МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Інститут інформатики та радіоелектроніки, факультет радіоелектроніки та телекомунікації
(повне найменування інституту, факультету)

Кафедра Захисту інформації
(повне найменування кафедри)

Пояснювальна записка

до магістерської роботи

на тему: Аналіз захищеності мереж мобільного зв'язку

Виконав: студент 2 курсу, групи РТ-719М

Спеціальності 125 Кібербезпека
(код і найменування спеціальності)

Освітня програма (спеціалізація)
Системи технічного захисту інформації, автоматизація її обробки

Хемішінець Є.В.
(прізвище та ініціали)

Керівник Воскобойник В.О.
(прізвище та ініціали)

Рецензент
(прізвище та ініціали)

2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет Запорізька політехніка»

(повне найменування закладу вищої освіти)

Інститут, факультет: Інститут інформатики та радіоелектроніки, Факультет радіоелектроніки та телекомунікацій

Кафедра: Захисту інформації

Ступінь вищої освіти: магістр

Спеціальність: 125 Кібербезпека

(код і найменування)

Освітня програма (спеціалізація): Системи технічного захисту інформації, автоматизація її обробки

(назва освітньої програми (спеціалізації)

ЗАТВЕРДЖУЮ

Завідувач кафедри Карпуков Л.М.,

докт. техн. наук, професор

«02» 09 20 20 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТА

Хемішінець Євгеній Віталійович

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Аналіз захищеності мереж мобільного зв'язку

керівник проекту (роботи) Воскобойник Володимир Олександрович, канд. техн. наук, доцент

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом закладу вищої освіти від «06»листопада 2020року №314

2. Строк подання студентом проекту (роботи)24 грудня 2020 року

3. Вихідні дані до проекту (роботи): Аналіз захищеності мереж мобільного зв'язку. Література по темі.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):

1. Аналіз основних загроз безпеки в мережах мобільного зв'язку.
2. Аналіз безпек і небезбек в стільникових мережах.
3. Аналіз перспектив розвитку безпеки в мережал зв'язку

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень):
5 рисунків; 11 таблиць; презентація магістерської роботи

6. Консультанти розділів проекту (роботи):

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	Прийняв виконане завдання
Основні розділи	Воскобойник В.О., доцент		
Розділ з ОП і НС	Якімцов Ю.В., доцент		
Розділ з економіки	Круглікова В.В., доцент		
Нормоконтроль	Корольков Р.Ю., старший викладач	15.01.2021	

7. Дата видачі завдання «01»вересня 2020року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Складання та затвердження ТЗ	06.09-11.09	Виконано
2	Підбір літератури	11.09-15.09	Виконано
3	Огляд основних загроз безпеки в мережах SS7 мобільного зв'язку	15.09-30.09	Виконано
4	Аналіз безпеки і вразливостей в стільникових мережах	01.10-27.10	Виконано
5	Розгляд перспектив розвитку безпеки в мережах мобільного зв'язку	28.10-10.11	Виконано
6	Економічна частина	10.12-12.12	Виконано
7	Охорона праці	12.12-14.12	Виконано
8	Оформлення пояснювальної записки	14.12-20.12	Виконано
9	Оформлення графічної частини	20.12-24.12	Виконано

Студент _____ Хемішінець Є.В.
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ Воскобойник В.О.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

ПЗ: 71 сторінка, 5 рисунків, 11 таблиць, 41 джерело.

Актуальність дослідження. За допомогою вразливостей SS7 зловмисник з будь — якої точки планети може перетворити чужий телефон у відкриту книгу – перехопити SMS-повідомлення, виявити місцеположення і виконати інші нелегітимні дії. Ця техніка доступна не тільки спецслужбам, а й хакерам середньої кваліфікації.

Тема роботи – аналіз захищеності мереж мобільного зв'язку.

Об’єкт дослідження – мережі мобільного зв’язку.

Мета дослідження – визначення рівня захищеності мереж мобільного зв'язку.

БАЗОВІ СТАНЦІЇ, ЗАХИСТ ВІД НСД, ЗАХИЩЕННІСТЬ МОБІЛЬНОГО ЗВ’ЯЗКУ, ЗВ’ЯЗОК НОВОГО ПОКОЛІННЯ, МОБІЛЬНІ МЕРЕЖІ, СТІЛЬНИКОВІ МЕРЕЖ

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

GSM – Global System for Mobile Communications (Глобальна система мобільного зв'язку)

IMEI – International Mobile Equipment Identity (Міжнародний ідентифікатор мобільного обладнання)

IP – Internet Protocol (Інтернет протокол)

LTE – Long Term Evolution (Довготерміновий розвиток)

SS7 – Signalling System (Система сигналізації)

MAC – Media Access Control (Управління доступом до посередників)

MAP – Mobile Application Part (Підсистема мобільних додатів)

MIMA – Man in the Middle Attack (Людина посередині)

SIM – Subscriber Identification Module (Модуль ідентифікації абонента)

SMS – Short Message Service (Служба коротких повідомлень)

UMTS – Universal Mobile Telecommunications System (Універсальна мобільна телекомунікаційна система)

ВСТУП

Розроблена в 70-х роках минулого століття система SS7 містить певні недоліки в плані захищеності: відсутні, наприклад, шифрування і перевірка справжності службових повідомлень. Довгий час це не представляло небезпеки ні для абонентів, ні для оператора, — мережа SS7 була замкнутою системою, в яку підключалися тільки оператори фіксованого зв'язку. Однак час іде, мережа еволюціонувала для підтримання потреб мобільного зв'язку та надання додаткових послуг на початку 2000-х була запропонована специфікація SIGTRAN, що дозволила передавати службову інформацію SS7 по IP-мережах. Сигнальна мережа перестала бути ізольованою [1].

Перші публічні демонстрації вразливостей SS7 відбулися в 2008 році: німецький дослідник Тобіас Енгель показав техніку стеження за абонентами мобільних мереж. У 2015 році фахівці SR Labs в ефірі австралійської програми «60 хвилин», будучи в Німеччині, перехоплювали SMS-листування австралійського сенатора Ніка Ксенофонта і британського журналіста, а потім спостерігали за пересуваннями сенатора у відрядженні в Токіо з точністю до базової станції [2].

По інформації компанії Bloomberg, послуги які можуть вистежучі користувачив за допомогою SS7 пропонують дві компанії Defentek і Verint Systems. Експерти розуміли про ці недоліки задовго до того. В Адміністрації Президента США були занепокоїні ними у 2000 році. Про такі ж самі пропозиції зі сторони ізраїльської CleverSig і болгарської Circles говорили в витеклому листуванні Hacking Team. По інформації Брюса Шнайера, компанія Cobham продає більше 10 країнам систему, яка дозволяє визначити місце розташування будь-якого стільникового телефону з дуже високою точністю. Доля стеження через SS7 набирає більших оборотів, і відповідні ідеї все частіше ми бачимо на хакерських форумах [3].

Принаявності доступу до SS7 і знаючи номер телефону нашої жертви, можемо підслухати розмову, визначити точне місце розташування, перехопити SMS для доступу до Мобільного банку, відправити USSD-запит на платний номер та здійснити багато інших атак [3].

На чорному ринку є багато прикладів придбати повний доступ до мережі оператора за декілька тисяч доларів. Але звичайно, безпосередньо потрапити в сигнальну мережу буде неможливим. Для підключення потрібно знайти SS7-шлюз. У деяких країнах зв'язку можна і зовсім оформити ліцензію оператора навіть офіційно. Також, фахівець компанії-оператора може можливість виконувати ніску атак за допомогою легітимного набору команд або підключити до SS7 спеціальне обладнання. Існують інші методи потрапити в мережу через зламане операторське обладнання [3].

Оператори не мають можливість блокувати команди з окремих вузлів, це робить негативний вплив на сервіс і спричиняє до порушення принципів функціонування роумінгу. Атаки за допомогою SS7 можна виконувати з будь-якого місця на планеті, це робить метод одним з найперспективнішим для порушника. Злодію не потрібно фізично находитися поруч з абонентом, як у випадку з підробленою базовою станцією, тому вичислити його дуже складно, практично неможливо. Висока кваліфікація також не обов’язкова – в мережі багато готових додатків для роботи з SS7. При цьому оператори не мають змоги блокувати команди з окремих вузлів, це робить негативний вплив на весь сервіс і порушує принципи функціонування та роботи роумінгу [3].

За допомогою команд SS7 MAP можна на відстані розблокувати стільникові телефони. Слабка захищеність SS7 загрожує при цьому не тільки користувачам мобільних телефонів, але екосистемі промислових і IoT-пристроїв, банкоматів, GSM-систем контролю за роботою промислових станцій і т.д [3].

Недоліки сигнальних мереж дозволяють здійснювати найрізноманітніші атаки. У подібних обставинах забезпечення безпеки мереж SS7-одне з основних завдань при побудові системи захисту мобільного зв'язку [3].

Предметом дослідження є аналіз захищеності мереж мобільного зв'язку.

Завдання дослідження обумовлені поставленою метою і виглядають наступним чином:

- розглянути основні загрози безпеки в мережах SS7 мобільного зв’язку;
- проаналізувати вимоги з безпеки в бездротових мережах;
- провести класифікацію атак на мережі мобільного зв’язку;
- зробити аналіз існуючих методів вирішення проблем уразливості GSM;
- розглянути еволюцію та перспективи розвитку безпеки в мережах мобільного зв'язку;
- провести діагностику потреб інвестування досліджень з захищеності мереж мобільного зв’язку;
- розглянуті основні питання охорони праці та безпеки у надзвичайних ситуаціях.

Структура роботи відповідає меті та завданням дослідження. Робота включає вступ, п’ять основних розділів, висновок та список використаних джерел.

1 ОСНОВНІ ЗАГРОЗИ БЕЗПЕКИ В МЕРЕЖАХ SS7 МОБІЛЬНОГО ЗВ'ЯЗКУ

1.1 Характеристика загроз безпеки SS7 мобільного зв’язку

Для детального порівняльного аналізу були обрані результати 8 проектів з максимально великим обсягом перевірок. Експерти відділу безпеки компанії Positive Technologies в 2015 році здійснили 16 проектів з аналізу захищеності мереж SS7 мобільного зв'язку. Такі роботи проводилися для мереж провідних операторів регіонів EMEA і APAC [3].

За допомогою спеціальних програмних інструментів було проведено інструментальне сканування мережі SS7 для перевірки. В ході проведення робіт з аналізу захищеності мереж, були змодельовані дії зовнішнього порушника, який атакує з міжнародної або національної сигнальної мережі:

– можливість атаки на абонентів мобільного оператора.
– фільтрування сигнальних повідомлень та пов'язаних недоліків;
– можливість виконати атаку на вузли мережі сигналізації [3].

Фахівці брали до уваги модель порушника, який діє із-зовні по відношенню до сигнальної мережі і здійснює атаки, які базуються на проходженні запитів різних протоколів рівня додатків (MAP, CAP) в мережу оператора [3].

В ході аналізу захищеності, всі дані які були призначені для підвищення рівня захищеності мобільних сервісів та пониження ризиків порушення доступності мережі [3].

Результати проведеного дослідження дозволяють зробити наступні основні висновки:

– всі мережі SS7 вразливі;
– особисті дані абонентів під загрозою;
– мережі SS7 схильні до вразливостей, які може з успіхом для себе використати злодій. Як приклад, відмова в обслуговуванні окремого абонента

була здійснена близько у 80% випадків. Загрози, пов'язані з шахрайством, включаючи викрадення грошей з рахунків користувачів, були реалізовані в 67% випадків;

– мережі регіону EMEA менш захищені;

– у всіх мережах SS7, була можлива крадіжка інформації про абонента і перехоплення SMS;

– великі оператори не гарантують максимальний захист;

– невеликі оператори мобільного зв'язку гірше захищені від атак з боку зовнішнього порушника. Однак навіть найбільші в своїх регіонах оператори не можуть забезпечіті безпеку своїх абонентів: частина успішних атак була велика [3].

Загрози з боку порушника на мережі SS7 і абонентів мобільних операторів можна розділилити на три класи:

– збої в роботі.

– шахрайство;

– витік чутливої інформації;

Вони чреваті для оператора фінансовими втратами та зіпсованою репетуцією [3].

1.2 Витік інформації

Несанкціонований переказ грошових коштів з рахунків користувачів, переадресація викликів або внесення змін в профілі абонентів. Шахрайством в даних випадках вважалися всі неправомірні дії порушника [3].

Під витоком інформації йде мова про розголошення, перехоплення або розкрадання даних про користувачів оператора або даних про конфігурацію мережі SS7. Сюди відносять визначення місця знаходження абонентів, прослуховування переговорів, читання SMS [3].

Збої в роботі – атаки, спрямовані на відмову в обслуговуванні самої мережі SS7 або супутніх її сервісів [3].

Реалізувати перераховані загрози дозволяють уразливості і помилки конфігурації мережевого обладнання і використовуваного на ньому програмного забезпечення. Знайдені недоліки можна розділити на такі типи:

– неможливість перевірки до приналежності користувача мережі;

– відсутність перевірки місця розташування користувача;

– відсутність фільтрації невикористовуваних сигнальних повідомлень;

– недоліки конфігурації Home Routing.

SMS Home Routing – комплекс, який забезпечує функціювання проксування конфіденційних абонентських адресів обладнання під час прийому SMS-повідомлень [3].

Експлуатація названих вразливостей може призводити до реалізації різних класів загроз. У разі успішних атак з використанням вразливостей, які пов’язані з неможливістю перевірки приналежності користувача мережі, порушник може як визначати поточне місце розташування абонента, або перенаправляти його вихідні дзвінки на платний номер [3].

Наступні недоліки можна оцінити в більшості випадків як критично небезпечні. На одну мережу SS7 припадає понад 10 успішних атак, пов'язаних з експлуатацією вразливостей типу «відсутність перевірки реального місця розташування абонента». З них більше 3 успішних спроб експлуатації вразливостей може бути викликані неможливістю перевірки приналежності користувача до мережі [3].

Вище названі недоліки в загальному випадку можуть класифікуватися як вразливості конфігурації. Проблеми протоколів і систем (неможливість перевірки приналежності абонента мережі і відсутність перевірки реального місця розташування абонента) або як помилки в ПЗ яке використовується (до таких помилок відносять недолік, пов'язаний з відсутністю перевірки поточного місця знаходження користувача) [3].

У разі знаходження та розголошення інформації про інциденти з перерахуванням вразливостей в конкретній мережі оператор може втратити репутацію [3].

Щоб усунути недоліки кожної з категорій необхідно використати відповідний підхід. Це може бути як застосування додаткових технічних і програмних засобів захисту, так і внесення змін в налаштування систем [3].

Як зазначалося вище, загроза витоку інформації пов'язана з отриманням порушником будь-яких даних про абонентів операторів або інформації про налаштування мережі SS7. У загальному випадку реалізація таких загроз не несе збитку операторам зв'язку [3].

Загрози ІБ, які відносяться до даного класу:

– інформації про баланс користувача;
– крадіжка інформації абонента.
– перехоплення SMS-повідомлень;
– визначення реального місця находження абонента [3].

Для отримання даних абонентів мобільних мереж використовують, спеціально сформовані повідомлення наступних типів:

– SendRoutingInfoForLCS;
– SendRoutingInfo;
– Send IMSI.
– SendRoutingInfoForSM [3].

Використовуючи наступний метод, порушник може отримати інформацію про абонента, і визначити його реальне місце розташування. Метод SendRoutingInfo засновується на використанні недоліку, пов'язаного з відсутністю фільтрації невикористовуваних сигнальних повідомлень. SendRoutingInfo-повідомлення протоколу MAP, яке використовується при вхідному голосовому виклику і служить для запиту маршрутної інформації для локалізації абонента. При адекватному режимі функціонування це повідомлення повинно передаватися тільки між елементами своєї мережі [3].

SendRoutingInfoForSM-повідомлення має маршрутизуватися на обладнання SMS Home Routing, якщо воно встановлено в мережі оператора протоколу MAP, яке використовується при вхідному SMS-повідомленні і використовується для запиту маршрутної інформації для локалізації абонента-одержувача [3].

Кожна п’ята атака зловмисника з використанням цього методу виявилася успішною. SendlMSI-повідомлення протоколу MAP, яке використовується для запиту ідентифікатора IMSI абонента за його телефонним номером. Зараз час дане повідомлення практично не використовується операторами мобільного зв'язку, проте обладнання часто все ж обробляє його, відповідно до стандарту 3gpp [3].

Порушник може використовувати і інші методи атак з метою отримання інформації про місцезнаходження абонента, наприклад представлені нижче [3].

ProvideSubscriberInfo-повідомлення протоколу MAP, використовується для отримання інформації про місцезнаходження абонента. Не допускається проходження запитів з боку зовнішніх підключень на абонентів своєї мережі [3].

SendRoutunglnfoForLCS-повідомлення протоколу MAP, використовується в сервісах, що задіюють місце розташування абонента, і служить для запиту маршрутної інформації [3].

AnyTimelnterrogation-повідомлення протоколу MAP, використовується вузлами, які реалізують логіку інтелектуальних послуг, для запиту місця розташування абонента [3].

Коли при прослуховуванні вхідних викликів здійснюється атака, заснована на застосуванні методу підміни роумінгового номера з перекладом трафіку на інший комутатор [3].

InsertSubscriberData-повідомлення протоколу MAP, воно виконується для того, щоб змінити профіль абонента в базі даних VLR. Нападник має можливість замінити в профілі значення платформи для тарифікації викликів

на своє обладнання. У момент вихідного виклику мобільний комутатор відправить запит на продовження виклику на вказану зловмисником адресу [3].

Щоб перехопити вхідні SMS використовується метод UpdateLocation. UpdateLocation-повідомлення, яке використовується для запиту реєстрації в зоні дії нового мобільного комутатора (це повідомлення приходить, зокрема, з мережі роумінг-партнера, коли абонент намагається провести там реєстрацію). Шахрай має можливість зареєструвати користувача у несправжній мережі, після чого всі вхідні SMS приходять на вказану злодієм адресу [3].

1.3 Шахрайство та збої в роботі

Більшість мереж SS7 в тій чи іншій мірі схильні до недоліків, що дозволяє проводити атаки, спрямовані на відмову в обслуговуванні окремих абонентів [3].

Заміна номера здійснюється в момент виклику на атакованого користувача. Заздалегідь атакований повинен бути зареєстрований у фальшивій мережі. У відповідь на запит мобільного номера шахрай відправляє номер для перенаправлення виклику. Плата за встановлене з'єднання буде на операторі оператора [3].

Для того щоб перенаправити вихідні дзвінки застосовувався метод InsertSubscriberData. А атаки з метою перенаправлення вхідних викликів здійснюють за допомогою методів — підміни роумінгового номера і шахрайських дій з переадресацією [3].

У всіх, без виключення, системах можна виявити недоліки, котрі дозволяють реалізовувати злочинні плани з боку порушника. Такі дії служать для перенаправлення викликів, переказу грошових коштів з електронних гаманців абонентів або зміна профілю користувача [3].

Маніпуляція з переадресацією – неправомірна установка переадресації. Всі вхідні дзвінки будуть перенаправлятися на встановлений злочинцем номер, а плата за них буде на абоненті [3].

Метод UpdateLocation. У ході атаки на відказ в обслуговуванні абонента шахрай може викликати збої в роботі мережі для деяких абонентів мобільного оператора, порушення доступності або погіршення якості надання послуг для абонентів не відбувається. Таким чином порушник може проводити спрямовані напади [3].

2 АНАЛІЗ РІЗНИХ ВИДІВ БЕЗПЕКИ І ВРАЗЛИВОСТЕЙ В СТІЛЬНИКОВИХ МЕРЕЖАХ

2.1 Вимоги безпеки в бездротових мережах

Бездротовий мобільний зв'язок процвітає протягом останніх десятиліть. А мобільні технології – це еволюціонуюча концепція. Світ бачив різні покоління мобільних технологій, тобто 1-4G або, іншими словами, бездротовий мобільний зв'язок пережив феноменальне зростання, тобто спочатку вся бездротова система була заснована на комутації каналів, але сьогодні всі послуги голосового зв'язку та обміну повідомленнями засновані на комутації пакетів з використанням інтернет-протоколу (IP) [4]. Через легку доступність і велику зону покриття мобільний зв'язок приваблював багатьох користувачів, а також постачальників послуг. Однак, незважаючи на ряд переваг, завдяки широкому характеру інформація передається повітрям в якості засобу передачі, в результаті чого інформація, передана за допомогою радіопередачі, доступна як авторизованим, так і неавторизованим користувачам, оскільки через цю відкриту архітектуру мобільний зв'язок стикається з різними проблемами безпеки. Крім того, бездротовий зв'язок більш вразливий до шкідливих атак, ніж дротовий зв'язок.

Використання стільникових мобільних мереж і засобів зв'язку в нашому повсякденному житті зростає з кожним днем. В наші дні люди використовують свої смартфони, а також високошвидкісний інтернет для того, щоб займатися електронною комерцією, а також ділитися своєю конфіденційною інформацією, такою як паролі і багатьма іншими особистими даними в стільникових мережах. Цей обмін особистою інформацією приваблює хакерів, а також підслуховуючих осіб для здійснення різних кіберзлочинних дій.

Тому першорядну увагу слід приділяти боротьбі з такою незаконною діяльністю і зробити стільникову мережу більш надійною і надійною. У цьому

досліджені представлені різні проблеми безпеки, що існують у різних поколіннях стільникового зв'язку, тобто від 2 до 4g.

Вимоги безпеки в бездротових мережах є дуже важливими для забезпечення надійного зв'язку. Для підвищення надійності і забезпечення надійності необхідно виділити різні вимоги щодо підвищення якості обслуговування і забезпечення кращої безпеки (Рис. 2.1).

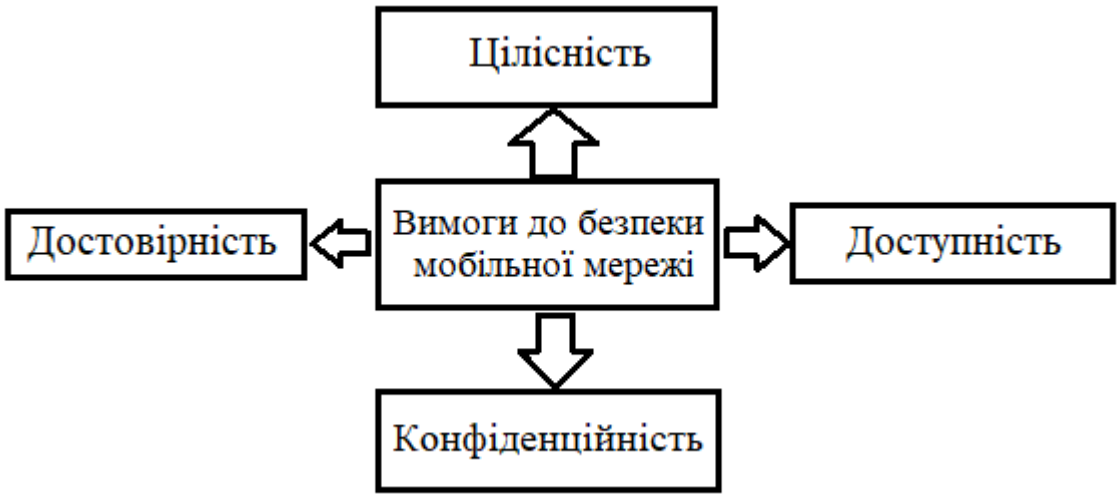

Рисунок 2.1 – Вимоги безпеки

Аутентичність (достовірність): простіше кажучи, вона включає в себе підтвердження особистості, щоб відрізнити авторизованого користувача від нелегітимного користувача. Перш ніж будь-якому користувачеві буде надано доступ до каналів, облікові дані, надані в момент запиту на доступ до каналу, вони порівнюються з обліковими даними, що зберігаються в базі даних. Якщо облікові дані збігаються, доступ надається, в іншому випадку відмова.

Конфіденційність. Цей принцип гарантує, що конфіденційні дані користувачів повинні бути розкриті тільки авторизованим користувачам, запобігаючи при цьому розкриття інформації неавторизованим. Дуже важливим компонентом захисту конфіденційності інформації є шифрування даних перед їх передачею. Останнім часом безпека фізичного рівня

використовується як засіб захисту даних від таких атак, як підслуховування [5,6].

Цілісність: оскільки інформація має свою цінність тільки тоді, коли вона правильно передана. Іншими словами, підроблена інформація може виявитися більш дорогою. Таким чином, цілісність означає захист інформації від будь-якого спотворення або зміни неавторизованими користувачами. Вона включає в себе підтримку послідовності, точності і достовірності даних. Криптографічні контрольні суми використовуються для перевірки цілісності даних.

Доступність: це стосується здатності користувача отримувати доступ до ресурсів у будь-який час і в будь-якому місці без будь-яких перерв. Виклик доступності, також відомий як DoS. DoS-це тип активної атаки, при якій будь-якому авторизованому користувачеві відмовляють у доступі до ресурсів, що призводить до незадовільної реакції користувача [7,8,9].

2.2 Класифікація атак на мережі мобільного зв’язку

Типи атак: відкрите середовище бездротової системи зв'язку робить її схильною до різних атак. Атаки можуть бути широко класифіковані за двома типами. Активні і пасивні атаки. Кожний з цих видів нападів коротко пояснюється нижче.

Пасивна атака: пасивна атака – це вид атаки, при якому зловмисник безперервно контролює систему, щоб перевірити відкриті порти і сприйнятливість. Такі атаки здійснюються з єдиною метою збору інформації. Щоб запобігти таким атакам, зловмисник постійно прослуховує весь трафік, що проходить через бездротову мережу. Хоча природа цих атак мовчазна і їх важко виявити, але ці атаки можуть бути використані для активних атак.

Активні атаки: активна атака – це мережевий експлойт, при якому зловмисник не тільки прослуховує інформацію, передану авторизованими

користувачами, але і завдає шкоди цілісності системи, тобто намагається внести зміни в передані дані. Різні типи активних атак описані нижче.

Атака «людина посередині» (MIMA): ця атака дозволяє віддаленим зловмисникам підробляти/реплікувати базову станцію. MIMA – це активна атака, в якій зловмисник підслуховує незалежне з'єднання жертв і ретранслює повідомлення між ними. Припустимо, що у користувача є TCP-з'єднання, зловмисник роздвоює це з'єднання, тобто він буде діяти як загальний вузол для обох з'єднань шини. Таким чином, будуть встановлені два з'єднання: перше з'єднання буде від першого користувача до атакуючого, а друге-від атакуючого до іншого користувача. Таким чином, вся інформація, яка буде передана між двома користувачами, буде проходити через зловмисника. Тому зловмисник може легко вкрасти інформацію, що проходить між ними. Сценарій MIMA показаний на рис. 2.2.

Рисунок 2.2 – Сценарій атаки MIMA

DoS: ця атака є явною спробою зловмисника і здійснюється для того, щоб перешкодити законним користувачам використовувати сервіси. DoS-атаки можуть бути в основному класифіковані на два типи: перешкодова і флуд-атака.

Перешкодова: в бездротовій мережі ця атака здійснюється з метою викликати збої в передачі даних між авторизованими користувачами. Перешкодова атака здійснюється шляхом випускання непотрібних радіосигналів. Щоб перервати передачу даних, глушник безперервно передає сигнали по загальному бездротовому каналу, і ця безперервна передача викликає великі втрати енергії, тому можна зробити висновок, що глушіння не є енергоефективним. Тому, щоб підвищити свою ефективність, глушник передає інтерферуючий сигнал тільки тоді, коли він виявляє авторизований активний передавач. Залежно від роботи каналів глушники можна розділити на п'ять типів: [10].

– реактивний глушник: у такому типі глушника всякий раз, коли виявляється законна передача, тільки накладається сигнал перешкоди;

– постійний глушник: в цьому типі глушника постійно передається сигнал аджаммінгу;

– адаптивний глушник: у цьому типі глушника сигнал глушіння налаштовується на рівень прийнятої потужності в приймачі оператора;

– переривчастий глушник: в такому типі аджаммінгу сигнал випускається час від часу;

– інтелектуальний глушник: такий тип глушника використовує слабкі місця протоколів верхнього рівня для блокування.

Флуд-атака: тут зловмисник відправляє величезну кількість пакетів з метою порушити мережевий зв'язок з іншими вузлами. Єдина мета зловмисника – викачати ресурси з пристрою жертви.

1. Replay / playback attack: це тип активної атаки, при якій передані дані повторюються зловмисно. Зловмисник перехоплює передані дані шин, щоб повторно відправити їх далі. Це повторення робиться для того, щоб вичерпати енергію мережі [11].

Impersonate attack і sybil attack: у цьому разі зловмисник отримує IP-адресу шини або MAC-адресу (Media Access Control) будь-якого авторизованого користувача, а потім робить цю IP-адресу своєю власною. Ця

атака дуже добре відома. Потім ця вкрадена IP-адреса може бути використана зловмисником для здійснення різних інших атак. Просунута версія уособлення атаки називається атакою Сибілли в такому типі атаки зловмисник краде кілька ідентифікаційних даних (рис. 2.3).

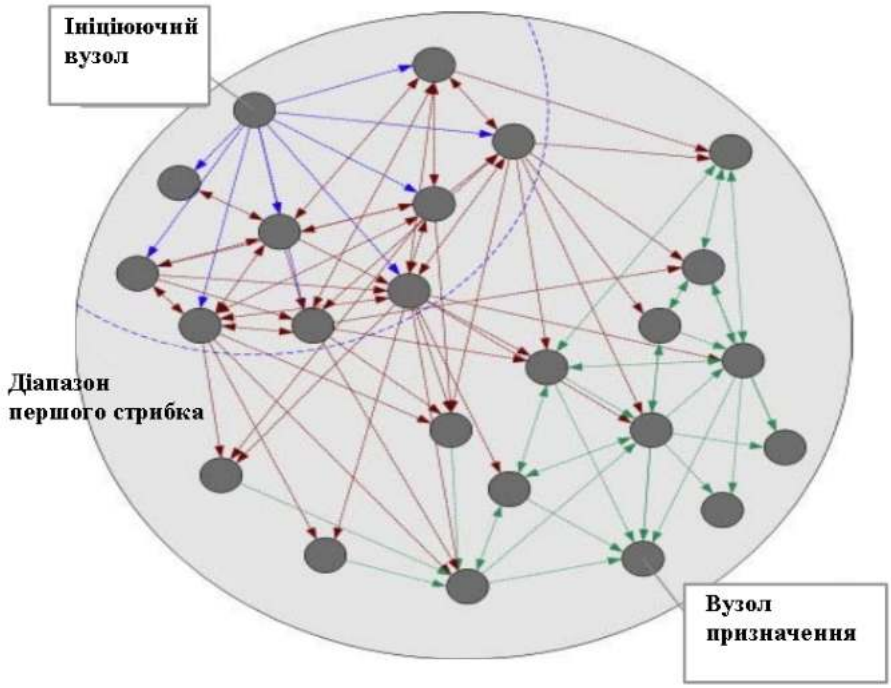

Рисунок 2.3 – Сценарій флуд-атак [12]

Послуги, що надаються мережею GSM, не можуть бути доступні жодному абоненту до аутентифікації, тобто він повинен бути попередньо аутентифікований. Для аутентифікації користувача GSM-мережа використовує алгоритм A3. Аутентифікація використовує механізм виклику-відповіді. А алгоритм A5 використовується для цілей шифрування [13].

Існують різні уразливості безпеки, виявлені в GSM. Деякі з цих проблем вирішуються в більш високих поколіннях стільникових мереж. Деякі з проблем, з якими стикаються мережі GSM, згадуються нижче.

Одностороння аутентифікація: мережа GSM автентифікує користувачів, але користувачі не автентифікують мережу, через це зловмисник використовує

підроблену базову систему трансрецепторів (BTS) з тим же кодом мобільної мережі, що і у законної абонентської мережі, щоб замаскувати себе і виконати атаку MIMT [14, 15].

Недоліки в реалізації алгоритмів A3/A8: алгоритм A3 і A8 знаходиться в SIM-карті, що може викликати проблеми безпеки при клонуванні даних SIM-карти можна отримати всі виклики серверів і повідомлення, що відстежуються з відповідного номера SIM-карти. Також, використовуючи технологію шин мобільних пристроїв, зловмисник може декодувати алгоритм і може атакувати мережу провайдера. Хоча в архітектурі безпеки GSM оператор може вибрати будь-який алгоритм аутентифікації, тобто або A3, або A8, але деякі оператори використовують COMP128, і цей алгоритм був розроблений Асоціацією Tire GSM. Пізніше в структурі COMF128 було виявлено безліч недоліків безпеки [16].

Клонування SIM-карти: ця атака добре відома вже більше 25 років, і коли ця атака виконується, різні дані, що зберігаються в SIM-карті, витягуються і програмуються в іншу чіпову карту, створюючи копію оригінальної SIM-карти. Клонування можливе як фізичними, так і повітряними методами (OTA) [17].

Фізичне клонування: при фізичному клонуванні дублікат SIM-карти створюється шляхом отримання доступу до цільової SIM-карти і вилучення її унікальних ідентифікаторів за допомогою зчитувача карт, а потім використовується пристрій запису карт для реплікації значень SIM-карти в нову SIM-карту. Для здійснення фізичного клонування зловмисник повинен володіти наступними речами [18]:

– програматор (Super sim, Sim Max) для читання SIM-карти;
– також необхідна порожня SIM-карта, на яку можна скопіювати дані;
– для цієї мети зазвичай використовуються срібні SIM-карти;
– програма для зчитування таких ідентифікаторів, як Ki, IMSI (International Mobile Subscriber Identity) і ICCID (ID SIM-карти);

– OTA: також можна витягти унікальні ідентифікатори SIM-карти, такі як Ki, IMSI, без будь-якого фізичного доступу. Для цього в сім-карту посилається кілька викликів, а потім ці виклики аналізуються. Однак цей підхід вимагає багато часу [19].

Короткий діапазон захисту. В мережах GSM конфіденційність забезпечується через шифрування, але інформація шифрується при її передачі безпровіному інтерфейсу, тобто між мобільною станцією (МС) і БТС. Це ясно вказує на те, що всякий раз, коли інформація передається по фіксованих частинах, ця інформація може бути легко підслухана зловмисниками, тому що вона передається без шифрування. Більш того, бездротовий інтерфейс вважається найслабшим для хакерів.

Витік анонімності користувача. Мережа GSM запитує користувача передавати свій IMSI візуально через бездротовий інтерфейс щоразу, коли користувач вперше входить в зону розташування або коли втрачається зіставлення між TMSI користувача (Temporary Mobile Subscriber Identity) і IMSI. Ця інформація може бути не використана зловмисниками [20].

Відсутність положення про цілісність. Архітектура безпеки GSM передбачала Положення про аутентифікацію та конфіденційність однак вимога безпеки вимагає включити положення про цілісність в архітектуру будь-якої мережі, щоб запобігти підробці інформації. Але захист цілісності був проігнорований в архітектурі безпеки GSM.

Уразливості в криптографічних алгоритмах. Два алгоритми, тобто A5 / 1 і A5/2, були використані для шифрування GSM, але основний потік, виявлений в цих алгоритмах, полягав у тому, що алгоритми були розроблені конфіденційно. Тому, коли алгоритми A5 були реалізовані публічно і проаналізовані криптоаналітиками, стало очевидно, що система може бути легко атакована і зламана відносно простими методами. Основною вразливістю, виявленою в цих алгоритмах, був згенерований ключ (Kc). Алгоритми (A5/1, A5 / 2) не були розроблені з використанням сучасних криптографічних знань [21].

2.3 Аналіз існуючих методів вирішення проблем уразливості GSM

Використання безпечних алгоритмів аутентифікації. Таке рішення може допомогти в запобіганні небезпечних атак клонування SIM-карт. Однак для реалізації цього рішення необхідно створити нові SIM-карти і модифікувати програмне забезпечення HLR (Home Location Register). В даний час, щоб перешкодити злому OTA Ki; GSM використовує як COMF128-2, так і COMF128-3, крім того, в алгоритмах COMF128-3 ефективна довжина ключа сеансового ключа була збільшена на 10 біт, що ще більше підвищує безпеку мереж GSM.

Використання алгоритмів безпечного шифрування. Шляхом впровадження алгоритмів безпечного шифрування і модифікації протоколів аутентифікації можна підвищити безпеку консорціуму GSM. Це допоможе убезпечити магістральний трафік від проблеми підслуховування з боку хакерів, а модифікацію переданих даних можна буде запобігти.

Наскрізне шифрування. Ще один спосіб забезпечення безпеки GSM-зв'язку – це розгортання наскрізного захисту або безпеки на прикладному рівні. End-to-End Enciyption (E2EE) ciypts конфіденційні дані. Ця інформація надійно переміщується по вразливих каналах до місця призначення, де вона розшифровується [22].

Поліпшення в UMTS в порівнянні з GSM: безпека UMTS була побудована шляхом збереження сильних функцій безпеки і переваг GSM і усунення вразливостей архітектури безпеки GSM. 3G ввів повністю пакетні мережі, в той час як більш ранні мобільні покоління були засновані на комутації каналів. Інші поліпшення в порівнянні з GSM включають в себе:

– взаємну аутентифікацію. Термін взаємна аутентифікація означає, що і користувач, і мережа повинні аутентифікувати один одного. У GSM аутентифікація проводилася тільки одним способом, тобто тільки від користувача до мережі, що робить GSM вразливим для багатьох атак, щоб

протистояти цим атакам UMTS використовує взаємну аутентифікацію, забезпечуючи безпеку від шахрайської базової станції;

– захист цілісності: UMTS також забезпечує надання механізму цілісності, який захищає повідомлення від будь-яких змін. Отже, механізм цілісності з поліпшеною аутентифікацією забезпечує захист від активних атак;

– якість обслуговування. Якість обслуговування не була повністю охоплена архітектурою безпеки GSM. В UMTS QoS був включений для того, щоб максимізувати користувальницький досвід, а також забезпечити оптимальний розподіл спектру для конкретного типу послуг передачі даних.

Еволюція LTE-безпеки. Оскільки архітектура безпеки стільникових мереж постійно еволюціонувала, у бездротовій мережі 1G (першого покоління) зловмисникам було дуже легко підслуховувати і отримувати доступ до мережі за допомогою шахрайських засобів [23]. У 2G GSM алгоритми, що використовуються для аутентифікації, були легко декодовані. Крім того, майстер-ключі безпеки було легко розкрити за допомогою декількох взаємодій з SIM-картою [24]. У бездротовій мережі 3G процес аутентифікації був посилений за рахунок використання взаємної аутентифікації. Крім того, безпека в 3G була додатково підвищена за рахунок використання 128-бітних ключів шифрування і цілісності [25] Потім наступне покоління, тобто система 4G або LTE, яка показала перехід від комутації каналів до пакетної, була розроблена як система на основі пакетів, яка пропонує багато переваг у порівнянні з попередніми мережами.

Уразливості в LTE: у зв'язку з впровадженням нових технологій радіодоступу і переходом до IP-архітектури виникли нові уразливості, нижче приведена класифікація і категоризація різних загроз архітектурі безпеки LTE (Рис. 2.4).

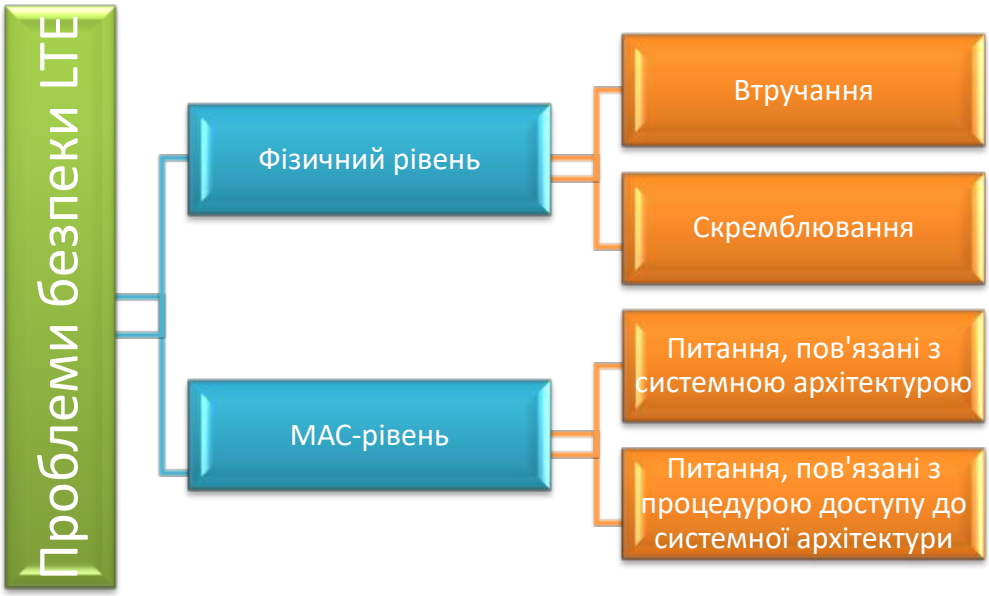

Рисунок 2.4 – Типи атак в LTE

Перешкоди викликають переривання безперебійного функціонування системи зв'язку через високий рівень сигналу. Інтерференція в будь-якій системі зв'язку може здійснюватися двома способами: шумовий, мультинесучий [26]. Шумові перешкоди можуть бути виконані з використанням білого гауссовського шуму (WGN).

Скремблювання також є одним з видів перешкод, які вставляються на невеликі проміжки часу. У цьому типі атак цілеспрямовано використовуються певні алгоритми. Щоб порушити роботу служб конкретного користувача, зловмисник націлюється на контрольну і керуючу інформацію. Однак зловмисник повинен бути досвідченим і добре обізнаним.

Проблеми рівня MAC. Проблеми відкритої архітектури: перехід до відкритого набору комунікаційних протоколів, тобто до набору TCP / IP, загрожував збільшенням числа проблем в LTE, таких як вразливість до модифікацій, атак підслуховування і більших ризиків конфіденційності, ніж в мережах GSM і UMTS [27]. Архітектура LTE стає більш вразливою до

традиційних шкідливих атак, таких як підміна IP-адресів, DoS-атак, спам-листів і дзвінків і т.д. [28].

Питання, пов'язані з процедурою доступу. Для досягнення взаємної аутентифікації між призначеним для користувача обладнанням (UE) і об'єктом управління мобільністю (MME) через еволюціонуючу універсальну мережу наземного радіодоступу (E-UTRAN) Архітектура LTE розширила угоду UMTS-Authentication and Key Agreement (UMTS-AKA) і представила новий підхід до забезпечення безпеки доступу, що еволюціонувала пакетну систему AKA (EPS AKA) і механізм J-PAKE (Password Authenticated Key Exchange by juggling). Однак ці протоколи автентифікації також страждають від різних вразливостей, таких як витік IMSI, витік ключа, перенаправлення трафіку, відстеження тимчасової ідентифікації, тобто GUTI [29]. Ці уразливості необхідно усунути, щоб забезпечити надійність архітектури безпеки.

Рішення для вразливостей LTE: різні рішення були запропоновані різними дослідниками для того, щоб задовольнити уразливості LTE. Деякі з них наведені запропонують гібридне рішення між аутентифікацією, авторизацією та ключами, засновану на платформі моделі довіри (TMP) та інфраструктурі відкритих ключів (PKI). З метою досягнення взаємної аутентифікації між призначеним для користувача обладнанням і гібридним вузлом паролі зв'язуються з відбитками пальців і відкритим ключем. Ця запропонована схема забезпечуватиме користувачам надійність доступу до конфіденційних служб і даних.

Таким чином, бездротовий мобільний зв'язок швидко розвивається і переживає феноменальне зростання. Оскільки він забезпечує доступ до користувачів в будь-який час і в будь-якому місці, мобільний зв'язок приваблює користувачів, а також постачальників послуг по всьому світі. Однак мобільний зв'язок стикається з різними проблемами безпеки. Однак необхідність посилення заходів безпеки може також привернути увагу дослідників до подальшого зміцнення користувацького обладнання мобільних станцій поряд з мережею.

3 ЕВОЛЮЦІЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ БЕЗПЕКИ В МЕРЕЖАХ МОБІЛЬНОГО ЗВ'ЯЗКУ

3.1 Безпека в мобільному звя'зку 2G-GSM

Головним нововведенням, перевіреним в GSM, стало використання модуля ідентифікації абонента (SIM), який містить і необхідні ідентифікаційні та охоронні дані. На відміну від аналогових стільникових систем першого покоління, які не підтримували жодного типу шифрування інформації, безпека в GSM була необхідна для забезпечення анонімності та конфіденційності, а також, щоб білінгові операції оператора проводилися правильному клієнтові, без можливості операторів втручатися випадково або навмисно. На цьому етапі SIM-карта використовує алгоритм під назвою A8, ключ Ki і виклик для отримання ключа сеансу (Kc), який відправляється на базову станцію. За допомогою цього ключа використовується алгоритм A5, який відправляє зашифровані дані на базову станцію. Алгоритми A3 і A8 зазвичай використовуються разом в одному, який може бути зламаний приблизно за 8 годин. Існує кілька версій алгоритму A5, і найслабша з них взламується всього за 2 хвилини [30].

Перше завдання, яке повинна виконати мережа, - це аутентифікація користувача, що відправляє випадковий 128-бітний виклик (RAND) на мобільний телефон користувача. Якщо СДСВ відповідає значенню, включеному в базову станцію, то переходять до наступного кроку. Потім SIM-карта використовує алгоритм, званий A3, і секретний і унікальний ключ кожного SIM-карти (Ki), щоб відповісти на виклик (SRES Signed RESponde).

Всі мобільні телефони мають унікальний номер, незалежний від SIM-карти, званої International Mobile Equipment Identify (IMEI), який зберігається в реєстрі ідентифікації обладнання (EIR). Кожна SIM-карта може бути ідентифікована за допомогою міжнародного ідентифікатора мобільного абонента (IMSI). Щоб люди не знали про IMSI, він надсилає IMSI кожен раз,

коли відбувається зв'язок з базовою станцією, коли мобільний телефон включений. EIP знижує загрози крадіжки мобільних телефонів, так як надає оператору можливість запобігати використанню вкрадених терміналів в своїх мережах. EIR має різні рейтинги для кожного IMEI: білий для дійсних мобільних телефонів, сірий для телефонів, за якими потрібно стежити, і чорний для заблокованих телефонів [30].

Під час розробки GSM передбачалося, що даний зв'язок буде фіксованим, і тому його не потрібно було шифрувати. Можлива атака, яка виконується в GSM, здійснюється через канал зв'язку між базовою станцією (BS) і контролером BS. Це посилання може бути прослухане, так як в момент з'єднання дані все ще розшифровуються. Під час розробки GSM передбачалося, що цей зв'язок буде фіксованим, і тому його не потрібно було шифрувати. Іншою формою атаки було б використання помилкової базової станції для передачі Rand по радіоінтерфейсу, позначеному Um (air). Іншим вагомим недоліком є алгоритм A3 / 8, який дозволяє дізнатися ключ Ki, якщо отримано 160000 пар RAND-SRES. Існують певні атаки, які можуть бути використані для отримання цих пар, найслабшими з яких є крадіжка мобільного телефону, видалення SIM-карти і підключення її до емулятора, який може бути використаний для відправки 160000 пар на SIM-карту і отримання відповідних SRES. Оскільки SIM-карта працює відносно повільно, для отримання потрібних пар буде потрібно 10 годин. Деякі з відомих слабких місць GSM є:

- цілісність даних не гарантується;
- можливість використання помилкової базової станції для перехоплення повідомлень;
- відсутність гнучкості;
- ключі шифрування і аутентифікаційні дані чітко передаються між мережами і всередині;
- шахрайство і юридичні перехоплення не розглядалися на етапі проектування проекту;

3.2 Безпека в мобільному звя'зку 3G-UMTS

Безпека GSM мала серйозні недоліки. UMTS security була заснована на механізмах безпеки GSM, підтримуючи і вдосконалюючи свої важливі структури безпеки. На додаток до вирішення цих проблем, безпека на 3G має також нові механізми безпеки та обслуговування. Основна мета архітектури безпеки 3G полягала у створенні гнучкої системи, здатної адаптуватися до нових викликів безпеки. Визначено п'ять ключових особливостей архітектури 3G [30]:

– безпека домену програми: включення додатків для безпечного обміну повідомленнями;

– безпека доступу до мережі: забезпечення конфіденційності ідентифікації користувача, сигнальних даних, цілісності даних, аутентифікації користувача та ідентифікації мобільного обладнання;;

– мережева безпека: можливість обмінюватися сигнальними даними і захистити від атак в мережі;

– безпека домену користувача: забезпечення авторизованого доступу до універсального модуля ідентифікації абонента;

– видимість безпеки та конфігурація: інформуйте користувача про те, чи працює певна функція безпеки і чи повинно надання та використання послуг залежачих від цієї функції.

Користувач ідентифікується за допомогою ідентифікатора радіоінтерфейсу, який об'єднується з ідентифікатором місця розташування області. Коли користувач намагається отримати доступ до послуг 3G, він ідентифікує себе через TMSI цієї області.

Для забезпечення безпеки в мережі необхідний доступ до аутентифікації і ключа угоди. Цей механізм виконує взаємну аутентифікацію користувача і мережі за допомогою симетричного ключа і виводить ключі шифрування і цілісності, що мають сумісність з архітектурою безпеки GSM. Безпека доступу до мережі є ключовим елементом архітектури безпеки 3G. Ця частина гарантує

конфіденційність користувача, де вони запобігають помилці щодо місця розташування доступу користувача зловмисниками [30].

Ризики і загрози, присутні в UMTS:

– скомпрометувати вектори аутентифікації в мережі. Зловмисник має вектор аутентифікації, який може включати пари виклик/відповідь, ключі шифрування і ключі цілісності. Ці дані отримані шляхом компрометації вузлів мережі або перехоплення повідомлень в мережевих з'єднаннях;

– прослуховування: зловмисник перехоплює сигнальні канали і дані, пов'язані з іншим користувачем. Потрібна модифікована мобільна апаратура;

– уособлення іншого користувача: зловмисник посилає сигнали призначені для користувача, намагаючись створити в мережі враження, що вони були викликані цільовим користувачем. Потрібна модифікована мобільна апаратура;

– уособлення мережі: зловмисник посилає сигнали або дані цільовому користувачеві, намагаючись змусити користувача повірити, що вони походять зі справжньої мережі. Потрібна модифікована базова станція;

Захист цілісності сигнальних повідомлень між мобільним обладнанням і контролером радіомережі починається під час активації захисту таким чином, щоб були відомі ключ цілісності (IK) і алгоритм захисту цілісності. Код аутентифікації повідомлення (MAC) застосовується до кожного повідомлення в сигнальному шарі RRC універсальної наземної мережі радіодоступу (UTRAN) [30].

В UMTS відмовляє в обслуговуванні надаваних клієнту послуг коли:

– шахрайська базова станція: зловмисник з пристроєм змінив своє положення між сервісною мережею і цільовим користувачем.

– підміна запиту на зняття реєстрації: якщо мережа не може аутентифікувати повідомлення;

– підміна запиту на оновлення місця розташування: замість відправки заявок на реєстрацію зловмисник відправляє запит на оновлення місця розташування іншій області, де знаходиться користувач.

Щоб забезпечити цілісність і захист шифрування, необхідно слідувати процесу з кожним новим сигнальним з'єднанням між мобільним пристроєм і регістром місця розташування відвідувача (VLR). Можливості забезпечення безпеки мобільного обладнання передаються на контролер радіомережі [30].

У 3G security дані користувача і деякі елементи сигнальної інформації вважаються конфіденційними і тому повинні бути захищені. Механізм, що забезпечує таку гарантію цілісності, заснований на алгоритмі цілісності UMTS (UIA-який пізніше буде називатися алгоритмом f9), який реалізований як в базовій станції, так і в модулі UTRAN closer central network, тобто RNC.

Процедура перевірки цілісності даних відбувається наступним чином: спочатку алгоритм користувацького обладнання f9 обчислює 32-бітний MAC для забезпечення цілісності даних на основі їх вхідних параметрів. На другому етапі MAC додається до повідомлення, і інформація передається по радіоінтерфейсу призначеного для користувача обладнання в RNC. На третьому етапі, як тільки RNC отримав інформацію і MAC, приєднаний раніше, потім обчислюється отримана сигнальна інформація XMAC і завершальний етап, цілісність сигнальної інформації перевіряється шляхом порівняння MAC і XMAC [30].

На відміну від алгоритму цілісності, який працює тільки з сигнальними даними, механізм конфіденційності працює як з сигнальною інформацією, так і з користувацькими даними. Алгоритм, встановлений для виконання завдань конфіденційності, позначається алгоритмами f8 і працює наступним чином: на першому етапі, використовуючи ключ шифрування CK, обчислюється вихідний потік бітів, що проходить через алгоритм F8 в апаратурі користувача. На другому етапі виконується операція XOR (біт за бітом) між вихідним бітовим потоком і потоком даних. На третьому етапі шифротекст передається в мережу через радіоінтерфейс, і на заключному етапі алгоритм f8 на RNC використовує ті ж записи, що і обладнання користувача, включаючи загальний ключ шифрування (CK), для генерації того ж вихідного потоку бітів, який був згенерований в обладнанні користувача. Для досягнення мети цієї останньої

фази необхідно буде знову виконати операцію XOR між вихідним бітовим потоком і отриманим шифрованим текстом для вилучення вихідної інформації.

Такі покоління зв’язку як GSM, UMTS теж схильні до загроз на рівні комунікацій між двома користувачами, проте зловмисник повинен володіти певними здібностями для успішного виконання атаки [30].

Зловмисник може пройти через мережу, щоб мати можливість «слухати», маскуючись під надійну мережу перед користувачем:

– придушення шифрування між користувачем і зловмисником: зловмисник з модифікованою БС залучає користувача для підключення до помилкової БС, і при запуску служби зловмисник не активує шифрування;

– придушення шифрування між користувачем і реальною мережею: в цьому випадку шифрувальні можливості мобільної станції змінюються під час виклику і в мережі з'являється несумісність алгоритмів шифрування і аутентифікації.

– примусове використання скомпрометованого ключа шифру: зловмисник з БС і вектором скомпрометованої аутентифікації переконує користувача зробити дзвінок, поки він знаходиться на помилковому БС. Потім зловмисник примусово використовує ключ шифрування.

Інший вид атаки – захоплення особистості. Мобільні користувачі ідентифікуються за тимчасовими ідентифікаторами, однак мережа просить користувача відправити свою постійну ідентифікацію:

– активне захоплення ідентичності: у цьому випадку зловмисник з модифікованою БС заохочує користувача використовувати цю БС і просить вас відправити свій IMSI.

– пасивне захоплення ідентичності: зловмисник з модифікованим мобільним пристроєм пасивно очікує нового запису або збою в базі даних. В обох випадках користувачеві пропонується відправити свою ідентифікацію в незашифрованому вигляді [30].

Зловмиснику також може бути дозволено пройти повз іншого користувача:

– через скомпрометований вектор аутентифікації: за допомогою MS і зміненого вектора аутентифікації зловмисник передає цільового користувача в мережу;

– перехоплення вихідних дзвінків в мережах з відключеним шифруванням: зловмисник робить виклик цільового користувача. Зловмисник змінює сигнальні елементи, щоб в мережі з'явилося повідомлення про те, що користувач хоче зробити виклик.

– прослуховуючи відповідь на аутентифікацію: зі зміненою MC зловмисник використовує – якщо виклик використовується знову;

– захоплення вихідних дзвінків в мережах з включеним шифруванням: аналогічно попередній атаці, але вимагає, щоб зловмисник також змінив можливості мобільного шифрування для придушення шифрування;

– захоплення вхідних викликів з відключеним шифруванням: коли хтось, пов'язаний з зловмисником, дзвонить цільовому користувачеві, те ж саме передається зловмисникук. Якщо мережа не активує шифрування, зловмисник використовує це посилання для відповіді на виклик;

– захоплення вхідних викликів без шифрування: аналогічно попередній атаці, але тут зловмисник повинен придушити шифрування.

Хоча основні загрози, яким може піддаватися UMTS, відомі, все ж можна реалізувати деякі заходи, щоб уникнути деяких атак, згаданих в попередньому пункті, а саме:

– щоб уникнути підміни запиту на скасування реєстрації, необхідний захист цілісності критичних сигнальних повідомлень. Сервісна мережа перевіряє цілісність заявки на реєстрацію;

– щоб уникнути підміни запиту на оновлення місця розташування, було запевнено, що він завжди захищений від повторень і модифікацій;

– для контратаки шахрайських БС вводиться захист цілісності критичних сигнальних повідомлень, що, в свою чергу, запобігає атакам типу «відмова в

обслуговуванні». Зловмисник не може змінювати сигнальні повідомлення, однак система не може перешкодити зловмиснику перехоплювати повідомлення між мережею і цільовим користувачем;

– для контратаки пасивного захоплення ідентичності використання тимчасових ідентичностей перешкоджає цьому захопленню, так як зловмисник повинен чекати нової реєстрації або збою в базі даних, щоб отримати профіль користувача в зашифрованому тексті [30].

3.3 Безпека в мобільному звя'зку 4G-LTE

Архітектура LTE заснована на секретному ключі, який зберігається на SIM-карті Один і той же ключ використовується для GSM, UMTS і LTE, а також може ефективно переміщати контекст безпеки між вузлами мережі, коли користувач переміщається між різними технологіями радіодоступу. абонента і домашньому абонентському сервері (HSS) в мережі. Ключі відомі eNodeB, вони активують перевірку цілісності і процес шифрування повідомлень RRC. Під час початкового контакту з мережею LTE викликаються процедури безпеки між призначеним для користувача обладнанням (UE), об'єктом управління мобільністю (MME) і HSS. Під час цього процесу UE автентифікується в мережі, а мережа аутентифікується в UE (взаємна аутентифікація). Секретний ключ залишається в захищеному середовищі і не може бути прочитаний потенційними зловмисниками, які шукають обмін повідомленнями на інтерфейсі між SIM-картою і мобільним пристроєм або HSS і MME. SIM-карти повинні бути здатні виконувати як UMTS, так і LTE-аутентифікацію одночасно. Старі SIM-карти, тільки для GSM, не можуть бути використані для аутентифікації LTE, і процедура підключення з такими SIM-картами відхиляється. Після виконання процесу аутентифікації генерується набір сеансових ключів. Після цього шифрування і захист цілісності можуть бути активовані для всіх повідомлень без доступу stratum, якими обмінюються UE і MME.

З появою відкритої і розподіленої IP-архітектури в LTE зловмисники можуть направлятися на мобільні пристрої та мережі і породжувати спам, шпигунство, поширення шкідливих програм, IP-спуфінг, крадіжку даних і послуг, розподілені атаки типу «відмова в обслуговуванні» (DDoS) і ряд інших варіантів кібератак і злочинів [30].

Процес механізмів безпеки в LTE проектується на власні сильні криптографічні методи, взаємну аутентифікацію між елементами мережі LTE з механізмами безпеки, вбудованими в їх архітектуру. Організація сектору безпеки виявили деякі уразливості, які слід оцінити до впровадження мережі. Оскільки повідомлення інкапсулюються в повідомлення RRC, вони проходять через два процеси шифрування і дві перевірки цілісності. Під час коли шифрування і перевірка цілісності включені, UE, MME і eNodeB можуть вибрати відповідний алгоритм шифрування і алгоритм цілісності зі списку алгоритмів, підтримуваних обома сторонами.. Функціонування алгоритмів шифрування і цілісності LTE вельми схоже в порівнянні з алгоритмами, описаними раніше в розділі UMTS.

Коли справа доходить до UE, основними загрозами / ризиками безпеки, які ми можемо виявити, є:

– відсутність стандартів безпеки та контролю. Існує все більше і більше смартфонів, планшетів та інших пристроїв різних виробників, які використовують LTE. Через це вони містять окремі, відкриті та власні операційні системи та програмне забезпечення;

– ризик втрати даних і конфіденційності. Через широкосмугові ресурси даних дані зберігаються на пристрої більше, ніж будь-коли, що робить їх привабливими цілями для зловмисників. Зловмисник може отримати доступ до даних користувача, користувач може стати жертвою різних злочинів, пов'язаних з крадіжкою особистих даних, втратою фінансової або конфіденційної особистої інформації та порушенням конфіденційності;

– фізичний напад. Смартфони – це портативні пристрої, що робить їх схильними до втрати/крадіжки. UE може бути фізично змінений і використаний для доступу до мереж операторів і атаки на них;

– вразливостей в програмному забезпеченні. Оскільки ЄЕС В LTE стали по суті пристроями, що використовують технологію IP, вони стали сприйнятливі до вразливостей і атак на основі IP. Користувачі, які завантажують Додатки і контент піддають свій пристрій впливу вірусів, спаму, фішингу та інших подібних загроз [30].

Коли мова заходить про мультимедійну підсистему IP (IMS), основними загрозами / ризиками безпеки, які ми можемо виявити, є:

– атаки на зловживання послугами. Абонент може діяти таким чином, щоб отримати більше привілеїв над послугою, ніж ті, які йому виділяються;

– несанкціонований доступ. Відкрита та розподілена архітектура IMS створює безліч точок розповсюдження, які повинні бути захищені. IP-пірінг між постачальниками послуг для різноманітної пропозиції послуг і різних стандартів безпеки часто знаходиться в напів-довірених зонах, які можуть зробити ядро IMS вразливим;

– мережеве шпигунство і захоплення сеансів. Цей тип атаки порушує конфіденційність з моменту перехоплення зловмисником потоку інформації між двома користувачами в сеансі SIP (Session Initiation Protocol). Без мережевого захисту зловмисники можуть використовувати такі інструменти, як Wireshark, для захоплення SIP-сигналізації. Захоплення сеансу відбувається, коли зловмисник вставляє шкідливі пакети, замінюючи трафік і порушуючи цілісність інформації, що вплине на якість обслуговування і самого сервісу.

Проте існують заходи, які здійснюються або виробниками, або операторами для пом'якшення цих загроз [30].

Використання цих заходів не обмежується лише виробниками та операторами, оскільки користувачі також можуть відігравати активну роль у забезпеченні додаткової безпеки своїх пристроїв, підключених до мережі.

Основними заходами щодо зниження загроз / ризиків безпеки є:

– навчання користувачів. Це найбільш ефективний підхід до захисту пристроїв, оскільки інформування користувача про ризики та збитки, які можуть бути заподіяні небезпечним пристроям, мотивуватиме його підтримувати свій пристрій у фізичній безпеці;

– встановлення норм безпеки в промисловості. Оператори та Виробники в даний час працюють разом над встановленням стандартів безпеки;

– використання надійних механізмів аутентифікації, авторизації та шифрування на рівні операційної системи.

– використання антивірусного програмного забезпечення. Після установки ПО пристрій повинен регулярно оновлюватися в якості основного механізму захисту пристрою [30].

Що стосується взаємозв'язку між пристроєм і мережею, то основними заходами щодо зниження загроз/ризиків безпеки є:

– впровадження пристроїв, що забезпечують фізичну безпеку. Розміщення пристроїв, що мають механізми, що використовують списки перевірки автентичності та контролю доступу;

– моніторинг мережі та впровадження систем запобігання вторгнень (IPS), як засобу виявлення зловмисників і мінімізації впливу, викликаного їх діями;

– впровадження механізмів аутентифікації, авторизації та шифрування між ЄЕС та eNodeBs. Впровадження механізмів шифрування з відкритим ключем (PKI), в яких відкритий ключ оператора зберігається в USIM, дозволяє UE шифрувати інформацію, пов'язану з конфіденційністю, наприклад IMSI, передану в eNodeB. Таким чином, дізнатися місцезнаходження абонента буде неможливо.

Коли мова заходить про БС, основними заходами щодо зниження загроз безпеки є:

– введення в архітектуру безпеки віртуальних приватних мереж (VPN) і віртуальних локальних мереж (VLAN). Їх використання може обмежити

шкоду, завдану зловмисниками в результаті несанкціонованого доступу, підміни та інших видів атак;

– моніторинг мережі, управління та балансування навантаження. Моніторинг мережі є незамінним механізмом для виявлення вторгнень в мережу. Однак визначення політики управління і пріоритизація трафіку мають вирішальне значення для запобігання накладних витрат, а також для зниження наслідків dos/DDoS-атак.

– здійснення прикордонної безпеки. IMS має механізми для захисту кордону мережі, для того щоб уникнути несанкціонованого доступу через інші мережі. Оскільки ця точка входу ненадійна, вона повинна бути захищена. Оператори інвестували кошти для забезпечення контролю своїх мережевих кордонів шляхом придбання інфраструктур безпеки, таких як брандмауери, для виконання фільтрації пакетів, маршрутизатори перетворення мережевих адрес(NAT), VPN і розширення можливостей шифрування між пірінговими мережами. Роумінгові абоненти отримуватимуть доступ до IMS через Інтернет;

– шифрування IKE/IPSec. Введення спрямоване на забезпечення аутентифікації, авторизації, цілісності та конфіденційності [30].

Коли мова заходить про IMS, основними заходами щодо зниження загроз/ризиків безпеки є:

– впровадження шлюзів безпеки. IMS-це єдина платформа, яка використовується кількома постачальниками послуг, управління безпекою виходить за рамки простого використання традиційних брандмауерів і маршрутизаторів, оскільки існує кілька активних сеансів і застосування політик аутентифікації і шифрування. Оператори інвестують у впровадження шлюзів безпеки для управління цією складною ситуацією.

– активація протоколів безпеки зв'язку та передачі даних між пристроями та ICM. Активація таких протоколів, як SSL/TLS і IPSec, дозволяє встановлювати безпечні з'єднання.

3.4 Безпека в мобільному звя'зку 5G

Для того щоб відповісти основним вимогам мереж 5G, очікується повне використання декількох технологій, таких як віртуалізація мережевих функцій (NFV), програмно-визначена мережа (SDN), програмно-визначене Радіо (SDR) і хмарна мережа радіодоступу (c-RAN). Їх використання дозволяє гнучко використовувати технологію доступу, забезпечує обчислювальну, запам'ятовуючу і загальну ємність мережі, коли це необхідно [30].

Основні зміни в механізмах безпеки прогнозуються в декількох областях, таких як:

– управління аутентифікацією;
– управління ідентифікацією та конфіденційністю;
– захист конфіденційності користувачів;
– безпека на мережевих інтерфейсах;
– алгоритми шифрування;
– захист від DoS-атак.

В даний час модель довіри телекомунікаційних мереж може бути представлена тільки двома елементами, так як вона формується користувачами і мережею (рис. 3.1).Телекомунікаційні мережі відповідають тільки за аутентифікацію користувачів при доступі до мережі. Процес аутентифікації між Користувачем і сервісами не покривається мережами [30].

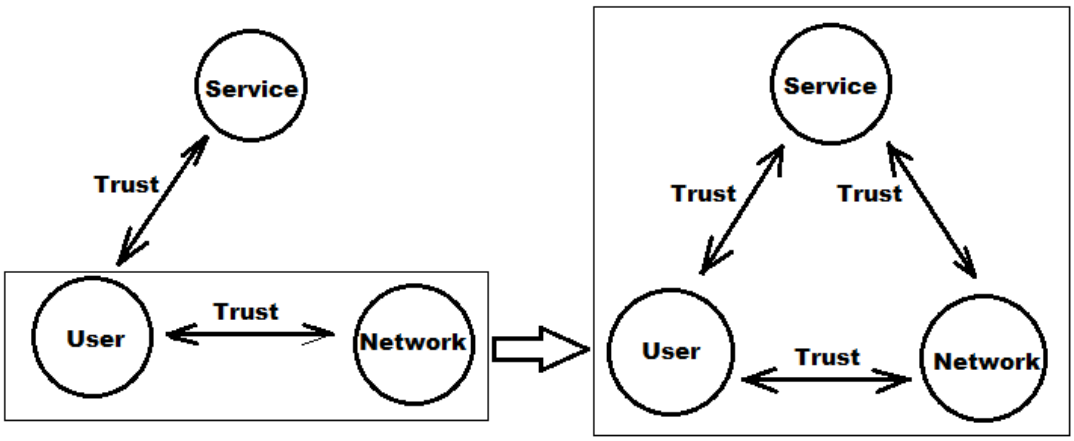

Рисунок 3.1 – Модель довіри телекомунікаційних мереж

Управління особистими даними та конфіденційністю. Стільникові мережі покладаються на USIM-карти для управління посвідченнями користувачів і ключами. У 5G очікується два типи парадигм :

– поєднання ідентифікатора пристрою та ідентифікатора служби: у новій структурі управління ідентифікацією ідентифікатор складається з ідентифікатора пристрою та ідентифікатора служби. Кожен ідентифікатор пристрою глобально унікальний і може бути присвоєний пристрою на етапі виробництва. Ідентифікатори служб призначаються постачальниками послуг або мережами [30];

– пристрої одного і того ж користувача можуть спільно використовувати квоти. Перехід від управління на основі пристроїв до управління на основі користувачів: дозволити користувачам вирішувати, якому з їх пристроїв дозволено отримувати доступ до мережі і яку службу дозволено використовувати. пропускної здатності як в режимі онлайн, так і в автономному режимі.

Розробка та впровадження нових криптографічних алгоритмів. Використання енергоефективних криптографічних алгоритмів передбачено в рамках 5G в даний час існуючі методи засновані на використанні CRC-шифрування (Krawczyk) і кодів аутентифікації повідомлень (MAC s), які мають деякі обмеження, такі як [30]:

– ретрансляції витрачають енергію даремно і збільшують середню затримку пакетів;

– обидва методи не допускають виправлення помилок;

– якщо перевірка MAC завершується невдало, повідомлення відкидається і запитується повторна передача;

– надмірні ретрансляції, які можуть призвести до перевантаження мережі.

У галузі, яка відповідає управлінню аутентифікацією, очікується, що в 5G мережі можуть співпрацювати з постачальниками послуг для виконання ще більш безпечного і ефективного управління ідентифікацією, що

призводить до трьох моделей аутентифікації, які можуть співіснувати в 5G: аутентифікація, виконувана тільки мережами; аутентифікація, виконувана тільки постачальниками послуг, і аутентифікація, виконувана мережами і постачальниками послуг [30].

Щоб захистити конфіденційність користувача, необхідно визначити нові правила виявлення, пов'язані з послугами, щоб реагувати на проблеми користувачів, пов'язані з їх конфіденційністю. Правила повинні обумовлювати, як буде використовуватися конфіденційність інформації і яке звернення має бути застосоване після її використання.

З розвитком технологій інтелектуального аналізу даних пошук інформації про конфіденційність користувача став простішим. Оскільки мережі 5G обслуговуватимуть велику кількість вертикальних галузей і це має на увазі велику відповідальність за великий обсяг інформації, пов'язаної з конфіденційністю користувача, будь-який витік інформації може мати серйозні наслідки. Тому інформація про конфіденційність користувачів повинна бути надійно захищена в мережах 5G, щоб користувачі і вертикальні галузі могли використовувати ці мережі, не турбуючись про витік інформації [30].

Безпека між терміналами та мережею. Існує поділ сигналізації безпеки між рівнями AS і NAS, щоб забезпечити підвищення безпеки між терміналами і мережею.

В даний час за допомогою технологій інтелектуального аналізу даних третя сторона може отримати детальну інформацію про конфіденційність користувача за допомогою аналізу даних [30].

Безпеки на мережевих інтерфейсах. Оскільки розвиток дуже щільних і спеціальних мереж зі зворотним рейсом зажадає систем, які можуть автоматично організовувати свою топологію, адаптуватися до наявного спектру і забезпечувати зв'язок між пристроями. Ця зміна буде здійснюватися виключно з використанням нових протоколів, належним чином розроблених для цієї мети.

Видимість і конфігурованість системи безпеки. Бізнес-спільнота була сильно поставлена під сумнів можливість надання користувачеві можливості інформувати мережу про функції безпеки, які повинні бути активовані для запуску певних додатків [30].

Щоб відповісти на це питання, Дуброва та її команда запропонували деякі рішення, включаючи новий тип MAC та новий потоковий шифр.

Пропонований MAC ефективно поєднує захист на рівні цілісності з однобітною корекцією помилок, таким чином, можна зберегти переваги CRC і обійтися без тесту неприводимості, що робить його хорошим кандидатом для більш простих типів радіозв'язку 5G і для випадків з обмеженими ресурсами, таких як міжмашинний зв'язок (M2M) [30].

Можна сказати, що електроніка, яка використовується протягом поколінь, зазнала значного скорочення з точки зору площі. Однак це скорочення не означає втрати ефективності в її завданнях. Швидше за все, чіпи стають все менше і мають все більш високу обчислювальну потужність [30].

Захист від атак типу «відмова в обслуговуванні». Справитися з цим типом атаки непросто, проте можна мінімізувати її наслідки і впровадити нові механізми протидії мережевим накладним витратам.

3.5 Безпека в мобільному звя'зку 5G & IoT

Інтернет речей (IoT) - це інтернет широкого спектру підключених пристроїв (званих речами), які можуть бути простими датчиками, дронами або транспортними засобами, які можуть бути з'єднані у велику мережу. Оскільки більшість речей використовують бездротовий зв'язок, існуючі мережі мобільного зв'язку використовуються в якості основи зв'язку, які будуть розвиватися з урахуванням необхідності обробляти мільйони речей, підключених одночасно з використанням різних додатків і послуг [30].

У контексті стандартизації розробляються наступні стандарти аутентифікації пристроїв:

– проект IEEE 15.9, що містить рекомендації щодо підтримки управління ключами в стандарті IEEE 802.15.4. даний стандарт, про який йде мова, визначає всі специфікації зв'язку з фізичного рівня і середнього рівня доступу для бездротових мереж зв'язку, що працюють з низькими швидкостями передачі даних.

– IEEE 802.1 X-2010, призначений для локальних і столичних мереж, управління доступом до мережі яких засноване на портах. Охоплює архітектуру, функціональні елементи та протоколи для взаємної аутентифікації та безпечного зв'язку між клієнтами портів, підключених до однієї локальної мережі;

– IEEE 802.1-AR 2009, придатний для локальних обчислювальних мереж і метрополітену, в центрі уваги якого знаходиться Асоціація локально важливих ідентифікаційних пристроїв з ідентифікацією, що поставляється виробником для використання протоколів ініціалізації та аутентифікації [30];

Незважаючи на існування цих стандартів, не робилося ніяких постійних зусиль зі стандартизації засобів масової інформації. Що, в свою чергу, призводить до того, що дана ситуація стає неприйнятною з точки зору наданої інфраструктури зв'язку і QoS, оскільки співвідношення ефективності та енергії криптографічних алгоритмів, використовуваних цими службами, є визначальним фактором для їх зразкової продуктивності.

З точки зору безпеки, з'єднання мільйонів речей і використання нестандартних протоколів безпеки, оскільки практично кожен виробник використовує власні протоколи з низьким рівнем безпеки для здійснення комунікацій, може зробити негативний вплив на безпеку не тільки Інтернету речей, але і всіх інших пристроїв, підключених до мобільної мережі [30].

4 ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ТЕХНІЧНОЇ ЧАСТИНИ

4.1 Загальні положення

Інвестиції - це сукупність витрат, спрямованих у формі цілеспрямованого вкладу коштів в різні сфери і галузі діяльності для подальшого отримання прибутку і досягнення певного результату. Інвестиціями є всі види майнових та інтелектуальних цінностей, що вкладуються в об’єкти підприємницької та інших видів діяльності, в результаті якої створюється прибуток або досягається економічний чи соціальний ефект.

Об’єктами інвестиційної діяльності можуть бути будь-яке майно, в тому числі основні засоби і оборотні активи в усіх галузях та сферах народного господарства, цінні папери, цільові грошові вклади, науково- технічна продукція, інтелектуальні цінності, інші об’єкти власності, а також майнові права.

Суб’єктами інвестиційної діяльності можуть бути громадяни і юридичні особи України та іноземних держав, а також держави [31].

Метою дипломної роботи є аналіз захищеності мереж мобільного зв’язку на основі технології 5G. Даний аналіз в майбутньому допоможе доповнювати засоби захисту операторів мереж мобільного зв'язку та звертати увагу на уразливі місця та повідомлення мережі 5G. Все це робить аналіз захищеності мереж мобільного зв’язку на основі технології 5G економічно доцільним.

Далі представлена економічна оцінка аналізу захищеності:

– короткий опис аналізу;
– визначення вартості аналізу;
– економічна оцінка роботи;
– висновок.

4.2 Короткий опис ідеї

В межах підпункту було проаналізовано і подано у вигляді таблиць:

– зміст ідеї (що пропонується);

– можливі напрямки застосування;

– основні вигоди, що може отримати користувач товару (за кожним напрямом застосування);

– чим відрізняється від існуючих аналогів та замінників.

Перші три пункти подані у вигляді таблиці (таблиця 4.1) і дають цілісне уявлення про зміст ідеї та можливі базові потенційні ринки, в межах яких потрібно шукати групи потенційних клієнтів.

Таблиця 4.1 – Опис ідеї

Зміст ідеї	Напрямки застосування	Вигоди для споживачів (користувачів)
Пропонується створити систему захищеності мереж мобільного зв’язку на основі технології 5G	Виявлення можливості захисту	Технології 5G дає змогу організувати більш надійний захист мереж від можливих атак зловмисників
	Аналіз фінансового стану і рівня захищеності мобільного зв’язку.	Дозволить операторам мереж мобільного зв’язку уникати великих фінансових і репутаційних втрат
	Виділення корисної інформації серед великих масивів даних про мобільних операторів серед захищеності мереж мобільного зв'язку.	Надасть конкурентну перевагу на ринку конкурентів мобільних операторів серед захищеності мереж мобільного зв'язку
	Автоматизація систем моніторингу (відстеження змін у динаміці).	Дає змогу зрозуміти тренди у просуванні свого продукту, торгової марки, компанії і т.д.

Аналіз потенційних техніко-економічних переваг ідеї порівняно із пропозиціями конкурентів передбачає:

– визначення переліку техніко-економічних властивостей та характеристик ідеї;

– визначення попереднього кола конкурентів (проектів-конкурентів) або товарів-замінників чи товарів-аналогів, що вже існують на ринку, та проведення збір інформації щодо значень техніко економічних показників для ідеї власного проекту та проектів конкурентів відповідно до визначеного вище переліку;

– проведення порівняльного аналізу показників: для власної ідеї визначені показники, що мають;

- гірші значення (W, слабкі);
- аналогічні значення (N, нейтральні);
- кращі значення (S, сильні) (таблиця 4.2).

Таблиця 4.2 – Визначення сильних, слабких та нейтральних характеристик ідеї проекту

Технікоекономічні характеристики ідеї	(Потенційні) товари/концепції конкурентів				W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
	Мій проект	Кон-нт 1	Кон-нт 2	Кон-нт 3			
1	2	3	4	5	6	7	8
Форма виконання	Програма	Веб додаток	Веб додаток	Програма			+
Собівартість	Низька	Середня	Низька	Висока	+		
Наявність адміністратора	Не треба, дистанційно	Треба	Треба	Треба	+		

Продовження таблиці 4.2

1	2	3	4	5	6	7	8
Наявність інтернету	Не треба	Необхідно	Необхідно	Не треба		+	
Кросплатформенність	Так	Так	Так	Ні		+	
Складність використання/автономність	Так	Ні	Так	Ні			+

Визначений перелік слабких, сильних та нейтральних характеристик та властивостей ідеї потенційного товару є підґрунтям для формування його конкурентоспроможності.

4.3 Аналіз ринкових можливостей запуску стартап-проекту

Визначення ринкових можливостей, які можна використати під час ринкового впровадження проекту, та ринкових загроз, які можуть перешкодити реалізації проекту, дозволяє спланувати напрями розвитку проекту із урахуванням стану ринкового середовища, потреб потенційних клієнтів та пропозицій проектів-конкурентів. Спочатку проводиться аналіз попиту: наявність попиту, обсяг, динаміка розвитку ринку (таблиця 4.3).

Таблиця 4.3 – Попередня характеристика потенційного ринку

	Показники стану ринку (найменування)	Характеристика
	1	2
1	Головні конкуренти	4

Продовження таблиці 4.3

	1	2
2	Динаміка ринку (якісна оцінка)	Зростає
3	Наявність обмежень для входу (вказати характер обмежень)	Немає
4	Специфічні вимоги до стандартизації та сертифікації	Немає

Середня норма рентабельності в галузі (або по ринку) порівнюється із банківським відсотком на вкладення. За умови, що останній є вищим, можливо, має сенс вкласти кошти в інший проект. За результатами аналізу таблиці зроблено висновок щодо того, чи є ринок привабливим для входження за попереднім оцінюванням. Так, надалі визначаються потенційні групи клієнтів, їх характеристики, та формується орієнтовний перелік вимог до товару для кожної групи (таблиця 4.4).

Таблиця 4.4 – Попередня характеристика потенційних клієнтів

Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
Необхідне програмне забезпечення, яке здатне робити аналіз захищеності мобільного зв'язку	Потенційними цільовими групами є великі компанії, організації, що займаються наданням інформації, компанії, що прагне автоматизувати систему захищеності мережі мобільного зв'язку.	Цільова аудиторія має досить великі масиви даних про зловмисників, аналіз яких може дати великі переваги при подальшому захисті.	Рішення має бути швидким, зрозумілим у використанні (інтуїтивно зрозумілим), не бути сильно дорогим.

Після визначення потенційних груп клієнтів проведено аналіз ринкового середовища (табл. 4.5)

Таблиця 4.5 – SWOT- аналіз

Сильні сторони:	**Слабкі сторони:**
- Ціна - Сильний захист мережі мобільного зв'язку.	- Наявність зловмисників.
Можливості:	**Загрози:**
– Більш широке поширення технологій з підтримкою віртуальної реальності, поява нових технологій моніторингу операторів. – Зростання можливостей потенційних покупців. – Зниження довіри до конкурента.	– Конкуренція. – Зміна потреб користувачів.

Розроблення ринкової стратегії першим кроком передбачає визначення стратегії охоплення ринку: було проведено опис цільових груп потенційних споживачів (таблиця 4.6).

Таблиця 4.6 – Вибір цільових груп потенційних споживачів

Опис профілю цільової групи потенційних клієнтів	Готовність споживачів прийняти продукт	Орієнтований попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу в сегмент
Користувачі смартфонів з віком 10 – 40	Висока	Високий	Висока	Середня
Користувачі смартфонів з ОС	Невисока	Невисока	Низька	Середня

За результатами аналізу потенційних груп споживачів було обрано цільову групу, для якої буде запропоновано даний товар, та визначено стратегію охоплення ринку — стратегію концентрованого маркетингу (компанія зосереджується на одному сегменті).

4.4 Склад, чисельність та фонд заробітної плати виробничих працівників

Таблиця 4.7 – Склад, чисельність та фонд заробітної плати виробничих працівників

Категорії працівників	Наявна чисельність, осіб		Тарифна ставка за розрядом виконуваних робіт, грн / годину	Ефективний фонд робочого часу, годин	Тарифний заробіток, грн.	Преміальний відсоток до тарифного заробітку	Розмір премії, грн.	Річний фонд заробітної плати,	ЄСВ, грн.
	за зміну	на добу							
Виробничі працівники, в тому числі: 1.Основні працівники	2	2	48.29	8	8500	15%	5600	204000	446,19
2.Допоміжні працівники	2	2	39.20	8	6900	15%	5600	165600	46,19
3.Черговий та ремонтний персонал	2	2	22.72	8	4000	15%	5600	96000	446,19
Разом виробничих працівників			110.21		19400			465600	

Основна заробітна плата – це винагорода за виконання роботу відповідно до встановлення норм пращ (годині, виробітку, обслуговування, посадових обов'язків) [32].

Основна заробітна плата виконавців аналізу розраховується на підставі наступних даних:

- трудомісткість виконання робіт $Т_{гол.\ інж}$ та $Т_{інж}$;

- оклад основних працівників за місяць (двадцять два робочих дня) складає 8 500 грн., денна ставка восьми часового робочого дня керівника проекту складає $С_{гол.інж.}$ = 386,36 грн.;

- оклад допоміжніх працівників за місяць (двадцять два робочих дня) складає 6900 грн., денна ставка восьми часового робочого дня інженера складає $С_{інж}$ = 313,64 грн;

- оклад чергового та ремонтног персоналу за місяць (двадцять два робочих дня) складає 4000 грн., денна ставка восьми часового робочого дня інженера складає $С_{інж}$ = 181,81 грн;

- єдиний соціальний внесок ЄСВ = 22%;

- відсоток додаткової заробітної плати = 15%.

Основна заробітна плата виконавців ($З_{осн\ з/пл}$) розраховується за формулою:

$$З_{осн.з/пл}=Т_{гол.інж.} * С_{гол.інж.} + Т_{інж.} * С_{інж.} \quad (4.1)$$

$З_{осн.з/пл}$ = 2 * 386,36 + 2 * 313,64 + 2*181,81 = 1763,62 грн.

Додаткова заробітна плата — це винагорода за понаднормативну працю, трудові успіхи та винахідливість і за особливі умови праці. Вона включає доплати, надбавки, гарантії та компенсації, передбачені чинним законодавством, премії, пов'язані з виконанням виробничих завдань та функцій [50].

Додаткова заробітна плата виконавців (Здодат з/пл) розраховується за формулою:

$$З_{додат.з/п} = З_{осн.з/пл*15/100} \quad (4.2)$$

$З_{додат.з/пл}$ = 1763,62 * 0,15 = 264.54 грн.

Єдиний соціальний внесок - обов'язковий платіж до системи загальнообов'язкового державного соціального страхування, що справляється в Україні з метою забезпечення страхових виплат за поточними видами загальнообов'язкового державного соціального страхування [33].

Внески розраховуються за формулою:

$$В_{соц.} = (З_{осн.з/пл} + З_{додат.з/пл}) * ЄСВ/100 \quad (4.3)$$

$$В_{соц.} = (1763,62+ 264,54)*0,22 = 446,19 \text{ грн}$$

Таблиця 4.8 – Склад, чисельність та фонд заробітної плати адмінперсоналу

Посада	Кіль-кість осіб	Посадовий оклад, грн	Преміальний відсоток до окладу, %	Сума премії грн	Місячна заробітна плата, грн	Річний фонд оплати праці, грн	ЄСВ, грн
Головний інженер	2	477,27	15%	5600	10500	252 000	448,49
Інженер	2	409,09	15%	5600	9000		448,49
Разом управлінського персоналу	10		30%				

- оклад головного інженера за місяць (двадцять два робочих дня) складає 10500 грн., денна ставка восьми часового робочого дня керівника проекту складає $С_{гол.інж.}$ = 477,27 грн .;
- оклад інженера за місяць (двадцять два робочих дня) складає 9000 грн., денна ставка восьми часового робочого дня інженера складає $С_{інж}$ = 409,09 грн;
- єдиний соціальний внесок ЄСВ = 22%;
- відсоток додаткової заробітної плати = 15%;

Основна заробітна плата адмінперсоналу:

$З_{осн.з/пл}$ = 2 * 477,27 + 2 * 409,09 = 1772,72 грн.

Додаткова заробітна плата адмінперсоналу:

$З_{додат.з/пл}$ = 1772,72 * 0,15 = 265,91 грн.

Внески адмінперсоналу:

$В_{соц.}$ =(1772,72+ 265,91)*0,22 = 448,49 грн

4.5 Матеріальних витрати

Вартість витратних матеріалів, необхідних для виконання роботи, визначається виходячи з величини їх витрат, діючих цін і транспортних витрат. В даному розрахунку відносяться використані при виконанні аналізу матеріалів. Калькуляція витрат - Таблиця 4.9.

Таблиця 4.9 – Розрахунок матеріальних витрат

Матеріальні витрати	Норматив у розрахунку на один. продук. (послуг)	Виробнича програма	Обсяг сировини	Ціна	Сума грн
Папір для принтера			1	124	124
Картридж для принтера			1	149	149
Транспортні витрати				14	
Разом					553

4.6 Споживчі послуги

Витрати, пов'язані з утриманням техніки, є складовою всіх витрат підприємства. Усі витрати на утримання техніки поділяють на постійні і

змінні. Постійні витрати - це витрати, які не залежать від інтенсивності використання техніки - кількості годин роботи або виконаного обсягу робіт.

Змінні витрати на техніку безпосередньо пов'язані з її експлуатацією. До них відносять витрати на паливо і мастила, ремонт техніки, оплату праці робітників, які її обслуговують, інші витрати [34].

При розробці методики використовувалося обладнання у вигляді двох комп'ютерів з первісною вартістю 11 700 грн. кожен. Для них необхідно прорахувати витрати на електроенергію і амортизаційні відрахування:

- розмір тарифу споживання електроенергії $С_{ел}$ = 0,9 грн кВт * ч;
- розмір споживання комп'ютером за 8 годин роботи $К_{ел.}$ = 1,76 кВт;
- розмір споживання о світленням за 8 годин роботи $О_{ел.}$ = 2,88 кВт;
- первісна вартість комп'ютера $В_{комп.}$ = 11 700 грн.;
- час використання основного засобу інженером Твик інж =2 місяці;
- час використання основного засобу головним інженером $Т_{вик.гол.інж.}$ = 2 місяці;
- термін амортизації комп'ютера = 36 місяців, норма амортизації комп'ютера за 3 місяці На = 8 %;
- коефіцієнт для розрахунку коштів не враховуючи 20 % ПДВ = 1,2.

Для розрахунку витрат на електроенергію на комп'ютери (Зелкомп), скористаємося формулою:

$$В_{ел.комп} = (Т_{гол.інж} + Т_{інж.}) * К_{ел} * (С_{ел.}/1,2)*8 \quad (4.7)$$

$В_{ел.комп.}$ = (8 + 15) * 1,76 * 0,75 * 8 = 242,88 грн.

Для розрахунку витрат на електроенергію освітлення ($В_{ел.осв.}$), скористаємося формулою:

$$В_{ел.осв} = (Т_{гол.інж+} Т_{інж.})* О_{ел.}*(С_{ел.}/1,2)*8 \quad (4.8)$$

$В_{ел.осв.}$ = (8 + 15) X 2,88 X 0,75 X 8 = 397,44 грн .

Загальні витрати на електроенергію ($В_{заг.ел}$) є сумою витрат електроенергії, що пішла на комп'ютери ($В_{ел.комп}$) і освітлення ($В_{ел. осв}$) скористаємося формулою:

$$В_{заг.ел.} = В_{ел.комп.} + В_{ел.осв} \quad (4.9)$$

$В_{заг.ел}$= 242,88 + 397,44 = 640,32 грн.

Амортизаційні відрахування – процес поступового перенесення вартості основних засобів на продукт, що виготовляється з їх допомогою. Для заміщення зношеної частини основних засобів виробництва підприємства роблять амортизаційні відрахування, тобто відрахування певних грошових сум відповідно до розмірів фізичного і морального зносу засобів виробництва [35].

Таблиця 4.10 – Розрахунок амортизації

Група основних засобів	Норма амортизації	Первісна вартість ОЗ на 01.01	Надійшло ОЗ		Вибуло ОЗ		Сума грн
			дата	пер. вар.	дата	пер. вар.	
1	2	3	4	5	6	7	8
Комп'ютери	8	23400	31,02		31,04		234
Разом	8	23400					

Розрахуємо амортизаційні відрахування по основному засобу за 3 місяці:

$$А_{комп.} = В_{комп.} * (Н_а/100) \quad (4.10)$$

$А_{комп.}$ = 11 700 × 0,08 = 936 грн.

Обчислимо амортизаційні відрахування по основному засобу для кожного з виконавця щодо часу його використання:

$$А_{інж} = А_{комп} * (Т_{вик інж}/12) \quad (4.11)$$

$А_{інж}$ = 936 Х — = 156 грн.

$А_{інж}$ = 936 ×2/12= 156 грн.

Загальна амортизація є сумою амортизації інженера і головного інженера:

$$А = А_{гол.інж.} + А_{інж.} \quad (4.12)$$

А = 78 + 156 = 234 грн.

4.7 Загальний кошторис витрат на аналіз

Кошторис витрат являє собою зведений план усіх витрат підприємства виробничо-фінансової діяльності за певний календарний період. До кошторису включаються витрати основного і допоміжного виробництва, пов'язані з виготовленням та продажем продукції, товарів і послуг, а також на утримання адміністративно-управлінського персоналу.

Таблиця4.11 – Загальний кошторис витрат

№	Найменування статті	Сума, грн.
1	2	3
1.	Витрати на оплату праці	10035,48
2.	Єдиний соціальний внесок	1416,8
3.	Витрати на матеріали	553
4.	Витрати на послуги сторонніх організацій	146,4
5.	Витрати на утримання, експлуатацію та амортизацію обладнання	640,32

Продовження таблиці 4.11

1	2	3
6.	Амортизаційні відрахування	234
7.	Накладні витрати	6166,66
Загалом витрат		19192,66

4.8 Економічна оцінка роботи

Вважаю доцільними витрати на аналіз безпеки мобільних мереж на базі технології 5G. Цей аналіз допоможе доповнювати захист операторів мобільного мережі в майбутньому і звернути увагу на уразливості і повідомлення в мережі 5G. Вивчення аналізу підвищить рівень безпеки мобільних операторів, що дозволить їм уникнути значних фінансових і репутаційних втрат.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

5.1 Аналіз потенційних небезпек

На підвищення ефективності діяльності спеціаліста, котрий виконує процедури розробки систем безпеки мобільного зв'язку впливають різні шкідливі виробничі фактори: електромагнітні поля, інфрачервоне та іонізоване випромінювання, шум й вібрації, статична електрика, недостатність робочої площі, що сприяє росту напруженості. Симптоми впливу комп'ютера на суб'єкта: біль та різь в очах, біль голови, біль в області спини та шиї, загальна втома, втома м'язів рук, підвищена роздратованість, порушення сну, погіршення пам'яті[36].

ДНАОП 0.00-1.31-99 виокремлює структурні механізми організації робочого простору працівника. Для робочих місць, де є комп'ютери застосовують такі показники - мінімальна площа для працівника - 6 ($м^2$), мінімальний об'єм кімнати - 20 ($м^3$). Розраховуючи структурні показники достатнього протору на одну людину враховують площу, де є одна одиниця обладнання зі всім внутрішнім устаткуванням. Це - удільна виробнича площа на одиницю обладнання. До цієї площі додається допоміжна площа на кожну одиницю обладнання, що забезпечує достатню відстань до сусіднього обладнання, + площа проходів, проїздів, площа службових і побутових приміщень [37].

5.2 Аналіз шкідливих і небезпечних виробничих чинників

Небезпечний виробничий фактор при певних умовах впливає на людський організм, що призводить до травм або іншим раптовим пошкодженням здоров'я. Згідно ГОСТ 12.1.003-74. ССБТ «Класифікація небезпечних і шкідливих факторів виробництва» Шкідливі чинники виробництва діляться на фізичні (електричний струм, рухомі автомобілі,

шум, вібрація, недостатнє освітлення, електромагнітні поля, іонізуюче випромінювання); хімічні - шкідливі речовини еа організм в різних біологічних станах; біологічгі - дія різних мікроорганізмів, рослин і тварин; психофізіологічні - фізичні та емоційні перевантаження, психічні навантаження, одноманітність роботи.

У дослідженні робочого простору працівника з обладнання системи аутентифікації виділено декілька шкідливих виробничих чинників, котрі негативно впливають на працівника. Це – забрудненість повітря робочої зони, недостатній рівень освітлення в приміщенні, виробничий шум та вібрації, небезпека ураження електричним струмом, пожежна небезпека. Розглянемо ці чинники більш детальніше.

5.3 Аналіз стану повітря робочої зони

Комп’ютерна техніка — це джерело значного тепловиділення, що може зумовити підвищення температури та зниження вологості повітря у приміщенні. Під впливом комп’ютерів на робочих місцях відбувається трансформація іонного складу повітря. Якщо в 1куб.см чистого зовнішнього повітря налічується 1000 негативних і позитивних іонів, то вже через 5 хв.роботи комп’ютера концентрація легких іонів (позитивно діютчих на організм людини) знижується у 8 разів, а за три години їх кількість становить 0. Висока концентрація у повітрі негативних іонів впливає на розумову та фізичну працездатність. В приміщеннях, у яких розташовані, обладнані комп’ютерами, робочі місця, об’єм повітря на одну людину має бути не меншим 20 $м^3$. Під впливом комп’ютерів та інших технічних пристроїв на робочих місцях упродовж зміни відбувається трансформація іонного складу повітря. ДНАОП 0.03-3.06.-80 «Санітарно-гігієнічні допустимі рівні іонізації повітря виробничих і громадських приміщень» регламентує рівні іонізації повітря приміщень під час роботи за комп’ютером. В приміщенні з комп'ютерами спостерігається підвищення рівня забруднення повітря.

Наприклад, якщо в чистому повітрі концентрація CO2 становить 0,03 %, то в повітрі робочої зони вона сягає від 0,12 — 0,13 до 0,19 %. Особливо велику небезпеку для здоров'я працівників становить підвищена концентрація озону, який вважається не лише подразнюючою, а й канцерогенною речовиною. Відповідно до ДСТУ 12.1 005-88 уміст озону в повітрі робочої зони не повинен перевищувати 0,1 мг/ м^3; уміст окисів азоту — 5 мг/ м^3, уміст пилу – 4 мг/ м^3.

5.4 Аналіз виробничого освітлення

Штучне освітлення переважно використовують люмінесцентні лампи типу ЛБ або ДРЛ. Якщо комп'ютери не працюють, то у робочих приміщеннях треба створити такий же високий рівень освітлення, як і в інших службових приміщеннях. Однак, коли комп'ютери працюють, їхні користувачі, звичайно, багаторазово переводять погляд з екрану в навколишнє середовище й назад, а тому очі вимагають і світлової й темрявої адаптації. Рівень освітлення у приміщенні при роботі комп'ютера не повинен перевищувати. Доцільно для освітлення використовувати лампи денного світла в комбінації з лампами теплового білого світла (жовтого, рожевого), що разом імітують колірну гаму, яка відповідає спектральному складу природного світла в сонячний день[38].

5.5 Аналіз виробничого шуму та вібрації

Шум – хаотичне поєднання різних за рівнем і частотою небажаного шуму. Вухо людини сприймає коливання з частотою від 20 до 2000 Гц, коливання нижче 20 Гц – інфразвук, понад 20 Гц – ультразвук. Інтенсивність звуку, що сприймається на слух – від 10^{-12} Вт/м^2 до 10^2 Вт/ м^2. Діапазон звуку поділяється на: - низьку частоту; - середню частоту; - високу частоту. Вібрація –механічне коливання пружних тіл на низьких частотах з великими

амплітудами, які характеризується частотою, амплітудою, швидкістю та прискоренням [39]. Рівень шуму на робочому місці не повинен перевищувати 65 дБ.

5.6 Аналіз небезпеки ураження електричним струмом

Електричні установки, до яких відноситься практично усе комп'ютерне устаткування, представляють для людини велику потенційну небезпеку, оскільки в процесі експлуатації або проведенні профілактичних робіт людина може торкнутися частин, що знаходяться під напругою, а будь-яка дія струму може привести до електричної травми, тобто до ушкодження організму, викликаного дією електричного струму або електричної дуги. До електричного облаштування робочого місця відносять: комп'ютер, відео монітор, принтер. До допоміжного устаткування відносяться лампи місцевого освітлення, вентилятори і інші електричні прилади. Електроустаткування, перелічене вище, відноситься до установок напругою до 1000 В [40]. Електробезпека в приміщенні залежить від захисту проти короткого замикання; перевантаження; непрямого дотику (в разі порушення ізоляції напруга може потрапити на частини переносних або стаціонарних пристроїв, що проводять, і дотик до них призведе до електротравми); прямого дотику (не можна торкатися оголених дротів, що знаходяться під напругою); пожежі (у разі порушення ізоляції може виникнути струм витоку, який зумовлює іскріння і електричну дугу, які, у свою чергу, призведуть до займання проводки й пожежі).

5.7 Аналіз пожежної безпеки

Пожежна безпека - стан об'єкту, при якому зі встановленою вірогідністю виключається можливість виникнення і розвитку пожежі, а також забезпечується захист матеріальних цінностей. Пожежа - поза

регламентний процес знищення або пошкодження майна, під впливом якого виникають чинники, небезпечні для живих істот і довкілля [41]. У сучасних комп'ютерах дуже висока щільність розміщення елементів електронних систем, у безпосередній близькості один від одного розташовуються сполучні дроти, комунікаційні кабелі. При протіканні по них електричного струму виділяється значна кількість теплоти, що може привести до підвищення температури окремих вузлів до 80-100°С. При цьому можливе плавлення ізоляції сполучних дротів, їх оголення і, як наслідок, коротке замикання, що супроводжується іскрінням, веде до неприпустимих перевантажень елементів електронних схем, які нагріваються та згорають з розбризкуванням іскор. Живлення до електроустановок подається кабелем ліній, які представляють особливу пожежну небезпеку. До заходів з поліпшення умов праці можна віднести: санітарно – гігієнічні заходи (стабілізація показників мікроклімату у приміщенні), організаційні заходи (ефективний розподіл праці, направлений на поліпшення умов існування робітника), інженерно – технічні заходи (конструктивні та схемо-конструктивні заходи перебудови устаткування приміщення).

ВИСНОВКИ

В результаті проведеного дослідження отримані наступні результати:

1. Було представлено детальне дослідження як вразливостей, так і існуючих заходів безпеки, доступних в різних мережах.

2. Телекомунікаційні компанії використовують різні заходи захисту, але їх явно недостатньо, щоб компенсувати весь спектр методів, які можуть застосовувати потенційні порушники. Абоненти навіть великих операторів зв'язку не захищені від несанкціонованого прослуховування дзвінків, перехоплення SMS-повідомлень, перенаправлення викликів і розкрадання грошових коштів з рахунку. Крім того, порушники можуть в будь-який момент визначити поточне місцезнаходження абонента.

3. Як і еволюція механізмів безпеки в дротових мережах, а також в стільникових мережах мобільного зв'язку, існує заклопотаність з приводу поліпшення пов'язаних з безпекою аспектів, зокрема аутентифікації, шифрування і цілісності.

LTE з'явився, щоб відповісти на потреби збільшення пропускної здатності і зниження затримки для поліпшення якості обслуговування. Що стосується безпеки, то вона була розроблена з використанням надійних криптографічних методів, взаємної аутентифікації між елементами мережі і механізмів безпеки, вбудованих в її архітектуру.

4. Для кожного нового покоління мереж зв'язку (2G, 3G, 4G) розроблявся новий радіоінтерфейс, в мережі рухомого зв'язку технології 5G/IMT планується застосовувати як новий радіоінтерефейс, так і еволюцію стандарту LTE-Advanced.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Взлом стільникових мереж: не просто, а дуже просто [Електронний ресурс] - Режим доступу: https://3dnews.ru/923316

2. Атакуем SS7: анализ защищенности сотовых операторов в 2015 году [Електронний ресурс] – Режим доступу: https://habr.com/ru/company/pt/blog/305472/

3. Основные угрозы безопасности в сетях SS7 мобильной связи. Статистика [Електронний ресурс] - Режим доступу: https://cyberway.golos.io/~k2iajg5vpbpo/osnovnye-ugrozy-bezopasnosti-v-setyakh-ss7-mobilnoi-svyazi-statistika

4. Barakovic, S. and L.S. Kapov, 2013. Survey and challenges of QoE management issues in wireless networks. J. Comput. Netw. Commun., 2013: 1-28.

5. Wyner, A.D., 1975. The wire-tap channel. Bell Sy st. Technical J., 54: 1355-1387.

6. Chen, X., K. Makki, K. Yen andN. Pissinou, 2009. Sensor network security: A survey. IEEE Commun. Surveys Tutorials, 11: 52-73.

7. Wood, A.D. and J. A. Stankovic, 2002. Denial of service in sensor networks. IEEE Comput. Mag., 35: 54-62.

8. He, D., J. Wang and Y. Zheng, 2008. User authentication scheme based on self-certified public-key for next generation wireless network. Proceedings of the 2008 International Symposium on Biometrics and Security Technologies (I SB A ST 2008), April 23-24, 2008, IEEE, Islamabad, Pakistan, ISBN:978-1-4244-2427-6, pp: 1-8.

9. Huang, H., N. Ahmed and P. Karthik, 2011. On a new type of denial of service attack in wireless networks: The distributed jammer network. IEEE. Trans. Wirel. Commun., 10: 2316-2324.19.

10. Pelechrinis, K., M. Iliofotou and S.V. Krishnamurthy, 2011. Denial of service attacks in wireless networks: The case of jammers. IEEE. Commun. Suiv. Tutorials, 13: 245-257.

11. Feng, Z., J. Ning, I. Broustis, K. Pelechrinis and S.V. Krishnamurthy et al., 2011. Coping with packet replay attacks in wireless networks. Proceedings of the 8th Annual IEEE Conference on Communications Society on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), June 27-30, 2011, IEEE, Salt Lake City, Utah, ISBN:978-1 -4577-0094-1, pp: 368-376.

12. Oberg, L. and Y. Xu, 2007. Prioritizing bad links for fast and efficient flooding in wireless sensor networks. Proceeding of the International Conference on Sensor Technologies and Applications, October 14-20, 2007, Valencia, Spain, pp: 118-126.22.

13. Chandra, P., 2005. Bulletproof Wireless Security, GSM, UMTS, 802.11 and Ad hoc Security. Newnes Publisher, Newnes, New South Wales, ISBN:9780750677462, Pages: 237.

14. Siddique, S.M. and M. Amir, 2006. GSM security issues and challenges. Proceedings of the 7th IEEE International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, July 19-20, IEEE Computer Society, Washington DC, USA., pp: 413-418.

15. Niemi, V. and K. Nyberg, 2003. UMTS Security. John Wiley and Sons, Chichester, England, ISBN:0-470-85314-X, Pages: 283.

16. Rankl, W. and W. Effing, 2004. Smart Card Handbook. 3rd Edn., John Wiley and Sons, Chichester, England, ISBN:9780470856680, Pages: 1120.

17. Gonzalez-Castano, F.J., J. Vales-Alonso, J.M. Pousada-Carballo, F.I. de Vicente and M.J. Fernandez-Iglesias, 2002. Real-time interception systems for the GSM protocol. IEEE Trans. Veh. Technol., 51: 904-914

18. Biryukov, A., A. Shamir and D. Wagner, 2000. Real time ciyptanalysis of A5/1 on a PC. Proceedings of the 2000 International Workshop on Fast Software Enciyption (FSE), March 20-23,2000, Springer, Berlin, Germany, pp: 1-18.

19. Barkan, E., E. Biham and N. Keller, 2003. Instant ciphertext-only ciyptanalysis of GSM enciypted communication. Proceedings of the 23rd Annual

International Conference on Ciyptology (Ciypto 2003), August 17-21, 2003, Springer, Santa Barbara, California, pp: 600-616.

20. Bocan, V. and V. Cretu, 2006. Mitigating denial of service threats in GSM networks. Proceedings of the 1st International Conference on Availability, Reliability and Security (ARES 2006), April 20-22, 2006, IEEE, Vienna, Austria, ISBN: 0-7695-2567-9, pp: 1-6.

21. Katugampala, N.N., K.T. Al-Naimi, S. Villette and A.M. Kondoz, 2005. Real-time end-to-end secure voice communications over GSM voice channel. Proceedings of the 13th European Conference on Signal Processing, September 4-8, 2005, IEEE, Antalya, Turkey, ISBN:978-160-4238-21-1, pp: 1-4.

22. Rekha, A.B., B. Umadevi, Y. Solanke and S.R. Kolli, 2005. End-to-end security for GSM users [speech coding method]. Proceedings of the IEEE International Conference on Personal Wireless Communications (ICPWC 2005), Januaiy 23-25, 2005, IEEE, New Delhi, India, ISBN:0-7803-8964-6, pp: 434-437.

23. Zhang, M. and Y. Fang, 2005. Security analysis and enhancements of 3GPP authentication and key agreement protocol. IEEE. Trans. Wirel. Commun, 4: 734-742.

24. Shin, M., J. Ma, A. Mishra and W.A. Arbaugh, 2006. Wireless network security and interworking. Proc. IEEE, 94: 455-466.

25. Putz, S. and R. Schmitz, 2000. Secure interoperation between 2G and 3G mobile radio networks. Proceedings of the 1st International Conference on 3G Mobile Communication Technologies, March 27-29, 2000, IET, London, UK., pp. 28-32.

26. Husso, M., 2006. Performance analysis of a WimAX system under jamming. MSc Thesis, Helsinki University of Technology, Espoo, Finland,

27. Al-Humaigani, M., D.B. Dunn and D. Brown, 2009. Security transition roadmap to 4G and future generations wireless networks. Proceedings of the 41st Southeastern Symposium on System Theoiy (SSST 2009), March 15-17, 2009, IEEE, Tullahoma, Tennessee, ISBN:978-l-4244-3324-7, pp: 94-97.

28. Park, Y. and T. Park, 2007. A survey of security threats on 4G networks. Proceedings of the IEEE Workshops on Globecom, November 26-30,2007, IEEE, Washington, DC., USA., ISBN:978-1-4244-2024-7, pp: 1-6.

29. Vintila, C.E., V.V. Patriciu and I. Bica, 2011. A J-PAKE based solution for secure authentication in a 4G network. Proceeding of the 10th WSEAS International Conference on Electronics, Hardware, Wireless and Optical Communications (NEHIPISICT1), February 20-22, 2011, WSEAS, Cambridge, ISBN: 978-960-474-276-9, pp. 42-47.

30. The Evolution and Future Perspective of Security in Mobile Communications Networks João Pavia1, Diogo Lopes1, Pedro Cristóvão1, Pedro Sebastião1,2, Américo Correia1 (PDF) The Evolution and Future Perspective of Security in Mobile Communications Networks. Available from: [Електронний ресурс] - Режим доступу: https://www.researchgate.net/publication/320601176_The_Evolution_and_Future_Perspective_of_Security_in_Mobile_Communications_Networks[accessed Dec 22 2020]

31. Об'єкти та суб'єкти інвестиційної діяльності [Електронний ресурс] - Режим доступу: https://buklib.net/books/35263/

32. Види заробітної плати та їх характеристика [Електронний ресурс]- Режим доступу: https://pidru4niki.com/16400116/ekonomika/vidi_zarobitnoyi_plati_harakteristika

33. Єдиний соціальний внесок [Електронний ресурс] – Режим доступу : https://index.minfin.com.ua/ua/labour/social/

34. Андрійчук, В. Г. Економіка аграрних підприємств [Електронний ресурс] / В.Г. Андрійчук. - Режим доступу: https://kneu.edu.ua/ua/science_kneu/scientific_schools/agrm/agrm_praci/agrm_prazi/ecpidapk/

35. Амортизація [Електронний ресурс] - Режим доступу: https://pidru4niki.com/84344/ekonomika/amortizatsiya_osnovnih_zasobiv_pidpriyemstva

36. Кучерявий В. С. Охорона праці. Навчальне видання /В. С. Кучерявий. - Львів, «Оріяна-Нова», 2007.- 360с.

37. Кобевнік В. Ф. Охорона праці / В. Ф. Кобевнік. - К.: Вища шк., 1990. - 286 с.

38. Жидецький В. Ц. Основи охорони праці / В. Ц. Жидецький. - Львів: Афіша, 2000. - 351с.

39. ДСН 3.3.6.042-99 Санітарні норми мікроклімату виробничих приміщень / упоряд. та голов. ред. Л. Х. Муляр, О. П. Авдієнко, А. А. Нечепорчук. - К.: Держспоживстандарт України, 2000 – 23 с.

40. Кучерявий В. П. Охорона праці: навчальний посібник / В. П. Кучерявий, Ю. Є. Павлюк, А. Д. Кузик. – К: Оріяна – Нова, 2007. – 368 с.

41. НАПБ Б.03.002-2007 Норми вивчення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою / упоряд. та голов. ред. М. Я. Откідач, О. О. Сізіков, В. С. Куликівський, В. Ф. Слєпченко, М. В. Білошицький, К. П. Чеботаєв. – К., 2007. – 25 с.