування помилкових викликів зловмисниками. Одержані залежності показують, що такий підхід до аутентифікації викликів користувачів забезпечує високу імітозахищеність при цьому не знижуючи завадостійкість викликів конфіденційних користувачів.

У магістерській роботі було описано процес розроблення системи криптоаналізу блочного симетричного алгоритму шифрування KASUMI. При цьому, для криптоаналізу було застосовуано метод типу «сендвіч-атака». Після здійснення аналізу криптоаналітичного методу були запропоновані шляхи підвищення швидкості його реалізації за допомогою декомпозиції обчислювальної задачі та її розподілу між окремими обчислювальними засобами.

Таким чином, можна зробити висновок, що шифр KASUMI як найбільш криптостійкий є оптимальним вибором для шифрування даних у мережах мобільного зв'язку.

Також у магістерський дипломній роботі запропоновано застосовувати штучну нейронну мережу для розв'язанння задачі ідентифікації абонента системи мобільного зв'язку. У такій системі вхідний пароль перетворюється згідно алгоритму у вибірку, яка є навчальною для нейроннної мережі. При перемішу-

ВНТУ ФІРЕН ТКСТБ МКР 2019

ванні елементів триманого вектору вагових коефіцієнтів. Завдяки використанню штучної нейронної мережі, система отримає такі переваги:

1) знижується можливість виникнення колізій завдяки великій надмірності хеш-значень тавідсутності кореляції між хеш-значенням та паролем;
2) підвищується стійкість до криптографічних атак завдяки довгому процесу отримання хеш-значення.

В економічній частині роботи були розрахована вартість розробки, виробнича собівартість, ціна реалізації та термін окупності нового пристрою.

В розділі ”Безпека життєдіяльності” проаналізовані умови праці в лабораторії для досліджень, виконано організаційно-технічні, санітарно-гігієнічні заходи та протипожежні заходи.

ВНТУ ФІРЕН
ТКСТБ МКР 2019

ПЕРЕЛІК ПОСИЛАНЬ

1. Габарчук В. Кибернетический подход к проектированию систем защиты информации / В. Габарчук, З. Зинович, А. Свиц – К.: Киев-Луцк-Любляны, 2003. – 653 с.
2. Одарченко Р.С. Обгрунтування основних вимог до систем безпеки стільникових мереж 5-го поколения. - Безпека информации. Віп №3 (Том 21) - 2015., С. 229-235
3. Одарченко Р.С., Беженар Ю.В., Ксендзенко А.О. Аналіз вразливостей систем захисту інформації в Мережа Wi-Max та методів їх Усунення // Захист інформації. Зб. наукових праць.- К .: НАУ, 2011. - Вип. 18. - С. 39-44.
4. Щербаков В. Б Безопасность беспроводных сетей: стандарт IEEE 802.11. / В. Б. Щербаков, С. А. Ермаков - Москва : РадиоСофт, 2010. - 256 с.
5. Замула О. А. Застосування теорії нечітких множин та лінгвістичної невизначеності при оцінюванні ризиків інформаційної безпеки / О. А. Замула, В. І. Черниш, О. І. Аніщенко // Системи обробки інформації. - 2011. - Вип. 5. - С. 152-155.
6. Богдан В. П. Блокування засобів стільникового зв’язку і бездротового доступу / В. П. Богдан // Сучасна спеціальна техніка. - 2013. - № 1. - С. 100-107.
7. Пархоменко І. І. Проблеми захисту інформації в мережах мобільного зв’язку третього покоління / І. І. Пархоменко, Ю. О. Кривий. Наукоємні технології, 2009. № 3–4 (7–8). – с.77-80.
8. Москаленко А. О. Дослідження механізмів забезпечення інформаційної безпеки в існуючих та перспективних системах рухомого зв’язку А. О. Москаленко, О. В. Федін // Наука і техніка Повітряних Сил Збройних Сил України. - 2013. - № 1. - С. 99-103.
9. Кондрацький Ю.О. Дослідження криптостійкості алгоритму KASUMI на доступних високопродуктивних обчислювальних засобах / Ю.О. Кондрацький, С.А. Лупенко, А.М. Луцків. – Proceedings of the Second International

ВНТУ ФІРЕН ТКСТБ МКР 2019

Conference "Cluster Computing" CC 2013 (Ukraine, Lviv, June 3-5, 2013). – p. 101-104.

10. Корсунский А. С. Аутентификация корреспондентов в сетях UMTS при использовании псевдослучайных последовательностей Голда и Касами / А.С. Корсунский, О.В. Шейкина. – Автоматизация процессов управления. – 2010. – №2. – с. 40-47.
11. Корсунский А. С. Способ аутентификации вызовов корреспондентов в сетях подвижной радиосвязи с кодовым разделением каналов / А. С. Корсунский // Труды 63-й конференции, посвященной дню радио.– СПб. : СПбГЭТУ ЛЭТИ, 2008. –458 с.
12. Беляев С.С. Повышение информационной безопасности процессов управления мобильными объектами в системах управления на основе сетей сотовой связи третьего поколения / С.С. Беляев, Г.П. Жигулин. Известия Южного федерального университета. Технические науки. 2014. № 3(152). С. 194-200.
13. Особенности декодера турбокода в программируемых радиостанциях при воздействии помех / С.П. Ливенцев, С.В. Зайцев, С.В. Кныр [и др.] // Зв'язок. – 2007. – № 2. – С. 31 – 35.
14. Зайцев С.В. Анализ пропускной способности дискретно-непрерывного канала связи для программируемых радиостанций с цифровыми методами модуляции сигнала при воздействии организованных помех / С.В. Зайцев // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – 2006. – № 2 (13). – С. 27 – 32.
15. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие / М.А. Иванов, И.В. Чугунков. – М.: Изд-во НИЯУ МИФИ, 2012. – 400 с.
16. Костів Ю.М. Апаратна реалізація і дослідження модифікованих генераторів Фібоначчі / Ю.М. Костів, В.М. Максимович, М.М. Мандрона, О.І. Герасимчук // Комп’ютерні технології друкарства. – Львів : Вид-во Української академії друкарства. – 2013. – Вип. 29. – С. 167-174.

ВНТУ ФЛРЕН ПКСТБ МКР 2019

17. ГОСТ 12.0.003-74.ССБТ. Опасные и вредные производственные факторы. Классификация.
18. ДСН 3.3.6.042-99. Санітарні норми мікроклімату виробничих приміщень.
19. ДБН В.2.5-28-2006. Природне і штучне освітлення.
20. Пособие по расчету и проектированию, естественного, искусственного и совмещенного освещения НИИСФ – М.: Стройиздат. 1985. – 384 с.
21. ДСН 3.3.6-037-99. Санітарні норми виробничого шуму, ультразвуку та інфразвуку.
22. ДСН 3.3.6.039-99. Державні санітарні норми виробничої та загальної вібрацій.
23. ГОСТ 12.2.032-78. ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования.
24. Методичні вказівки до опрацювання розділу "Охорона праці та безпека в надзвичайних ситуаціях" в дипломних проектах і роботах студентів спеціальностей, що пов’язані з функціональною електронікою, автоматизацією та управлінням / Уклад. О. В. Березюк, М. С. Лемешев. – Вінниця : ВНТУ, 2012. – 64 с.
25. ДНАОП 0.00-1.21-98 Правила безпечної експлуатації електроустановок споживачів. – К. : Держнаглядохоронпраці, 1998. – 382 с.
26. ДБН В.2.5-27-2006. Захисні заходи електробезпеки в електроустановках будинків і споруд.
27. НАПБ Б.03.001-2004. Типові норми належності вогнегасників.
28. ДБН В.1.1.7-2002. Пожежна безпека об’єктів будівництва.
29. СНиП 2.09.02-85. Противопожарные нормы проектирования зданий и сооружений.

ВНТУ ФЛЕН ТКСТБ МКР 2019

ДОДАТКИ

ВНТУ ФІРЕН
ТКСТБ МКР 2019

Додаток А

(обов’язковий)

ВНТУ

ЗАТВЕРДЖУЮ

Зав.кафедри ТКСТБ

канд.техн.наук,

професор

Г.Г.Бортник

“__” _____ 2019 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання магістерської кваліфікаційної роботи

ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМ МОБІЛЬНОГО ЗВ’ЯЗКУ

08-34.МКР.002.00.000 ТЗ

ВНТУ ФІРЕН ТКСТБ МКР 2019

Керівник роботи

к.т.н., доц. кафедри ТКСТБ ВНТУ

Семенова О.О.

Виконавець: ст. гр. ТТК-18м

Вітюк М. О.

Вінниця-2019

1 ПІДСТАВА ДЛЯ ВИКОНАННЯ РОБОТИ

Робота проводиться на підставі наказу ректора по Вінницькому національному технічному університету від “02” 10 2019 року № 254 та індивідуального завдання на магістерську кваліфікаційну роботу.

Дата початку роботи: 02.09.2019 р.

Дата закінчення: 09.12.2019 р.

2 МЕТА І ПРИЗНАЧЕННЯ МКР

Метою даної магістерської кваліфікаційної роботи є дослідження механізмів забезпечення безпеки інформації у мережах мобільного зв’язку.

Об’єкт дослідження – фізичні процеси у пристроях мобільного зв’язку.

Предмет дослідження – пристрої системи мобільного зв’язку.

Основними завданнями роботи є:

- огляд механізмів забезпечення інформаційної безпеки у мережах мобільного зв’язку;
- аналіз проблемних місць у забезпеченні безпеки та способи їх подолання;
- розроблення методів підвищення інформаційної безпеки.

Отримані у ході виконання роботи дані пропонується застосовувати у мережах мобільного зв’язку для підвищення ефективності їх функціонування.

3 ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ МКР

Список використаних джерел розробки:

3.1 Габарчук В. Кибернетический подход *к* проектированию систем защиты информации / В. Габарчук, З. Зинович, А. Свиц – К.: Киев-Луцк-Любляны, 2003. – 653 с.

3.2 Одарченко Р.С. Обгрунтування основних вимог до систем безпеки стільникових мереж 5-го поколения. - Безпека информации. Віп №3 (Том 21) - 2015., С. 229-235

ВНТУ ФІРЕН ТКСТБ МКР 2019

3.3 Одарченко Р.С., Беженар Ю.В., Ксендзенко А.О. Аналіз вразливостей систем захисту інформації в Мережа Wi-Max та методів їх Усунення // Захист інформації. Зб. наукових праць.- К .: НАУ, 2011. - Вип. 18. - С. 39-44.

3.4 Щербаков В. Б Безопасность беспроводных сетей: стандарт IEEE 802.11. / В. Б. Щербаков, С. А. Ермаков - Москва : РадиоСофт, 2010. - 256 с.

3.5 Замула О. А. Застосування теорії нечітких множин та лінгвістичної невизначеності при оцінюванні ризиків інформаційної безпеки / О. А. Замула, В. І. Черниш, О. І. Аніщенко // Системи обробки інформації. - 2011. - Вип. 5. - С. 152-155.

3.6 Богдан В. П. Блокування засобів стільникового зв'язку і бездротового доступу / В. П. Богдан // Сучасна спеціальна техніка. - 2013. - № 1. - С. 100-107.

3.7 Пархоменко І. І. Проблеми захисту інформації в мережах мобільного зв'язку третього покоління / І. І. Пархоменко, Ю. О. Кривий. Наукоємні технології, 2009. № 3–4 (7–8). – с.77-80.

3.8 Москаленко А. О. Дослідження механізмів забезпечення інформаційної безпеки в існуючих та перспективних системах рухомого зв'язку А. О. Москаленко, О. В. Федін // Наука і техніка Повітряних Сил Збройних Сил України. - 2013. - № 1. - С. 99-103.

3.9 Кондрацький Ю.О. Дослідження криптостійкості алгоритму KASUMI на доступних високопродуктивних обчислювальних засобах / Ю.О. Кондрацький, С.А. Лупенко, А.М. Луцків. – Proceedings of the Second International Conference "Cluster Computing" CC 2013 (Ukraine, Lviv, June 3-5, 2013). – p. 101-104.

3.10 Корсунский А. С. Аутентификация корреспондентов в сетях UMTS при использовании псевдослучайных последовательностей Голда и Касами / А.С. Корсунский, О.В. Шейкина. – Автоматизация процессов управления. – 2010. – №2. – с. 40-47.

4 ВИКОНАВЕЦЬ

Вінницький національний технічний університет, кафедра телекомунікаційних систем та телебачення, студент групи ТТК-18м Вітюк Максим Олегович.

ВНТУ ФЛЕН ТКСТБ МКР 2019

5 ВИМОГИ ДО ВИКОНАННЯ МКР

Пропонується виконати обґрунтування методів підвищення інформаційної безпеки мобільних мереж.

Технічні вимоги, яким повинна відповідати розробка, наступні:

діапазон частот: 1920...2175 МГц,

довжина коду 20 і 50,

швидкість коду ½, ймовірність імітонав'язування не більше 10^{-9},

ймовірності прийому всього виклику не менше 0,95,

відношення сигнал/завада не менше 1,8дБ,

періодичність передачі пакету 100мс і 500мс,

розмір пакету 512 байт

6 ЕТАПИ МКР І ТЕРМІНИ ЇХ ВИКОНАННЯ

№	Назва та зміст етапу	Термін виконання		Очікувані результати	Звітна документа-ція
		початок	закінчення		
1	2	3	4	5	6
1.	Розробка технічного завдання (ТЗ)	02.09.2019р.	06.09.2019р.	Розроблене ТЗ	Додаток А
2.	Техніко-економічне обґрунтування тематики (ТЕО)	09.09.2019р.	13.09.2019р.	Розроблене ТЕО	Вступ. Розділ 1
3.	Дослідження особливостей захисту інформації	16.09.2019р.	04.10.2019р.	Результати досліджень	Розділ 2, 3

ВНТУ ФІРЕН ТКСТБ МКР 2019

1	2	3	4	5	6
4.	Розроблення системи ідентифікації користувача	07.10.2019р	25.10.2019р.	Схема структурна	Розділи 4
5.	Дослідження впливу завад	28.10.2019р.	08.11.2019р.	Результати досліджень	Розділ 5
6.	Аналіз економічної ефективності розробки	11.11.2019р.	15.11.2019р.	Економічна частина	Розділ 6
7.	Аналіз безпеки життєдіяльності (БЖД), цивільний захист (ЦЗ)	18.11.2019р.	22.11.2019р.	Частина БЖД, ЦЗ	Розділ 7
8.	Оформлення пояснювальної записки (ПЗ) та графічної частини	25.11.2019р.	29.11.2019р.	Оформлена документа-ція	ПЗ та графічна частина
9.	Попередній захист та рецензування МКР	02.12. 2019р.	06.12.2019р.	Позитивні відзиви	Відзив. Рецензія
10.	Захист МКР ДЕК		09.12. 2019р.	Позитивний захист	Протокол ДЕК

7 ОЧІКУВАНІ РЕЗУЛЬТАТИ ТА ПОРЯДОК РЕАЛІЗАЦІЇ МКР

В результаті виконання роботи будуть розроблені:

- структурна схема системи ідентифікації;
- структурна схема нейронної мережі;
- економічна частина МКР;
- розділ безпеки життєдіяльності і ЦЗ.

ВНТУ ФІРЕН ТКСТБ МКР 2019

Результати, отримані в процесі виконання даної роботи, будуть впроваджені в галузі телекомунікацій шляхом впровадження нових технологій.

Очікуваний техніко-економічний ефект. При впроваджені результатів досліджень очікується підвищення попиту на послуги зв'язку і, відповідно, підвищення їх якості.

8 МАТЕРІАЛИ, ЯКІ ПОДАЮТЬ ПІСЛЯ ЗАКІНЧЕННЯ РОБОТИ ТА ПІД ЧАС ЕТАПІВ

За результатами виконання МКР до ЕК подаються пояснювальна записка, графічна частина МКР, відзив і рецензія.

9 ПОРЯДОК ПРИЙМАННЯ МКР ТА ЇЇ ЕТАПІВ

Поетапно результати виконання МКР розглядаються керівником роботи та обговорюються на засіданні кафедри.

Захист магістерської кваліфікаційної роботи відбувається на відкритому засіданні ЕК.

10 ВИМОГИ ДО РОЗРОБЛЮВАНОЇ ДОКУМЕНТАЦІЇ

Документація, що розробляється в процесі виконання досліджень повинна містити:

- техніко-економічне обґрунтування розробки;
- структурну схему системи ідентифікації;
- структурну схему нейронної мережі;
- економічну частину та розділ БЖД і ЦЗ;
- рекомендації щодо подальшого використання отриманих результатів.

11 ВИМОГИ ЩОДО ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

У зв'язку з тим, що інформація не є конфіденційною, заходи з її технічного захисту не передбачаються.

ВНТУ ФІРЕН ТКСТБ МКР 2019

Додаток Б

(обов’язковий)

Схема моніторингу загроз

Плакат

ВНТУ ФІРЕН
ТКСТБ МКР 2019

Додаток В

(обов’язковий)

Генератор псевдовипадкової бітової послідовності

Структурна схема

ВНТУ ФІРЕН
ТКСТБ МКР 2019

Додаток Д

(обов’язковий)

Система ідентифікації

Схема структурна

ВНТУ ФІРЕН
ТКСТБ МКР 2019

Додаток Е

(обов’язковий)

Нейронна мережа

Структурна схема

ВНТУ ФІРЕН
ТКСТБ МКР 2019

Додаток Ж

(обов’язковий)

Дискретно-неперервний канал

Схема структурна

ВНТУ ФІРЕН
ТКСТБ МКР 2019

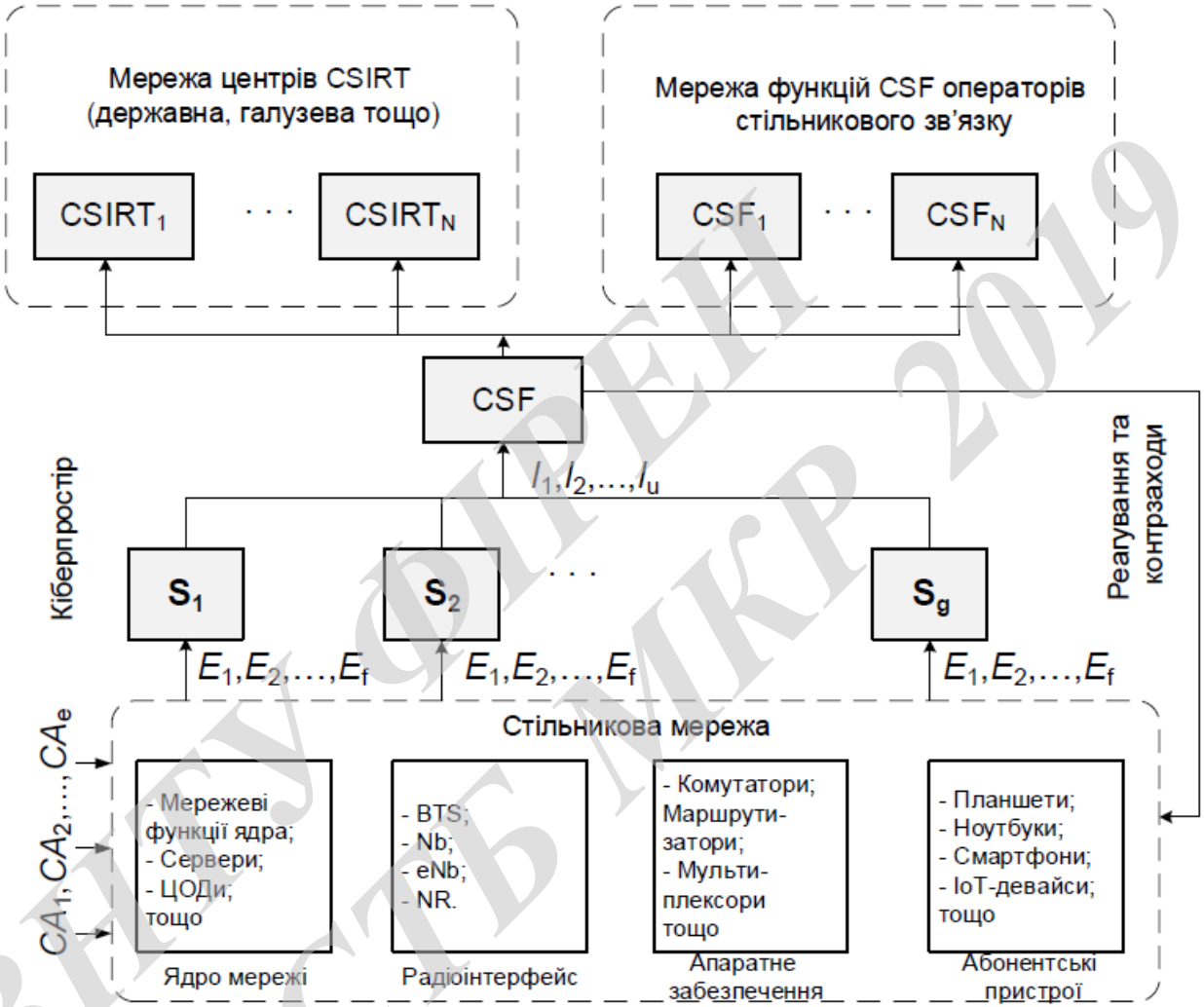
Додаток И

(обов’язковий)

Дослідження пропускної здатності

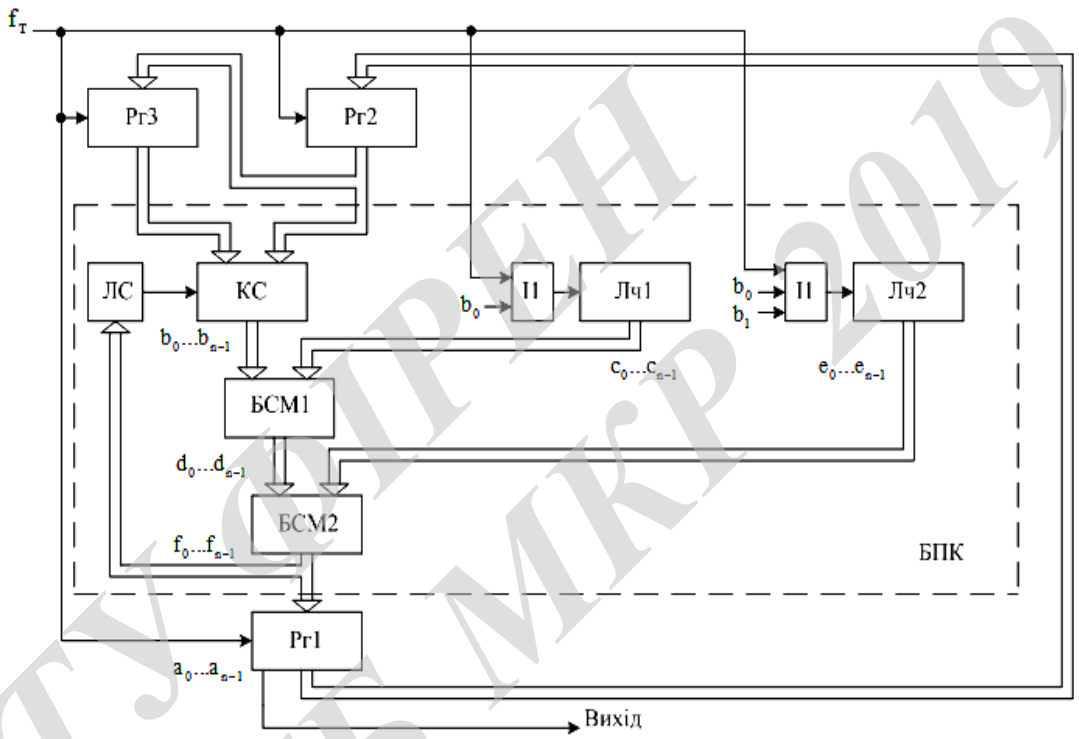
Плакат

ВНТУ ФІРЕН
ТКСТБ МКР 2019



ВНТУ ФІРЕН
ТКСТБ МКР 2019

					08-34.МКР.002.00.001 Е8		
Змн.	Лист.	№ докум.	Підпис	Дата	Схема моніторингу загроз Плакат	Літ.	Маса	Масштаб
Розроб.		Вітюк М.О.						
Перевір.		Семенова О.О.				Арк. 1	Аркушів 1	
Т.Контр.								
Реценз.								
Н.Контр.		Семенова О.О.				ВНТУ, ТТК-18м		
Затверд.		Бортник						

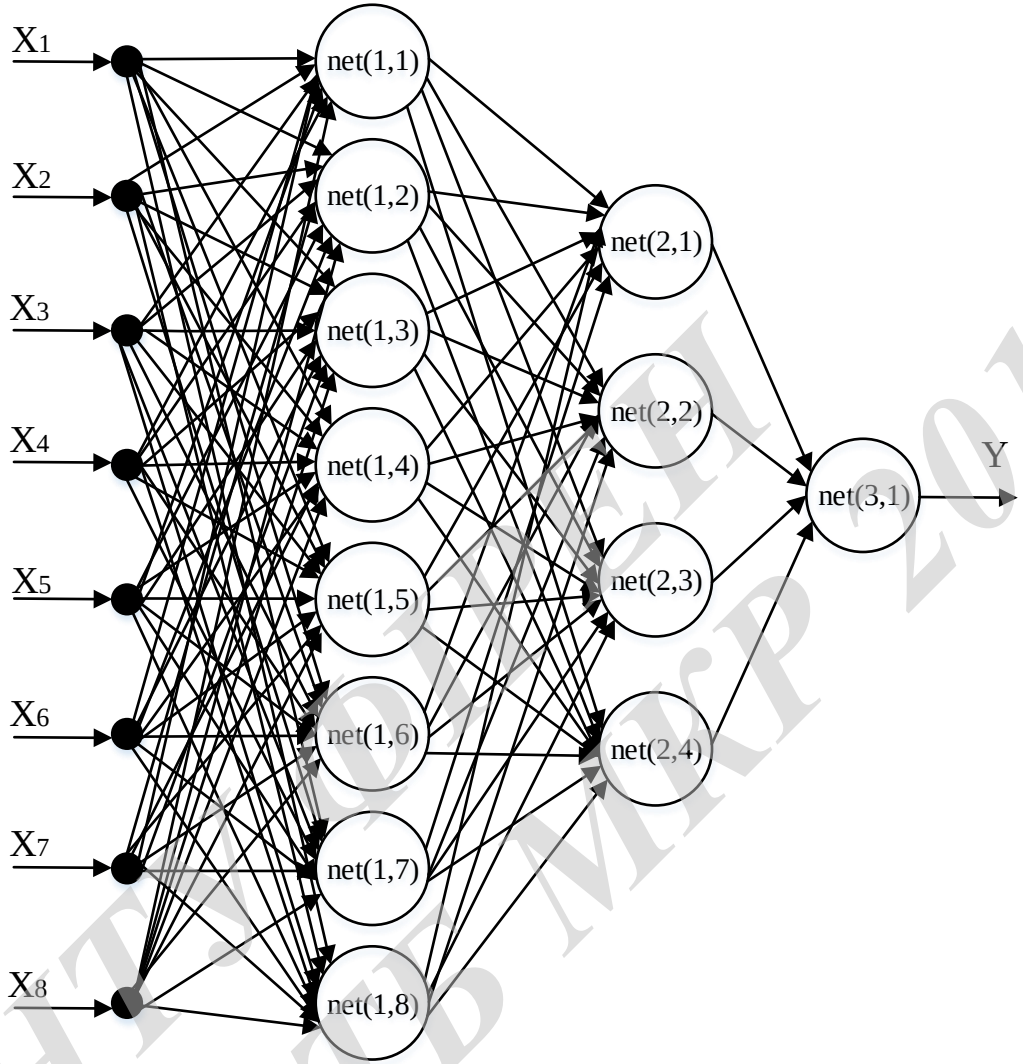


ВНТУ ОПРЕН ТКСТБ МКР 2019

					08-34.МКР.002.00.001 Е1			
Змн.	Лист	№ докум.	Підпис	Дата	Генератор псевдовипадкової бітової послідовності Структурна схема	Літ.	Маса	Масштаб
Розроб.		Вітюк М.О.						
Перевір.		Семенова О.О.				Арк. 1	Аркушів 1	
Т.Контр.								
Реценз.								
Н.Контр.		Семенова О.О.				ВНТУ, ТТК-18м		
Затверд.		Бортник						

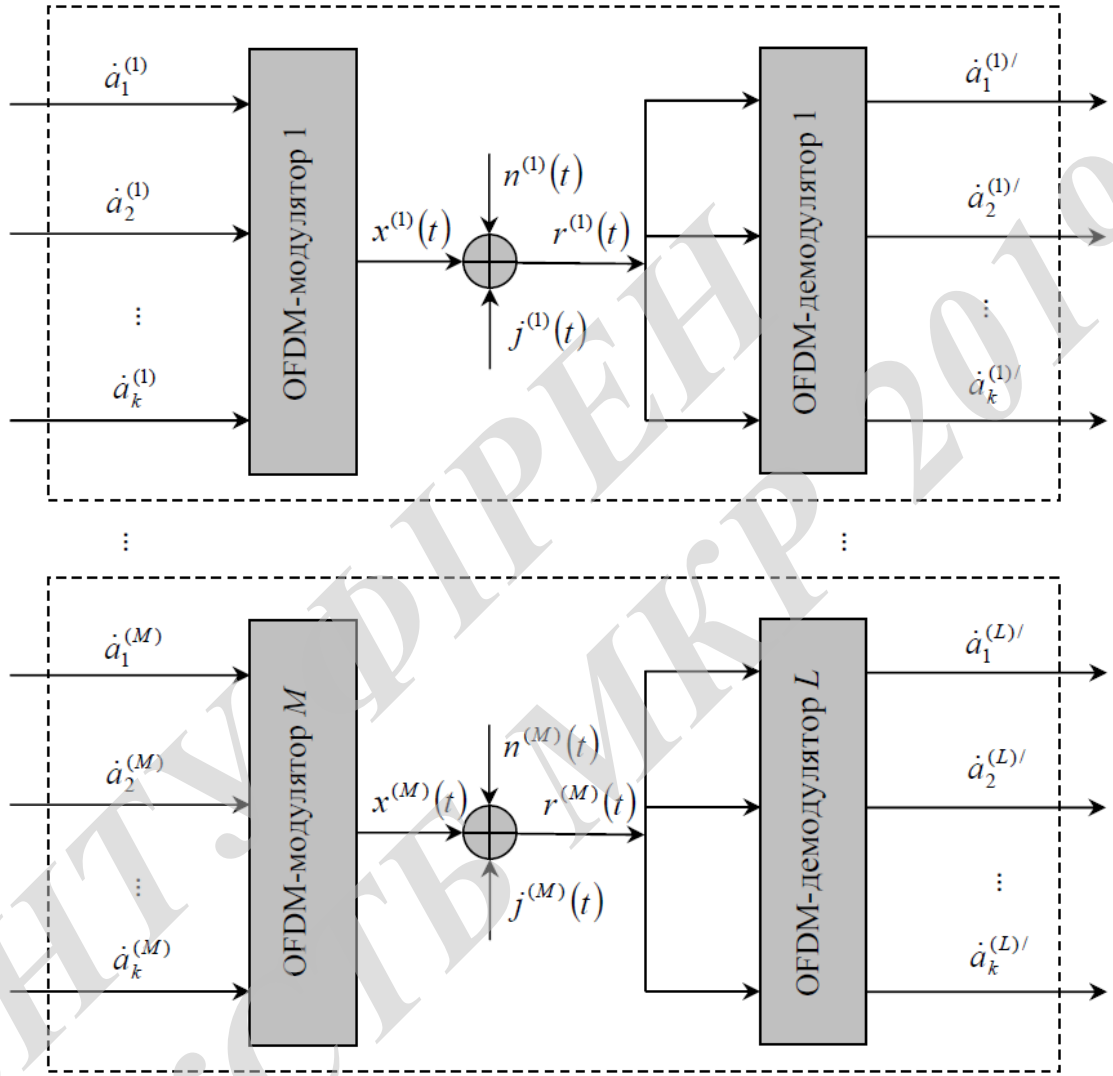
ВНТУ ФІРЕН ТКСТБ МКР 2019

					08-34.МКР.002.00.004 Е1			
Змн.	Лист.	№ докум.	Підпис	Дата	Система ідентифікації Схема структурна	Літ.	Маса	Масштаб
Розроб.		Вітюк М.О.						
Перевір.		Семенова О.О.				Арк. 1	Аркушів 1	
Т.Контр.								
Реценз.								
Н.Контр.		Семенова О.О.				ВНТУ, ТТК-18м		
Затверд.		Бортник						



ВНТУ, кафедра ТКСТВ МКР 2019

					08-34.МКР.002.00.003 Е1			
Змн.	Лист	№ докум.	Підпис	Дата	Нейронна мережа Структурна схема	Літ.	Маса	Масштаб
Розроб.		Вітюк М.О.						
Перевір.		Семенова О.О.				Арк. 1	Аркушів 1	
Т.Контр.								
Реценз.								
Н.Контр.		Семенова О.О.				ВНТУ, ТТК-18м		
Затверд.		Бортник						



ВНТУ, ТКСТБ МКР 2019

					08-34.МКР.002.00.002 Е1		
Змн.	Лист	№ докум.	Підпис	Дата	Дискретно-неперервний канал Схема структурна	Літ.	Маса / Масштаб
Розроб.		Вітюк М.О.					
Перевір.		Семенова О.О.				Арк. 1	Аркушів 1
Т.Контр.							
Реценз.							
Н.Контр.		Семенова О.О.				ВНТУ, ТТК-18м	
Затверд.		Бортник					

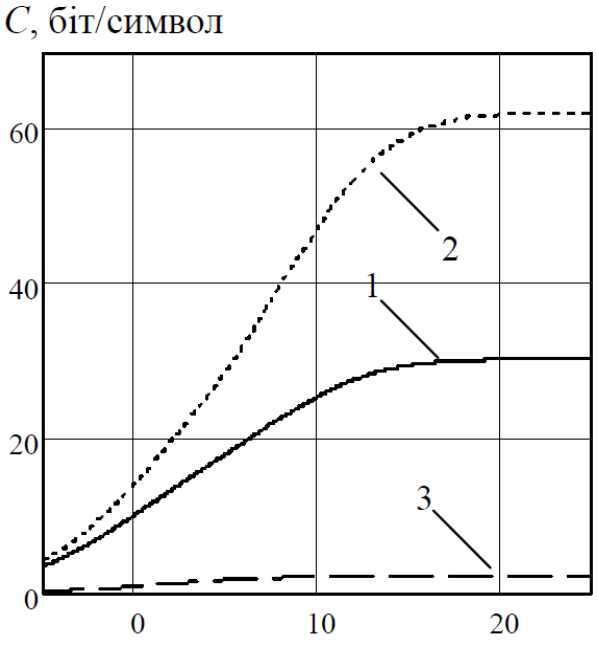


Рисунок 1 – Залежність пропускної здатності каналу від співвідношення сигнал/шум при впливі шумової завади в частині смуги та шуму на систему MIMO-OFDM (крива 1), при впливі лише шуму на систему MIMO-OFDM (крива2) та на систему MIMO із сигналами ФМ-2 (крива 3)

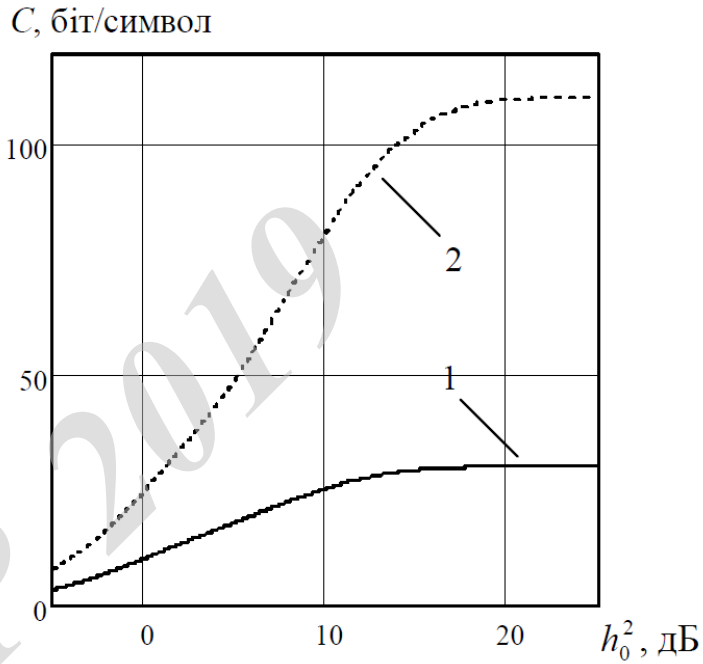


Рисунок 2 – Залежність пропускної здатності каналу від співвідношення сигнал/шум при впливі шумової завади в частині смуги та шуму на систему OFDM -MIMO 2×2 (крива1) та OFDM MIMO 4×4 (крива 2)

ВНТУ ФІРЕН ТКСТБ МКР 2019

					08-34.МКР.002.00.002 Е8			
Змн.	Лист.	№ докум.	Підпис	Дата	Дослідження пропускної здатності Плакат	Літ.	Маса	Масштаб
Розроб.		Вітюк М.О.						
Перевір.		Семенова О.О.				Арк. 1	Аркушів 1	
Т.Контр.								
Реценз.						ВНТУ, ТТК-18м		
Н.Контр.		Семенова О.О.						
Затверд.		Бортник						