ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ФАКУЛЬТЕТ ЕКОНОМІЧНОЇ ІНФОРМАТИКИ
КАФЕДРА КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Пояснювальна записка

до дипломної роботи

магістра

на тему: “Розробка мобільного застосунку та його захист від несанкціонованого доступу”

Виконав: студент 2 року навчання,
за освітнім ступенем “магістр”
зі спеціальності 125 “Кібербезпека”
Бофанов А.В.
Керівник: д.т.н., проф. Євсеєв С.П.

Рецензент: к.т.н., доц. Шматко О.В.

Харків – 2020 рік

ЗМІСТ

ВСТУП

У наш час освіта відіграє дуже важливу роль у житті кожної люди. Будь-яка робота потребує навичок, та безумовно, великого обсягу знань, які нам може запропонувати школа та університет. У цьому ланцюзі важливу роль відіграє викладач, бо саме ця людина не тільки вас навчить чогось нового, та й безумовно може надихати на гарні справи. Аби полегшити роботу викладача, у наш час, різні університети застосовую новітні технології, які надають можливість виконувати рутинну бюрократичну частку своєї роботи швидше та зручніше.

Протягом навчального року перед викладачем стає необхідність виконувати обов’язкові задачі що повторюються, наприклад:

відмічати наявність студентів;

оцінювати поточну успішність студентів;

перевіряти та редагувати розклад;

робити нотатки до занять.

Всі ці проблеми я намагався вирішити у моїй дипломній роботі. Також, моєю метою було у рамках розробки застосування створити платформу для швидкого та зручного додавання нового функціоналу для вирішення задач не що можуть з’явитися пізніше.

У еру інформації, особисті данні користувачів є одним з найважливіших ресурсів у світі. Якщо ці данні попадають до рук злочинців кошті користувача, функціонування структури в якої він працює, та навіть стабільність політичної ситуації в країні стає під загрозу. Тому вкрай важливо, у час розробки застосунку знати и бути готовим протидіяти усім кіберзагрозам що існують чи можуть з’явитися.

Перевагою для Харківського національного економічного університету імені Семена Кузнеця є те, що це застосування дозволить зменшити витрати часу на щоденні обов’язки професорсько-викладацького складу кафедри.

Головними перевагами мобільних застосунків є їх доступність у будь який час та у будь якому місці. Завдяки сучасним принципам дизайну, задачі які раніше вимагали використовування та зберігання різноманітних паперів, зараз

можуть бути виконані двома рухами пальців. Для користування застосунком необхідний тільки смартфон з підключенням до мережі що є майже в кожного українця в кишені. Наявність пристрою з встановленим застосункам надає викладачу змогу постійно бути в курсі усіх важливих подій в житті університету, та виконувати термінові задачу у будь якому місці без доступа к робочій станції.

Метою роботи є розробка мобільного застосунку для планування розкладу, ведення журналу відвідування та успішності, а також його захист від відомих кібератак.

Об’єктом роботи є мобільного застосунку та його захист від несанкціонованого доступу.

Предметом роботи є розробка мобільного застосунку та захист.

Для вирішення мети необхідно:

Розробити мобільний застосунок враховуючи потреби викладачів.

Проаналізувати можливі загрози несанкціонованого доступу до даних користувача через мобільний застосунок.

Розробити механізми захисту від проаналізованих кіберзагроз.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ЗАСТОСУНКУ: “КАБІНЕТ ВИКЛАДАЧА”

1.1 Системи інноваційно-активного університету

У наш час, в Україні панує стереотип о застарілості державної системи освіти. Цей стереотип з’являєтеся через порівняння університетів з сучасними онлайн курсами, що використовують новітні технології та підходи що спрощують доступ до інформації та інтеграцію з стейкхолдерами. Не зважаючи на виску якість освіти, державні університети насправді мають дещо застаріли структури роботи з інформацію в наслідок чого вони мають недостатній вплив на розвиток економічної системи країни. Як вирішення цієї проблеми, у ХНЕУ ім. Семена Кузнеця було впроваджено концепцію інноваційно-активного університету (ІАУ), що спрощує доступ до інформації та її прозорість, а також усуває більшість корупційних схем.

Концепція інноваційно-активного університету в ХНЕУ ім. Семена Кузнеця реалізується на основі корпоративної інформаційно-освітньої системи що базується на моделі взаємодії відкритих систем. Однак, майже всі сучасні протоколи можуть функціонувати в відкритому вигляді, що створює можливість для кібератак та ускладнює захист системи, у зв’язку з чи при розробці таких систем є необхідним використання додаткових заходів безпеки.

У ХНЕУ ім. Семена Кузнеця ця проблема вирішується за допомогою технології PKI що базується на технології цифрового підпису за стандартом X.509. На базі цієї технології було розроблено адаптивну систему захисту інформації (АСЗІ) основним елементом якої є центральна система ключів що забезпечує автоматичний контроль електронного документообороту, що знижує ризики появи корупційних схем та кібератак.

Окрім цього сервер LDAP що є частиною центральної системи ключів забезпечує безпечну автентифікацію користувачів у системі. На рис. 1.1 зображена фізична архітектура віртуальної мережі для розгортання системи комплексного захисту інформації [1].

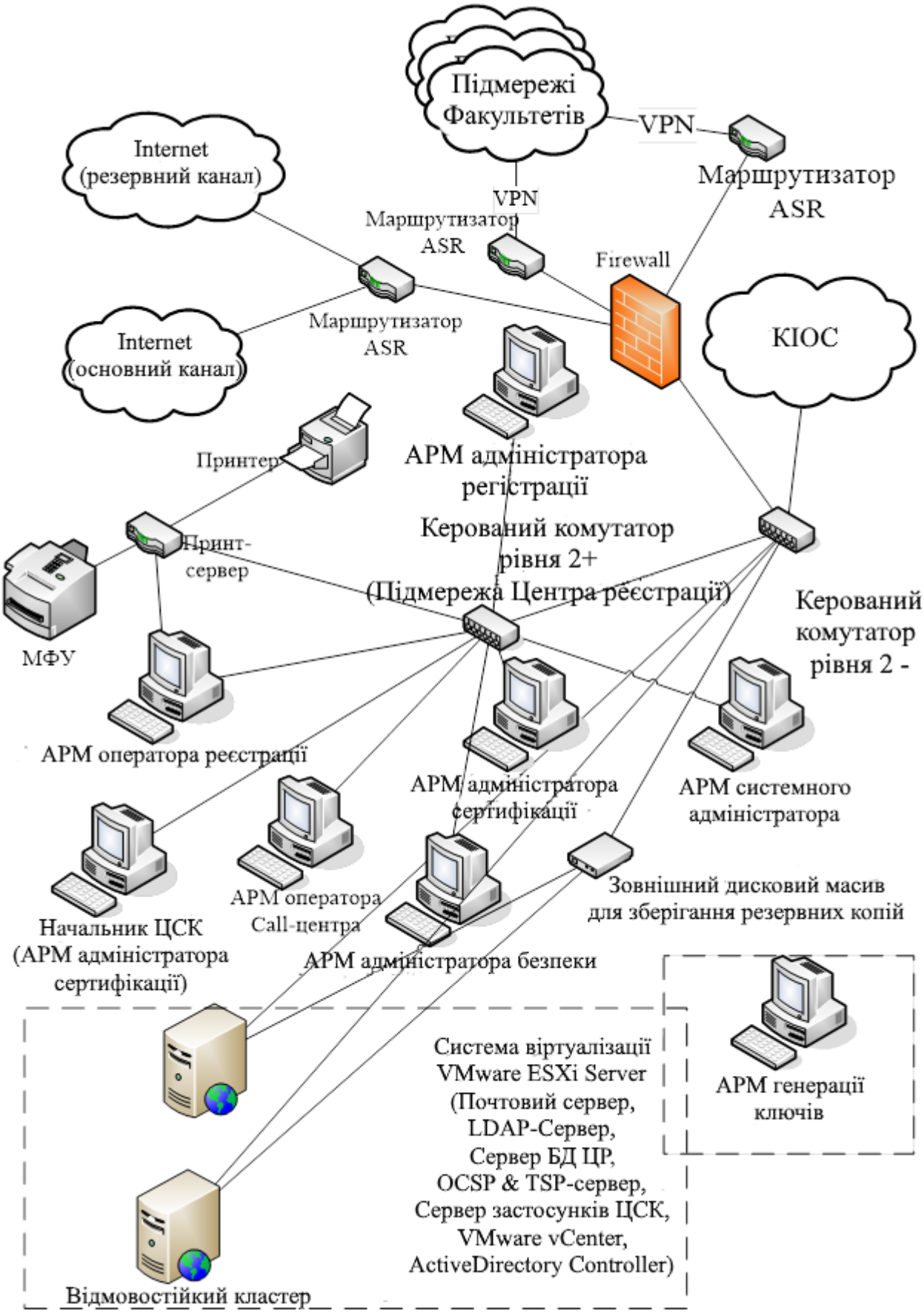

Рисунок 1.1 – Фізична мережа інфраструктури PKI

Приклад реалізації такий системи захисту наведено у рис 1.2 [2].

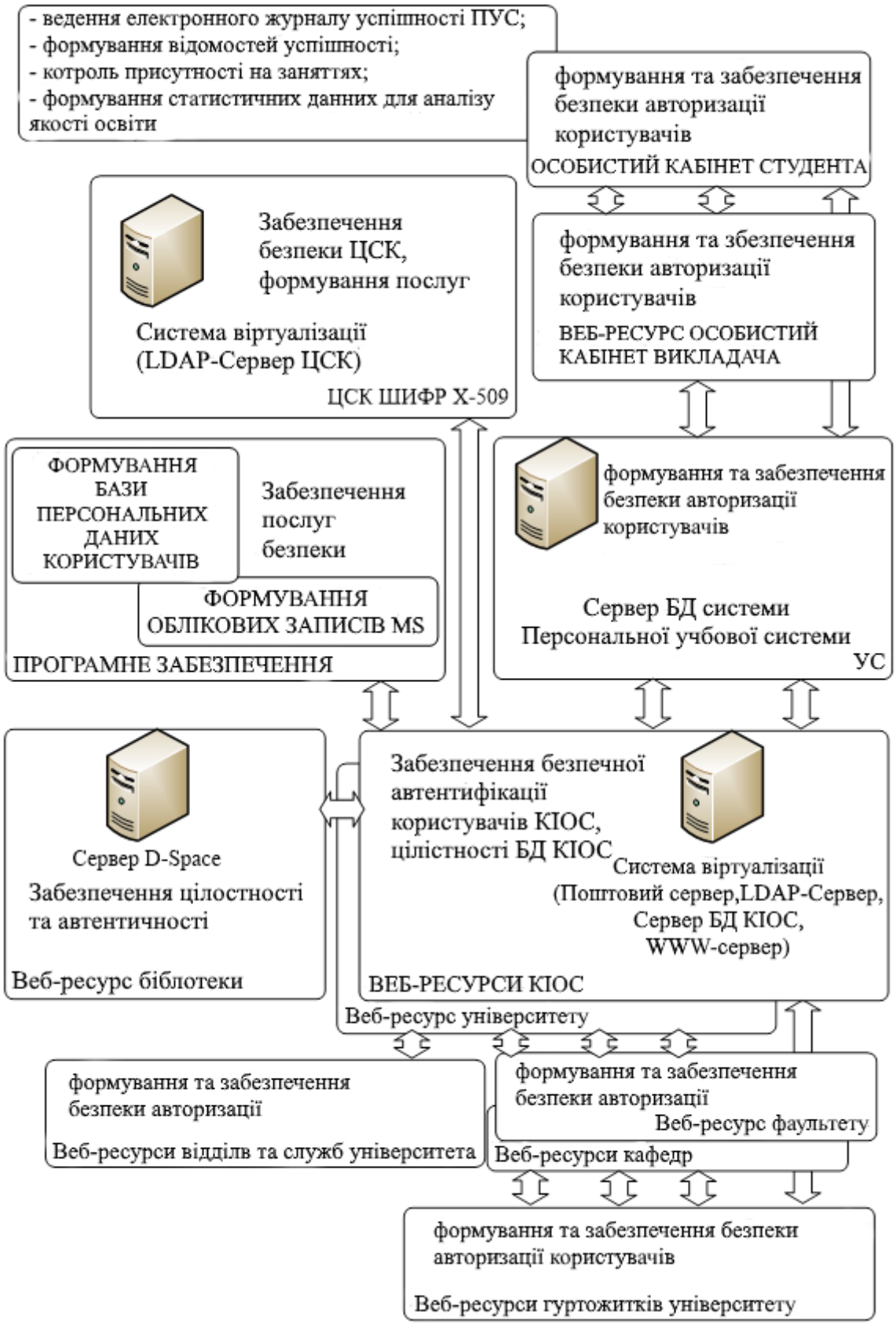

Рисунок 1.2 – Структурна схема корпоративній інформаційно-освітній системи інноваційно-активного університету

Індикатором користувача у цій системі є цифровий підпис що можна перевірити за допомогою сертифікату ключа, що може бути отриманий з підтверджуючого центру.

Система інноваційно-активного університету базується не веб технологіях, що дозволяє надати відкритий доступ до різноманітної інформації авторизованим користувачам. Але, ця система потребує відповідного захисту від несанкціонованого доступу.

1.2 Принципи роботи мережі мобільного радіозв'язку

Основною перевагою любого мобільного застосунку є можливість підключення до мережі з будь якої точки що є у покритті того чи іншого оператора. Ця перевага існує завдяки технологіям бездротового доступу до мережі інтернет, що реалізується за допомогою технології LTE. Тому, для планування захисту мобільного застосунку, необхідно розуміння технології функціонування мобільного зв'язку.

На сучасному етапі розвитку системи інформаційного зв'язку спостерігається попит на послуги, які передбачають значне розширення пропускної здатності мережі доступу. Такі завдання можна вирішити за допомогою використання дротових і бездротових засобів зв'язку. Для операторів мережі LTE та їх абонентів цікава ще одна сфера бездротового зв'язку: вирішення поточних проблем збільшення пропускної здатності мережі шляхом об'єднання з іншою системою радіодозв'язку. З цієї причини бездротовий доступ, який висвітлює технологію LTE, став дуже ефективним засобом модернізації мереж.

Стратегія мобільних операторів щодо об'єднання мереж 3G/LTE з іншими мережами радіодозв'язку пропонує ряд переваг. Надаючи абоненту свободу вибирати, як підключитися під час подорожі, оператори можуть "володіти" цим користувачем довше, а їх послуги можуть стати потенційно більш значущими. Інші оператори проводять стратегію плавного розширення своїх мобільних широкосмугових мереж, додаючи до основної стільникової інфраструктури

принципово різні технології радіодозв'язку, такі як LTE, DVB-H або неліцензійні технології мобільного доступу (UMA, Unlicensed Mobile Access).

У той же час, LTE розглядається як одне з доповнень до стратегії розгортання 3G/LTE. Технологія LTE забезпечує формування Концепції використання багатьох осяжних точок доступу з метою формування широкосмугового каналу та забезпечення доступу абонентів до нього в умовах, як у місті, так і в будь-якій точці сільської місцевості.

Можливість трансформувати і відкрити новий вектор обчислювальної потужності надає провайдерам величезні можливості, що сильно впливає на їх конкурентоспроможність на ринку. Більшість мереж доступу, які зараз працюють, є високою вартістю, низькою надійністю і не надають нових видів інформаційно-комунікаційних послуг. Вже сьогодні абонентам стільникових мереж доступні послуги електронної комерції та електронних банківських послуг, відеоконференції, відеоконференції і тому подібне. Однак перспективні послуги – дистанційне навчання, віддалений якісний доступ в Інтернет – вимагають збільшення швидкості. Збільшення швидкості необхідне для таких сервісів, як цифрове телебачення, фільми на вимогу, потокове відео. Нарешті, щоб отримати доступ до телевізора з якістю DVD або високою роздільною здатністю. При цьому в сучасних мережах передачі даних пропускна здатність коливається від 2 Гбіт/с до 1 ТБ на головному рівні, від 10 Мбіт/с до 1,1 Гбіт/с на рівні локальної мережі доступу (LAN) і лише від 50 Кбіт/с до 1,5 Мбіт/с на рівні доступу абонента.

Стандарт GSM використовує мультистанційний доступ з тимчасовим поділом (ущільнення каналу – TDMA), що дозволяє одночасно розмістити 8 голосових каналів на одній частоті носія. RPE мовлення кодек, LTP з регулярним імпульсом збудження і 13 Кбіт/с швидкість перетворення мовлення, використовується як пристрій, що визначає мовлення, і структурна схема показана на рис. 1.3.

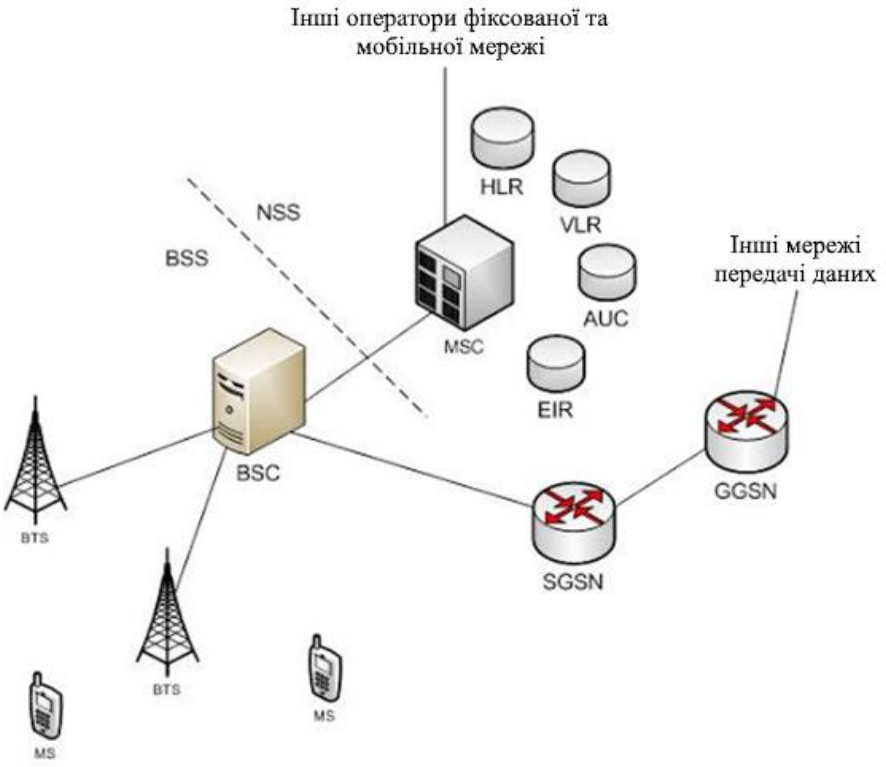

Рисунок.1.3 – Структурна схема GSM

Обробка мовлення в цьому стандарті здійснюється в рамках прийнятої системи DTX (Переривчаста передача), яка дозволяє вмикати передавач тільки тоді, коли користувач починає розмову і вимикає її в паузах і в кінці розмови. Система DTX керує детектором мовлення VAD (Детектор голосової активності), який виявляє і виділяє інтервали мови з шумом і шумом без мови, навіть коли рівень шуму може бути одного рівня з мовним рівнем.

Для захисту від помилок, які виникають в радіоканалах, використовується кодування і кодування блоків за допомогою функцій комутаційного рулону. Підвищення ефективності кодування і змішування при низькій швидкості переміщення рухомих мобільних станцій досягається шляхом повільного перемикання робочих частот під час сеансу зв’язку (зі швидкістю 217 стрибків/с). Для модульування радіосигналу використовується спектральна частотна маніпуляція Gauss з мінімальним зсувом частоти (GTMSK). Швидкість передачі даних GSM становить 9,6 Кбіт/с.

UMTS – це стільникова технологія 3G-покоління. Технологія W-CDMA використовується як спосіб передачі даних через повітряний простір. UMTS

також часто називають 3GSM для того, щоб підкреслити приналежність технології до мереж третього покоління 3G і її безперервність у розвитку від GSM мереж до рис. 1.4 Представлено структурний візерунок.

Однак на даний момент найвищими швидкостями є 384 Кбіт/с для мобільних станцій R99 і 3,6 Мбіт/с для станцій HSDPA в режимі передачі даних від базової станції до мобільного терміналу. Але це також безсумнівне поліпшення над значенням 9.6 Кбіт/с при передачі даних через GSM-канал, або за допомогою 9,6 Кбіт/с (зі швидкістю 14,4 Кбіт/с в CDMAOne) і разом з іншими технологіями бездротових даних (CDMA2000, PHS, WLAN), що дозволяє отримати доступ до Інтернету та інших сервісів через мобільні станції.

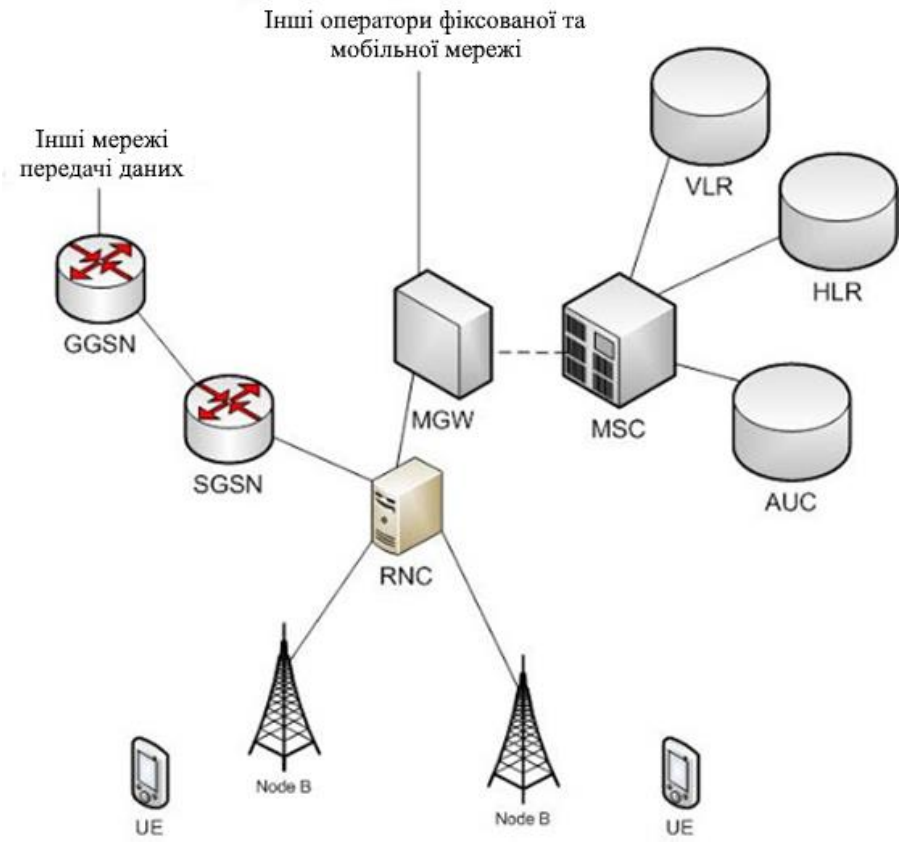

Рисунок 1.4 – Структурна схема UMTS

З 2006 року мережі UMTS були повсюдними в технології високошвидкісної пакетної передачі даних від базової станції до мобільного терміналу HSDPA, підходу, який був прийнятий для генерації 3,5G.

Системи LTE/SAE (Long-Term Evolution / System Architecture Evolution) забезпечують безпрецедентний рівень продуктивності як для нових, так і для вже використаних діапазонів частот в мережах 3GPP і 3GPP2, структурна схема показана на рис.1.5. Система LTE, специфікації якої запропоновані Проектом партнерства третього покоління 3GPP) для публікації у випуску 8, є наступним вагомим кроком у розвитку мобільного радіозв'язку.

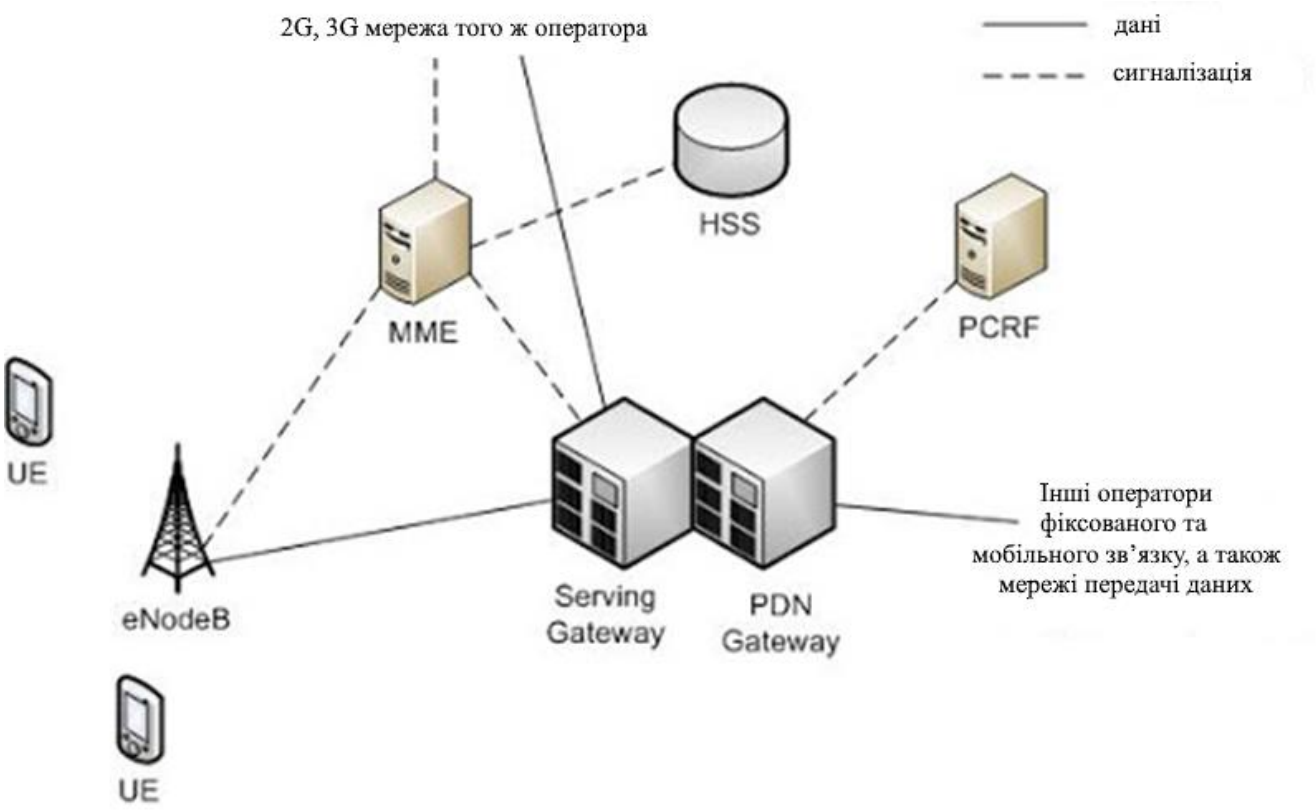

Рисунок.1.5 – Структурна схема LTE

Стандарт дозволяє такі сервіси, як інтерактивне телебачення, створене користувачами потокове відео, складні ігри та професійні послуги. Система LTE використовує технологію радіодоступу OFDM (розділення каналів ортогональних частот) разом з останніми досягненнями в технології антени.

На додаток до LTE, 3GPP визначив плоску архітектуру мережі з IP в рамках програми розвитку архітектури системи (SAE). Метою та суттю концепцій LTE/SAE є ефективна підтримка широкого комерційного використання будь-якої послуги на базі IP. Ця архітектура заснована і є подальшим розширенням

існуючих мереж GSM / WCDMA, що робить його набагато простішим в експлуатації і як розгортатися плавно і економічно ефективно. Нова модель плоскої архітектури означає, що тільки два типи (базові станції і шлюзи) потрібно буде модернізувати, щоб впоратися з трафіком, коли він значно збільшується.

LTE – універсальна технологія, її характеристики відповідають і навіть перевищують вимоги 3GPP. Максимальна швидкість передачі даних у нижнього каналу може перевищувати 200 МБ/с, а затримка відповіді мережі радіодозв'язку (RAN) становить менше 10 мс. Пропускна здатність гнучка від 1,4 МГц до 20 МГц для носіїв, які розміщуються в нових і вже використовуваних діапазонах частот. Підтримка продажів з дворівневим відділом частоти та дуплексом відділу часу

Можлива передача ретрансляції та роумінг на існуючі мобільні мережі (попередні покоління), що дозволяє з самого початку надати абонентам доступ до мобільного зв'язку, де б вони не були. Оператори можуть бути гнучкими у впровадженні технології LTE з урахуванням особливостей вже роботи мережі, спектру частот і комерційних завдань, які передбачається вирішувати за допомогою широкосмугового доступу, включаючи мультимедійні сервіси.

На рис. 1.6 спостерігається тенденція мобільного зв'язку.

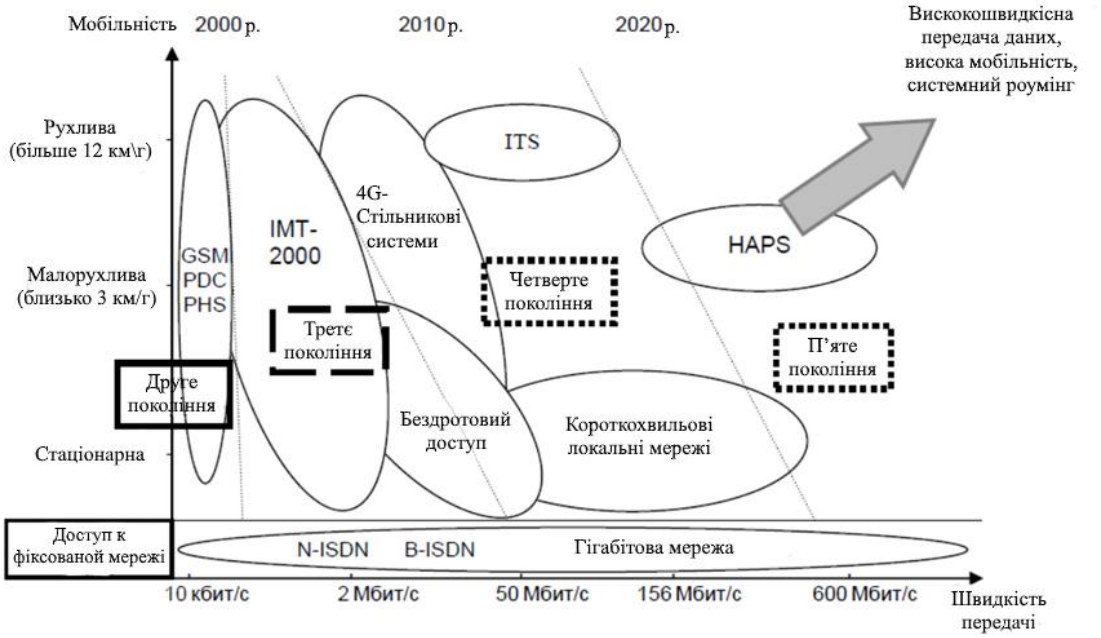

Рисунок 1.6 – Тенденції мобільного зв'язку

Аналіз рис 1.5 показав, що розвиток мобільних технологій сьогодні випереджає обчислювальні можливості стаціонарних та портативних ПК, що значною мірою дає можливість вважати цей вектор найбільш перспективним для передачі інформації. Сьогодні саме технологія “G” забезпечує швидкий розвиток різних гаджетів, що дозволяє практично повністю замінити ПК і їх модифікації.

Концепція 4G представлена в рис.1.7, де максимальна якість обслуговування клієнтів мережі забезпечується шляхом поділу функціоналу на три частини (прикладний, мережевий і фізичний рівні).

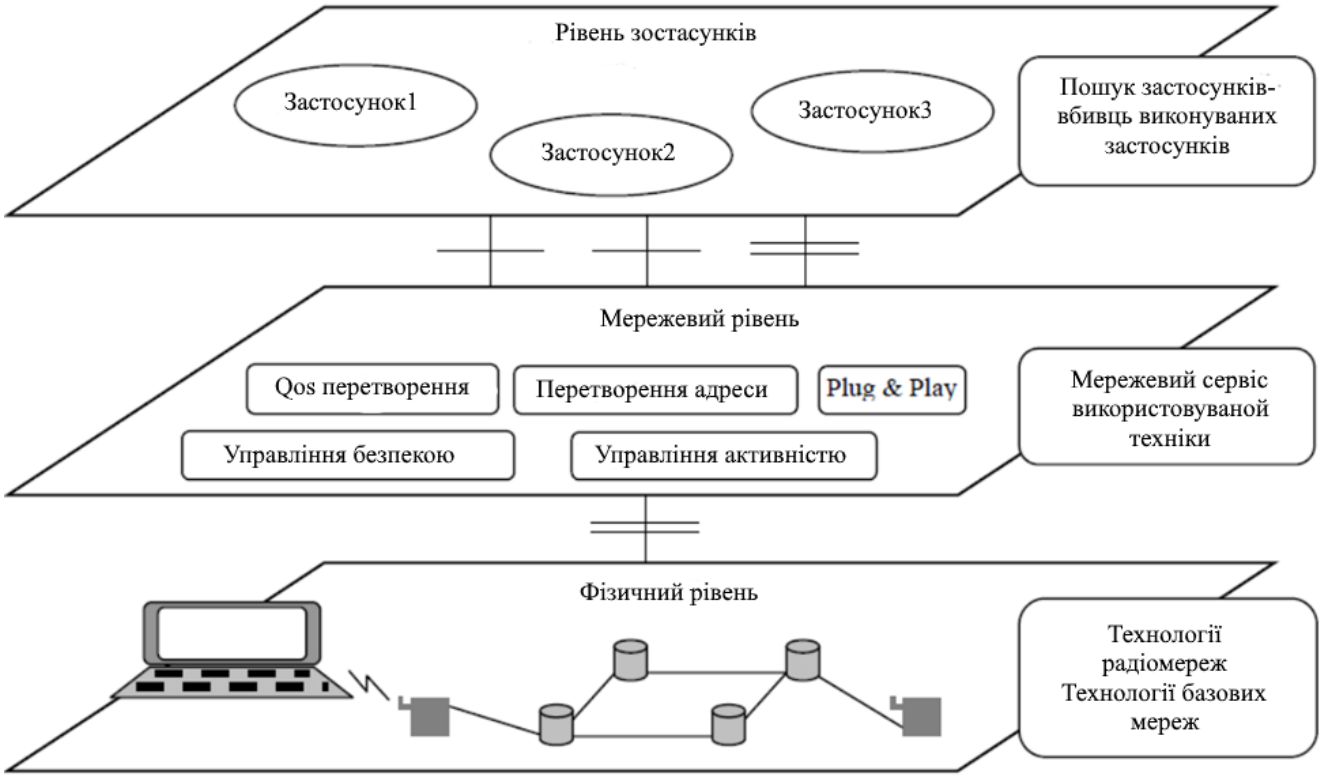

Рисунок 1.7 – Концепція технології 4G

Сучасний ITS заснований на синтезі програмного та апаратного забезпечення:

Автоматичне обладнання, що визначає місцезнаходження, використовується для визначення місця розташування на основі супутникової навігації;

Радіоканал для обміну цифровою та мовною інформацією між автомобілем і моніторинговим центром, або SUDA;

Програмно-картографічні інструменти для візуалізації простору-часу інформації про розвиток транспортно-технологічного процесу;

Засоби швидкого реагування – забезпечує інформаційне управління можливими інцидентами через автоматичну систему диспетчерського управління.

Такий підхід забезпечує надійний онлайн контроль транспортних засобів.

Концепція HAPS (High Altitude Platforms) розглядається як нова мережева інфраструктура між наземними і супутниковими мережами (платформи HAPS розташовані на висоті 20 км в стратосфері). Експерименти і попередні розрахунки показали, що абонентські термінали з антеною діаметром 5 см забезпечують високошвидкісний трафік (до 1 Мбіт/с) при дуже низьких швидкостях зв'язку.

1.3. Архітектура, послуги, позначення складової LTE, LTE-A, LTE-pro

Однією з вимог стандарту системи LTE є підтримання пікової швидкості завантаження з мережі до 100 Мбіт/с. Крім того, сама технологія дозволяє ще більш високі швидкості, такі як більше 200 Мбіт/с.

Перш за все, стандарт LTE здатний працювати в діапазоні частот різної ширини, починаючи від значень помітно нижче 5 МГц (1,5 МГц) до 20 МГц. Технологія LTE також може бути реалізована на основі різних принципів поділу сигналів, частоти і скроневих – FDD (Frequency Divission Duplex) і TDD (Time Division Duplex). Це означає, що оператор може спочатку запустити LTE в "нових" діапазонах, де зазвичай легше отримати смуги 10 МГц або навіть 20 МГц, а потім поступово вводити LTE у всіх доступних діапазонах.

Архітектура стандарту LTE базується на еволюції існуючої основної мережі GSM/WCDMA до спрощення операцій та органічного, економічно ефективного рис.1.8.

Є тільки два основних пристроїв на рівні користувача SAE: базова станція LTE (eNode) і шлюз SAE Gateway. Базові станції LTE підключаються до допоміжної мережі за допомогою інтерфейсу S1 – Core Network – RAN. Ця плоска архітектура зменшує кількість вузлів, необхідних для захисту з'єднання.

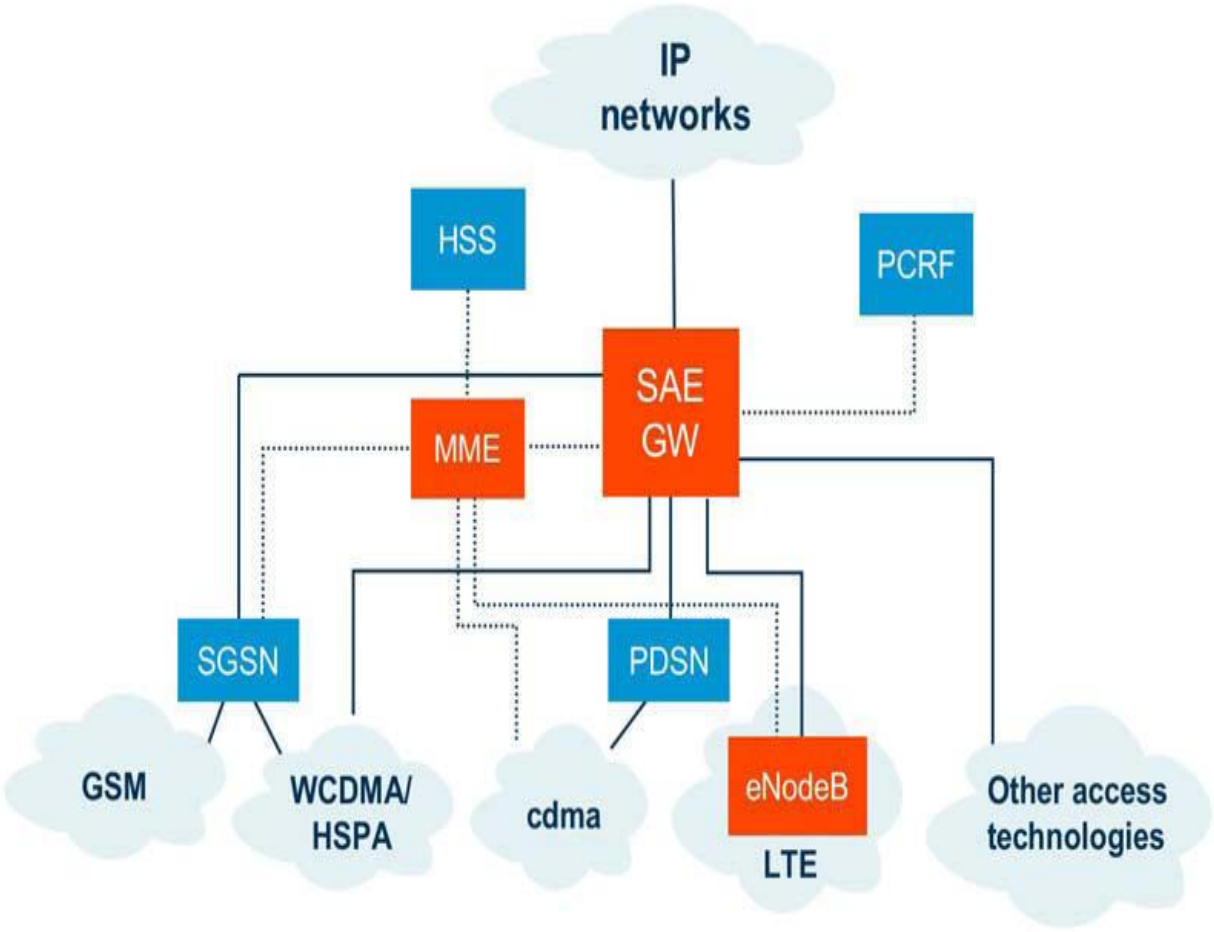

Рисунок 1.8 – Архітектура та концепція LTE-SAE

Існуючі системи 3GPP (GSM і WCDMA/HSPA) і 3GPP2 (CDMA2000 1xRTT, EV-DO) інтегровані в систему LTE за допомогою стандартизованих інтерфейсів, які забезпечують оптимізовану мобільність. Для систем 3GPP це означає наявність інтерфейсу сигналу між CDMA RAN і новою мережею підтримки. Ця інтеграція забезпечить підтримку як для подвійних, так і для одного радіо-вікенду, що дозволить плавно міграції до LTE.

Керування сигналом, наприклад, для мобільності, підтримується сутністю керування мобільністю (MME), присвяченою шлюзу. Це спрощує оптимізацію розгортання мережі та дозволяє гнучко масштабувати свою потужність.

Домашній абонентський сервер (HSS) підключається до пакетного ядра через інтерфейс на основі Diameter, а не систему сигналізації SS7, яка використовується в мережах GSM та WCDMA.

Існуючі системи GSM та WCDMA/HSPA інтегровані з LTE з використанням стандартизованих інтерфейсів між SGSN та мережами підтримки LTE.

LTE використовується як в парних (FDD), так і в непарних (TDD) областях спектра. Загалом, FDD є більш ефективним і являє собою більш високий потенціал для використання пристрою та інфраструктури, в той час як TDD може виступати в якості доповнення, наприклад, для заповнення прогалин. Оскільки обладнання LTE практично ідентичне для FDD і TDD випадків (за винятком фільтрів), це дозволяє операторам значну економію в ресурсах в масштабі, а також забезпечить широку доступність продуктів FDD.

До основних вимог до технології LTE відносяться:

Збільшення спадающої лінії зв’язку та стандартів даних для піку піку каналу;

масштабована пропускна здатність від 1,4 до 20 МГц вихідного каналу і при передачі інформації з космосу;

спектральна ефективність, з поліпшенням доступу до високошвидкісного пакета;

Час очікування 5 мілісекунд для IP-пакета;

Оптимізована робота: низька мобільна швидкість від 0 до 15 км/год; Високоефективна підтримка від 15 до 120 км/год, функціональна від 120 до 350 км/год, опора – 350–500 км/год.

Специфікації LTE успадковують всі діапазони частот, які використовуються в UMTS (табл. 1.1). Існує 13 груп FDD та 8 груп TDD.

Таблиця 1.1 – діапазони частот, підтримувані LTE

Частотний діапазон	Висхідний канал (UL), МГц	Спадний канал (DL), МГц	Розведення між UL і DL, МГц	Тип дуплексу
1	1920-1980	2110-2170	130	(у 200 за все)
2	1850-1910	1930-1990	20	(у 200 за все)
3	1710-1785	1805-1880	20	(у 200 за все)
4	1710-1755	2110-2155	355	(у 200 за все)
5	824-849	869-984	20	(у 200 за все)
6	830-840	875-885	35	(у 200 за все)
7	2500-2570	2620-2690	50	(у 200 за все)
8	880-915	925-960	10	(у 200 за все)
9	1749,9-1784,9	1844,9-1879,	60	(у 200 за все)
10	1710-1770	2110-2170	340	(у 200 за все)
11	1427,9-1452,9	1475-1500	23	(у 200 за все)
...				
13	777-787	746-756	21	(у 200 за все)
14	788-798	758-768	20	(у 200 за все)
...				
33	1900-1920	1900-1920	–	(у 200 за все)
34	2010-2025	2010-2025	–	(у 200 за все)
35	1850-1910	1850-1910	–	(у 200 за все)

Закінчення таблиці 1.1

Частотний діапазон	Висхідний канал (UL), МГц	Спадний канал (DL), МГц	Розведення між UL і DL, МГц	Тип дуплексу
36	1930-1990	1930-1990	–	(у 200 за все)
37	1910-1930	1910-1930	–	(у 200 за все)
38	2570-2620	2570-2620	–	(у 200 за все)
39	1880-1920	1880-1920	–	(у 200 за все)
40	2300-2400	2300-2400	–	(у 200 за все)

Різні типи інформаційних потоків передаються як у верхнього, так і в низхідному каналах.

У верхнього каналу їх три – Цільова державна служба (PUSCH), Канал управління (PUCCH) і Канал вільного доступу (PURCH). По-перше, це передача інформації про користувача. Канал керування містить такі відомості, як індикатор якості каналу, повідомлення про підтвердження доставки (ACK/NACK) і запит розкладу (на наявних ресурсах). Громадський канал і канал управління ніколи не транслюються одночасно тим же АП. Для перенесення каналу керування використовується одна одиниця ресурсів у кожному з слотів одного і того ж підрамкового. Залежно від формату PUCCH існує чотири варіанти його розташування на сітці ресурсів (рис. 1.9), визначені змінною *M*..

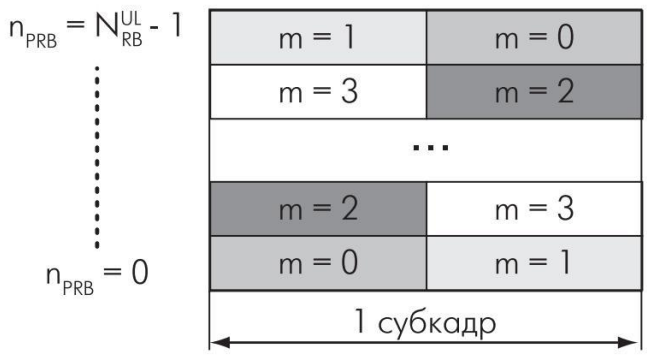

Рисунок 1.9 – Параметри розташування PUCCH у нижнього за течією каналу

Канал вільного доступу служить для запиту початкової ініціалізації в мережі, коли ви в дорозі, коли ви переходите з режиму очікування в активний режим. У низхідній спрямованості інформаційних каналів набагато більше. Це фізичний канал зворотного зв'язку (PDSCH), фізичний канал керування зворотним зв'язком (PDCCH), фізичний багатоадресний канал (PMCH), канал фізичного мовлення (PBCH), канал формату фізичного керування (PCFICH) і канал індикатора змішаного повторного запиту (HRA) Метою загального каналу є передача даних на конкретні абонентські пристрої. Канал керування PDCCH передає таблиці з призначенням ресурсів каналу абонентських пристроїв, як у низхідних, так і на верхнього рівня каналів. Канал PCFICH, який передається в кожному підрамнику, перераховує номери символів OFDM, які використовуються для трансляції повідомлень каналу PDCCH. Канал PHICH призначений для підтвердження доставки даних в каналі.

LTE-Advanced – це назва специфікації 3GPP на основі підключення LTE до WiMAX 2, офіційно визнана стандартом бездротового зв'язку четвертого покоління 4G.

WiMAX підходить для:

Підключення точок доступу Wi-Fi один з одним та іншими сегментами інтернету;

Забезпечення бездротового широкосмугового зв'язку як альтернативи виділеним лініям і DSL. Надання високошвидкісних послуг з передачі даних та телекомунікацій;

WiMAX дозволяє доступ до Інтернету на високих швидкостях, з набагато більшим покриттям, ніж мережі Wi-Fi. Це дозволяє використовувати технологію як "основні канали", за які слідують традиційні DSL і виділені лінії, а також локальні мережі. Як наслідок, такий підхід дозволяє створити масштабовані високошвидкісні мережі в масштабах цілих міст.

Набір переваг притаманний всій сім'ї WiMAX, але його версії істотно відрізняються один від одного. Кожна специфікація WiMAX визначає діапазони робочих частот, пропускну здатність, потужність випромінювання, методи

передачі та доступу, методи кодування та модуляції сигналу, принципи повторного використання радіочастот та інші показники. Таким чином, системи WiMAX на основі версій стандартів IEEE 802.16e та d практично несумісні. Труси по кожній версії нижче.

802.16-2004 (також відомий як 802.16d – Фіксований WiMAX). Специфікація була затверджена в 2004 році. Використовується мультиплексування ортогональних частот (OFDM), а фіксований доступ підтримується в районах з прямою лінією зору або без них. Користувальницькі пристрої є стаціонарними модемами для позакритих установок, а також картами PCMCIA для ноутбуків. У більшості країн діапазони 3,5 і 5 ГГц відкладені для цієї технології. За даними WiMAX Forum, вже існує близько 175 реалізацій фіксованої версії.

802.16-2005 (також відомий як 802.16e – мобільний WiMAX). Специфікація була затверджена в 2005 році. Версія, оптимізована для підтримки мобільних користувачів, підтримує ряд конкретних функцій, таких як ручна робота, режим простою та роумінг. Використовується масштабований доступ OFDM (SOFDMA), працювати можна за наявності або немає лінії зору, діапазони частот для мобільних мереж WiMAX: 2.3; 2,5; 3,4-3,8 ГГц. Конкурентами 802.16e є мобільні технології третього покоління.

Основна відмінність двох технологій полягає в тому, що фіксований WiMAX дозволяє обслуговувати тільки “статичних” абонентів, а мобільний орієнтований на роботу з користувачами, що рухаються зі швидкістю до 120 км/год. Мобільність означає наявність функцій роумінга і “безшовне” перемикання між базовими станціями при русі абонента (як це відбувається в стільникових мережах). У приватному випадку мобільний WiMAX також може бути використаний для обслуговування фіксованих користувачів.

Основні вимоги до LTE-Advanced:

Високий ступінь функціональності для надання широкого спектру високошвидкісних послуг на світовому ринку зі значною економічною ефективністю та якістю;

Можливість взаємодії з іншими системами радіодозв’язку, включаючи повну сумісність LTE (Rel’8);

Гармонізація та сумісність пристроїв підписки в міжнародному масштабі;

Впровадження роумінгу по всьому світу

Підтримка ширини каналу до 40 МГц включно;

Можливість організації ширшої смуги каналів (до 100 МГц), яка потенційно може забезпечити максимальну швидкість передачі даних 3 Гбіт/с в Downlink і 1,5 Гбіт/с в Uplink;

Забезпечення спектральну ефективність каналів Downlink до 15 біт/Гц на 4x4 MIMO і до 6,75 bps/Hz на 2x4 MIMO в каналах Uplink.

Таким чином, стандарт LTE-A є логічним продовженням стандарту LTE, що розширює спектр послуг на основі синтезу технічних рішень.

Подальшим розвитком стандарту на шляху до технології 5G стала технологія LTE-pro, заснована на вимогах стандарту 3GPP Rel.13 або вище: удосконалення BTC, Підтримка підтримки “громадської безпеки”, такої як D2D і ProSe – подвійне підключення до невеликих сот і відповідна мережева архітектура, покращена агрегація частот, взаємодія з Wi-Fi, LAA на 5 ГГц, 3D / FD-MIMO, підтримка позиціонування в приміщенні, точка-точка роботи для однієї комірки, а також затримка сигналу.

На рис. 1.10 представлені специфікації 4G і 5G технологій.

Ключові вимоги до технології 5G:

пікова швидкість до 20 Гбіт/с на лінії вниз (тобто від базової станції до мобільної); і до 10 Гбіт/с у зворотному порядку;

Практична швидкість на одного абонента до 100 Мбіт/с і більше;

спектральна ефективність в мережах 5G в 2–5 разів вище, ніж 4G. На лінії вниз: 30 бп/Гц, на лінії вгору – 15 бп/Гц;

Підвищення енергоефективності на два порядки величини. Це дозволить пристроям Інтернету речей працювати без підзарядки акумулятора протягом 10 років;

тимчасова затримка на радіо інтерфейсі до 0,5 мс (для наднадійних міжмоутерних сервісів URLLC) і до 4м (для надширокококалкові мобільні сервіси eMBB);

швидкість руху абонента до 500 км/год;

Загальна кількість підключених пристроїв становить до 1 млн/км$^{2.}$.

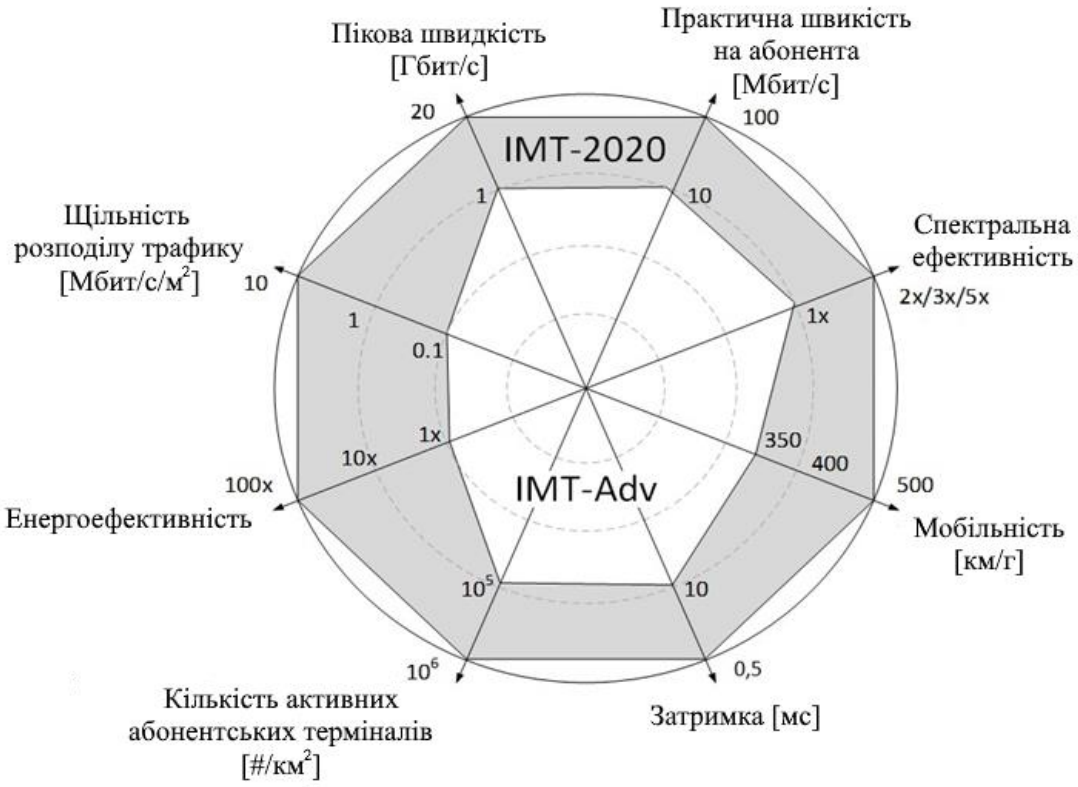

Рисунок 1.10 – Основні моменти технології 4G та 5G

Так, аналіз рис.1.10 показав основні тенденції розвитку мобільних радіотехнологій мереж, що дає можливість найближчим часом поставити їх на перше місце за допомогою технологій комп’ютерних мереж і технологій для обчислювальних ресурсів.

1.4 Мережі на основі протоколу Diameter

Diameter – це протокол передачі даних, який використовується в комп’ютерних мережах для автентифікації, авторизації та обліку різних послуг (AAA – Аутентифікація, авторизація, облік).

Цей протокол використовується в підсистемі мультимедіа для забезпечення автентифікації, авторизації та ідентифікації, а також обміну обліком між об’єктами IMS. Протокол Diameter побудований в типі Peer-to-Peer. Таким чином, кожен хост може виступати в якості сервера і клієнта, дозволяючи "гнучко" використовувати однорангові властивості цього протоколу, в залежності від архітектури мережі. Протокол Diameter на початку роботи автентифікує користувача і формує посилку на сайт, який обслуговує запит. Якщо процес автентифікації завершено успішно, облікові дані користувача входять до складу повідомлення про відповідь, і повідомлення надсилається назад до відповідного клієнта Diameter.“

Існує три типи агентів Diameter:

Relay Agent (агент-ретранслятор)- використовується для перенаправлення повідомлення відповідного одержувача, в залежності від інформації, що міститься в повідомленні. Ретранслятор може об’єднати запити з різних областей (або регіонів) до певної області, яка усуває обтяжливий параметр серверів доступу до мережі кожного разу, коли ви змінюєте сервер Diameter.

Proxy Agent (проксі-агент) використовується для перенаправлення повідомлень, але на відміну від ретранслятору, проксі-агент може змінювати вміст повідомлення і, отже, надавати додаткові послуги, застосовувати правила для різних повідомлень або виконувати завдання адміністрування для різних областей. На рис. 1.11 показує, як проксі-агент використовується для переспрямування повідомлення до іншого домену. Якщо проксі-агент не змінює вміст вихідного запиту, буде достатньо ретранслятору.

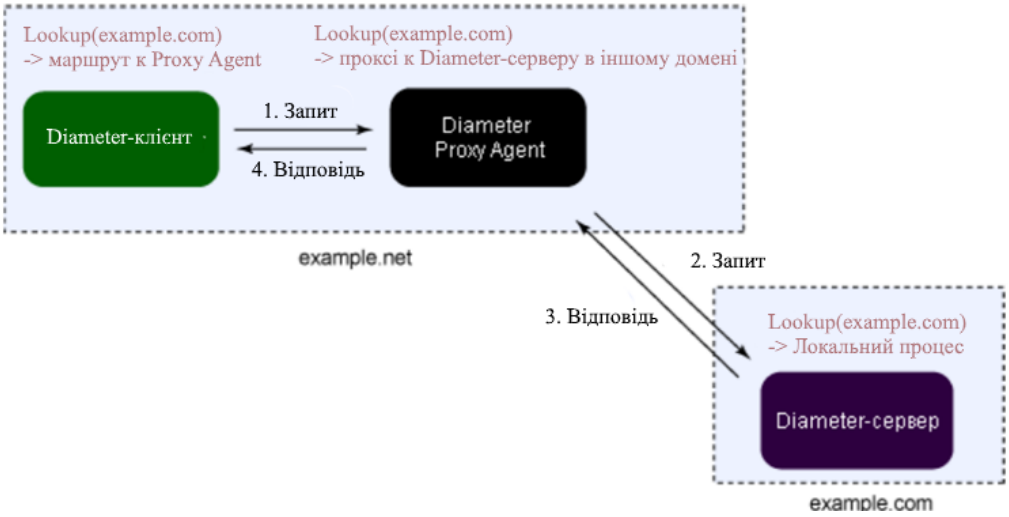

Рисунок 1.11 – Proxy Agent

Redirect Agent (агент-перенаправлення)- забезпечує формування бази даних для вузлів мережі Diameter. Після отримання повідомлення цей агент формує перенаправлення запиту на проксі-сервер, який забезпечує функції безпеки та відокремлює серверну частину від клієнта, працюючи на різних рівнях, рис.1.12 зображує роботу Redirect Agent.

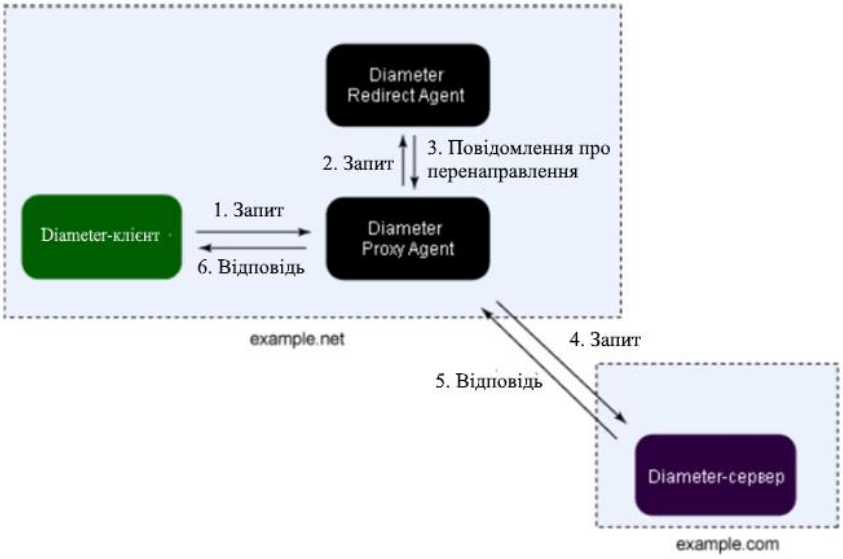

Рисунок 1.12 – Redirect Agent.

Сценарії роботи проксі-агенту (рис. 1.10 і 1.11) майже однакові, але на цей раз проксі-агент не знає адресу відповідного вузла Diameter в example.com. Отже, він шукає інформацію в агенті перенаправлення власної області, щоб отримати адресу.

На додаток до цих агентів є спеціальний агент під назвою Translation Agent -агент-перетворення (забезпечує перетворення повідомлення з одного протоколу AAA на інший). Translation Agent корисний компанії або постачальнику послуг для інтеграції бази даних користувачів двох прикладних доменів при збереженні оригінальних протоколів AAA. На рис. 1.13 показано, як один агент перетворює протокол RADIUS в протокол Diameter, або навпаки Diameter в Radius, чи Diameter TACACS+.

Рисунок 1.13 – Translation Agent

Diameter-повідомлення — це модуль що забезпечує обмін повідомленнями між вузлами Diameter. Для різних цілей протокол Diameter має різні типи повідомлень, залежно від коду команди. Розглянемо декілька з них:

Accounting-Request – визначає повідомлення як те що містить інформацію об аккаунті користувача;

Capability-Exchange-Request – надає інформацію про можливості Diameter-вузла, який передає повідомлення. Код команди використовується для ідентифікації наміру повідомлення, а реальні дані передаються як пари атрибут-значення (Attribute-Value-Pair – AVP). Протокол Diameter має заданий набір загальних атрибутів і призначає кожному атрибуту відповідну семантику. Ці AVP передають AAA деталі (інформацію, таку як маршрутизація, безпека та можливості) між двома вузлами Diameter. Крім того, кожна пара AVP пов’язана з форматом AVP Data Format, який визначається в протоколі Diameter (наприклад, OctetString, Integer32), тому значення кожного атрибута має слідувати формату даних. На рис. 1.14 показує зв’язок між повідомленнями Diameter та їх AVP.

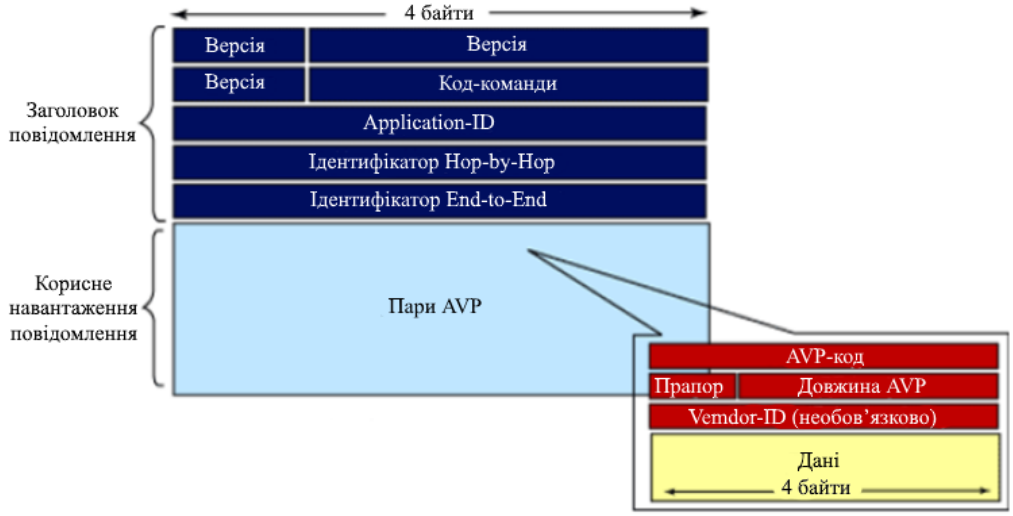

Рисунок 1.14 – Формат пакету Diameter

Diameter забезпечує зв'язок з протоколами транспортного рівня TCP або SCTP, що дозволяє використовувати кіберпростір на цьому рівні. Зв'язок використовується для обміну даними в комп'ютерних мережах на основі логічного підключення. Сеанс відноситься до взаємодії між клієнтом Diameter і сервером Diameter протягом певного періоду часу. Ідентифікатор сеансу потім використовується для ідентифікації певного сеансу під час подальшого обміну інформацією.

На рис. 1.15 Показано структурні схеми сеансу.

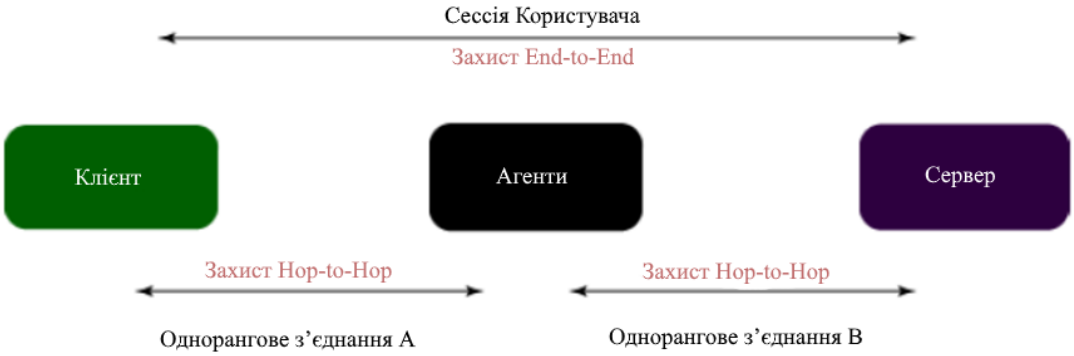

Рисунок 1.15 – Сеанс і з'єднання в Diameter

Автентифікація та авторизація пари AVP залежить від програми та того, що вони не визначені в базовому протоколі. Після отримання повідомлення запиту автентифікації, сервер Diameter може додати Authorization-Lifetime AVP в

відповідь. Ця пара AVP використовується для позначення кількості часу в секундах, що потрібно Diameter клієнту для повторної автентифікації. Після закінчення терміну дії то допустимого Auth-Grace-Period сервер Diameter видаляє сеанс зі списку сеансів і вивільняє всі ресурси, виділені йому.

Щоб забезпечити автентичність джерела даних, протокол може ініціювати перевірку автентичності джерела повідомлення.

Повідомлення про кінець сеансу використовується лише в контексті автентифікації та авторизації, і лише тоді, коли підтримувався стан сесії. Для облікових служб замість цього використовується повідомлення про зупинку обліку.

Таким чином, протокол Diameter забезпечує необхідний набір послуг автентифікації (AAA), підтримує надійне злиття на основі підключення до протоколів транспортування TCP, STCP, що дозволяє користувачеві забезпечити необхідний рівень якості обслуговування (QoS).

1.5 Загрози безпеки пакетної мережі

Широке використання мобільних мереж четвертого покоління полегшило мільярдам користувачів доступ до швидкого Інтернету. Однак не иільки смартфони, планшети та комп’ютери, масово підключаються до 4G. Висока швидкість передачі даних та мінімальні затримки в мережах LTE уможіть їх використання для побудови інфраструктури Інтернету речей. Однак головним питанням використання цих технологій є питання надання послуг безпеки: конфіденційності, цілісності, автентичності, доступності та залучення. Так, у 2016 році фахівці Positive Technologies провели роботи з безпеки сигнальної мережі 4G. Виявлені проблеми дозволяють відключити одного або багатьох абонентів, перехопити інтернет-трафік і SMS-повідомлення, відключити обладнання оператора і виконати інші нелегітимні дії. Процес використання вразливостей в мережах 4G не вимагає від зловмисника важко досяжності інструментів або високого рівня майстерності, і це дозволяє легко отримати необхідну конфіденційну інформацію. Крім того, можливість синхронізації особистих

облікових записів комп'ютерних мереж і технології 4G надає зловмиснику "простий" доступ до персональних даних в локальній домашній мережі.

Для мереж четвертого покоління консорціум 3GGP розробив нову архітектуру мережевого ядра System Architecture Evolution (SAE). Основним елементом нової архітектури є ядро мережі пакетів Evolved Packet Core (EPC), рис. 1.16. Мережі 4G побудовані за принципом All IP Network, що дозволяє передавати не тільки дані в пакетному середовищі, але і голосові дзвінки.

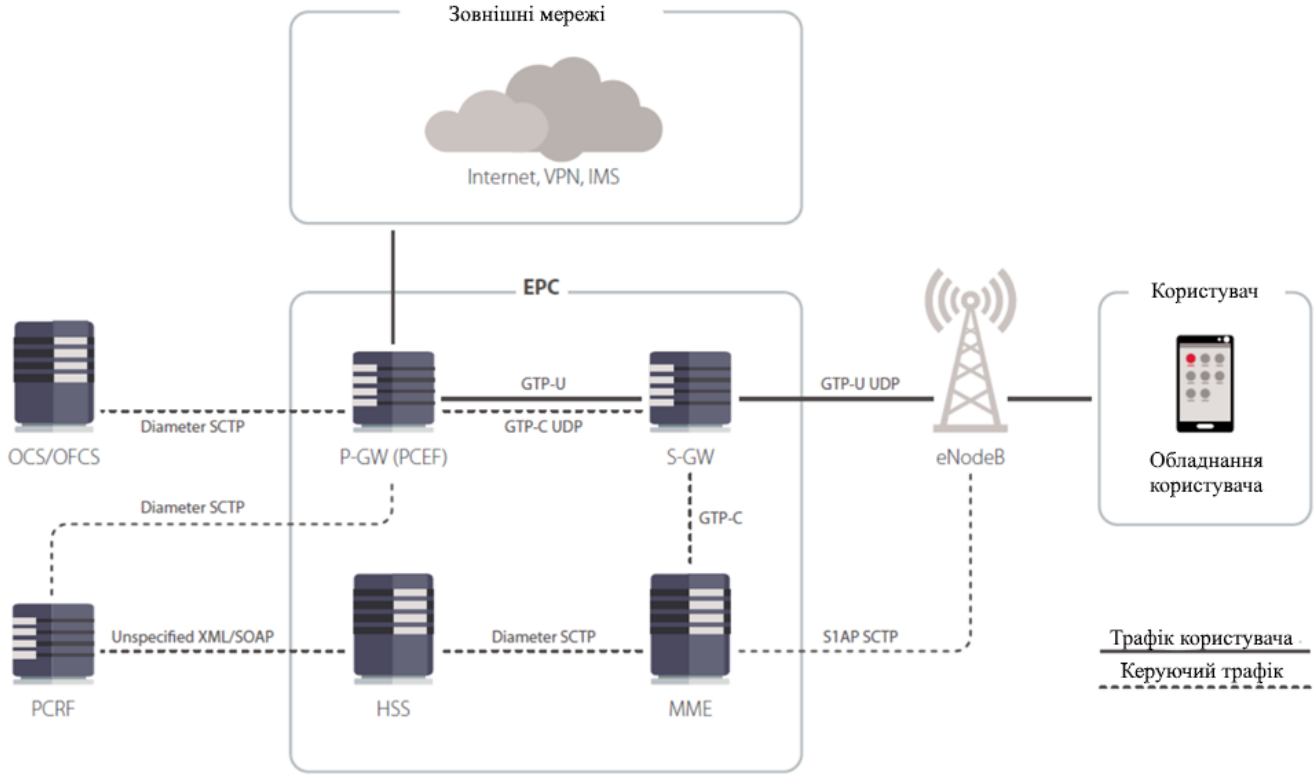

Рисунок 1.16 – Структура ядра пакетной мережі Evolved Packet Core (EPC)

Основними компонентами ядра пакетної мережі є:

Сервер даних абонента (HSS) забезпечує зберігання абонентської інформації;

Шлюх обслуговування S-GW забезпечує передачу та обробку даних користувачів між пристроями користувача (UE) та підсистемою базових станцій LTE (eNodeB) оператора;

Пакетний шлюз (P-GW) – управляє потоком даних, що передаються в зовнішні пакетні мережі;

Вузол управління мобільністю (MME) надає можливість перемикання між базовими станціями та роумінгом (забезпечує аутентифікацію UE шляхом взаємодії з HSS, а також вибору шлюзу S-GW);

Вузол EPC надає функції перевірки та фільтрації мережевих пакетів для їх вмісту (DPI);

GPRS Tunneling Protocol (GTP), S1 Application Protocol (S1AP), Diameter та інші протоколи – забезпечують взаємодію вузлів EPC.

Аналіз ядра показав, що з базових послуг надається тільки автентичність (тільки для ідентифікації користувача).

Таким чином, розробники не розглядають жодних практичних підходів до надання базових послуг безпеки, що дозволяє реалізувати будь-які загрози в цій технології. Для зловмисників практично достатньо стежити за сигнальним каналом, щоб забезпечити реалізацію загроз або отримати службову інформацію з сигнального трафіку.

Так, через відсутність крипто-алгоритмів, для надання послуг конфіденційності (захист даних при передачі даних від пасивних атак), цілісністності (захист даних при зберіганні) і автентичності (справжність джерела повідомлення) можна виділити наступні “класичні” атаки, рис. 1.17.

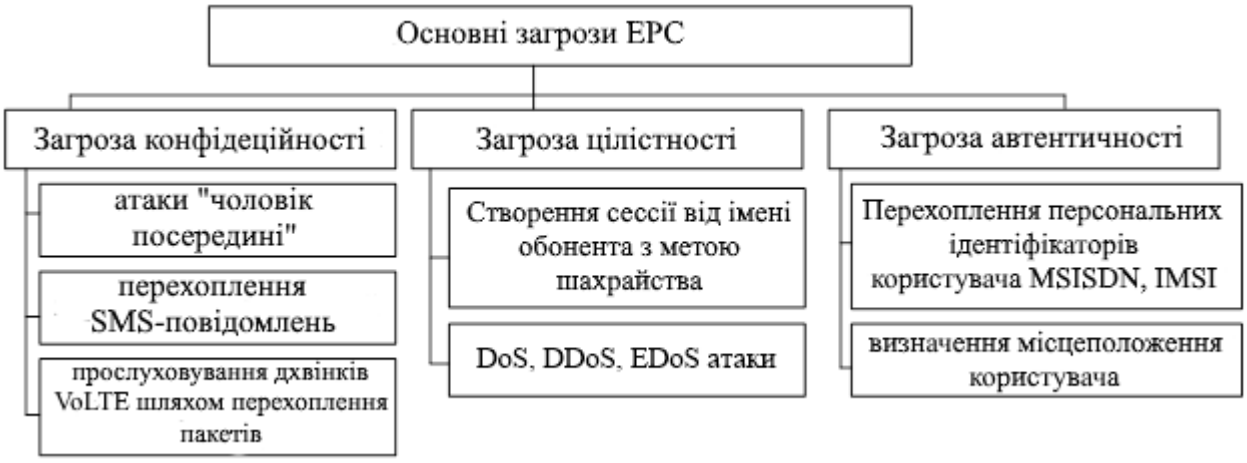

Рисунок 1.17 – Ключові види атак

На рис. 1.18, 1.19 наведено приклади реалізації атаки: вибір ідентифікатора кінцевої точки тунелю (TEID), визначення IMSI абонента, що дозволяє зловмиснику здійснювати практично будь-яку загрозу/шахрайство. Крім того, така критична відсутність базових рішень з безпеки, практично дозволяє “легко” зламати додатки електронного банкінгу і отримати доступ до будь-якої інформації, розташованої на всіх гаджетах користувачів.

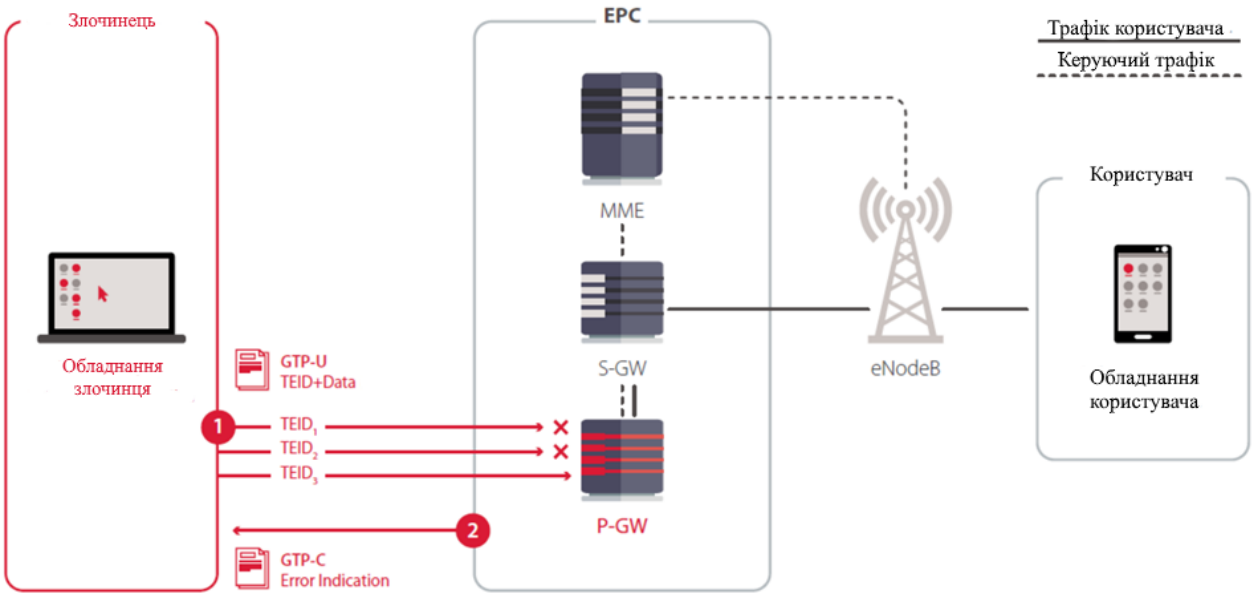

Рисунок 1.18 – Вибір ідентифікатора кінцевої точки тунелю (TEID)

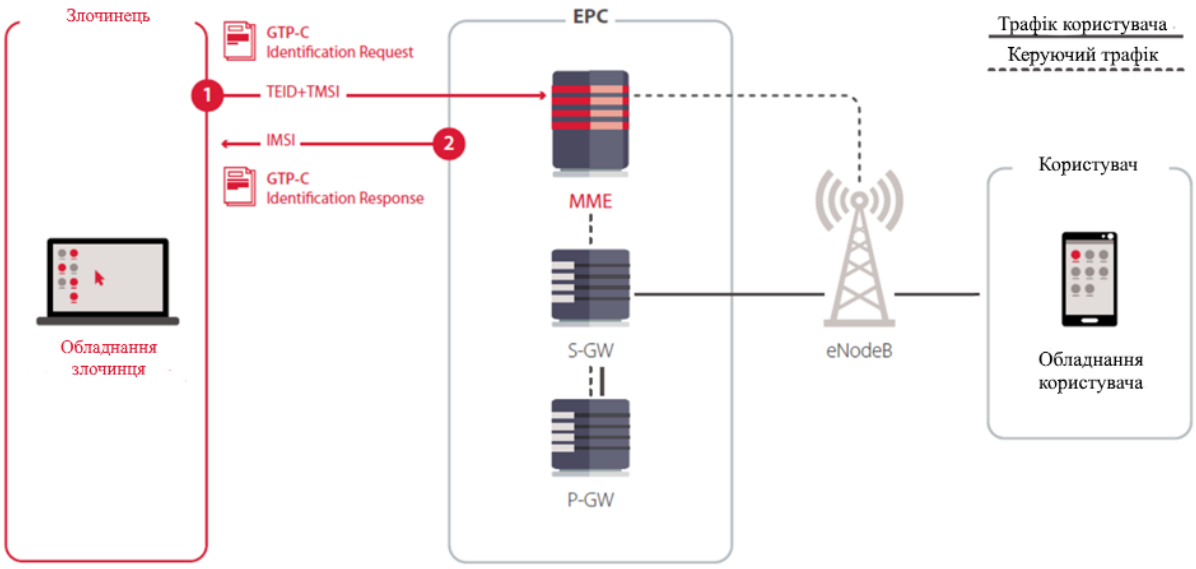

Рисунок 1.19 – Визначення IMSI абонента

На рис. 1.20, 1.21 представлено атаки на ядро EPC для того, щоб отримати повний доступ до всіх додатків гаджета користувача, на рис. 1.22 представлено можливість злому гаджета під час підключення до Інтернету.

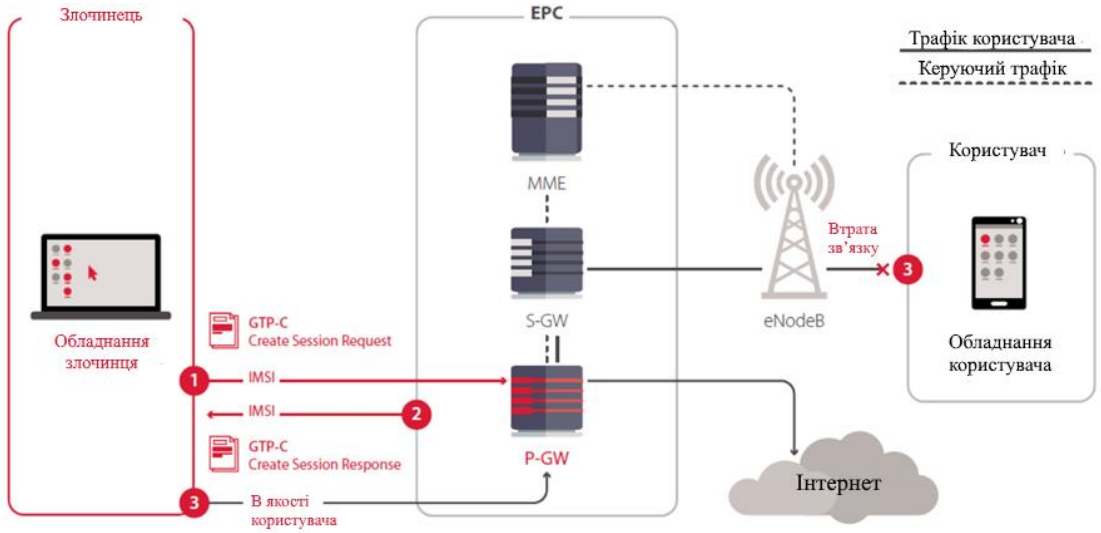

Рисунок 1.20 – Система злому за допомогою запиту GTP-C

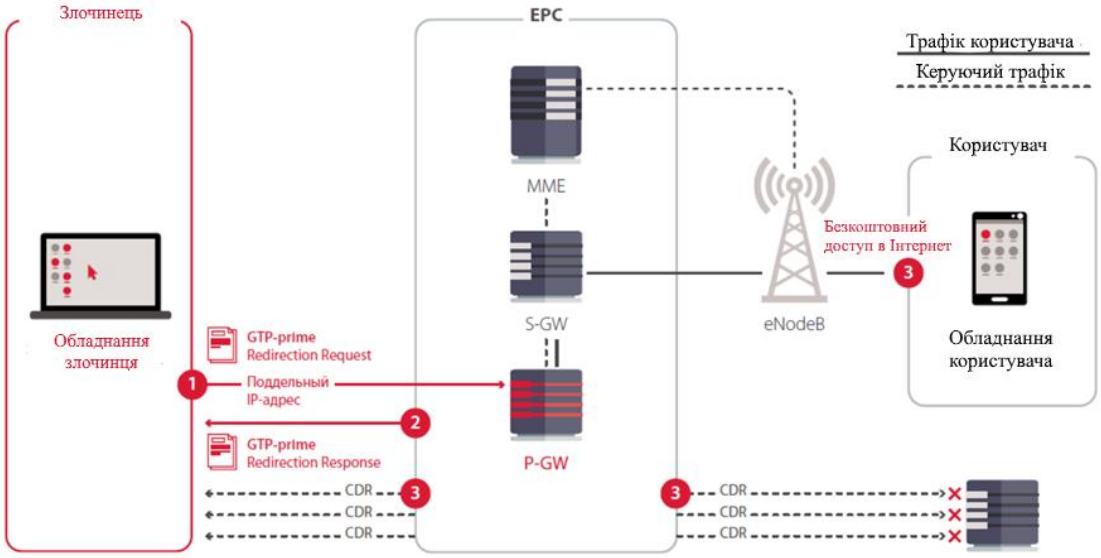

Рисунок 1.21 – Моніторинг шлюзу СГК

При цьому аналіз рис. 1.20–1.21 показує майже “нульові” витрати зловмисника з точки зору здійснення зламу.

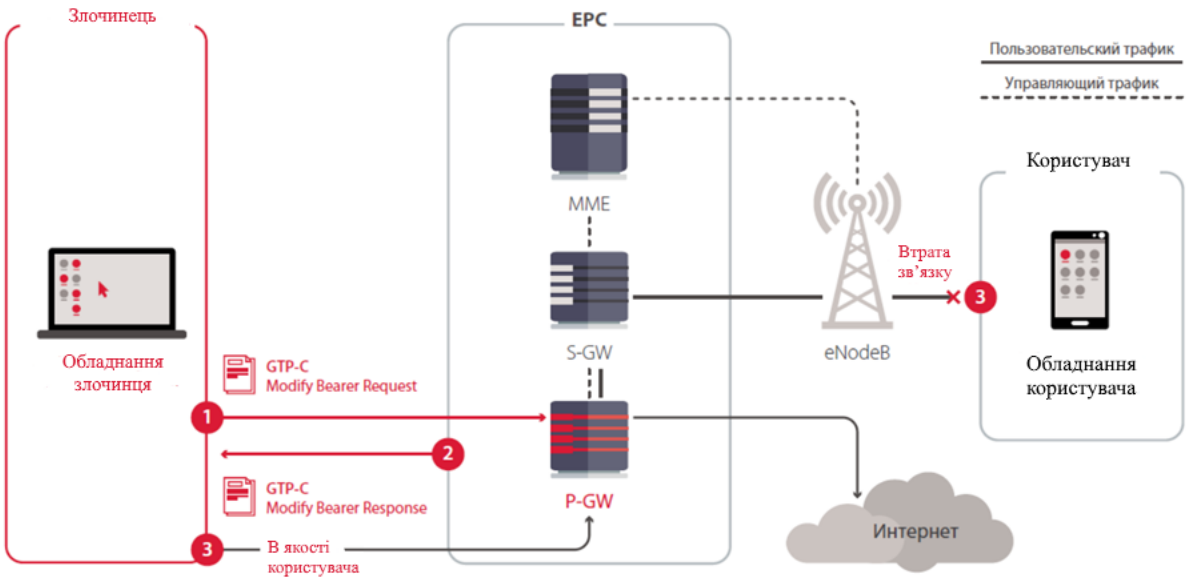

Рисунок 1.22 – Злом системи через атаку "Людина посередині"

Реалізація іншого типу DoS-атаки (DoS-атака – відмова в обслуговуванні, DDoS-атака – відмова в обслуговуванні конкретному користувачеві, EDoS-атака – відмова в обслуговуванні конкретного додатка) дозволяє перервати безперервність бізнес-процесів та/або якість послуг, що надаються користувачеві (ЙоS).

Розглянемо основні уразливості протоколу Diameter.

Протокол Dieamter, як і попередні протоколи мобільної мережі, був розроблений без вимог безпеки. тому вона має практично всі загрози, як і сама технологія “G”.

При цьому розробники в гонитві за надшвидкостями, не думають, що розвиток комп’ютерних технологій дозволяє зловмисникам (кібертерористам) “розширювати діапазон і межі” загроз, розглядати цю технологію в межах “вікна” в локальні мережі користувачів та/або корпоративні мережі.

Як показує практика, в мережах на основі протоколу Diameter можуть бути атаки, спрямовані на відмову в обслуговуванні, розкриття інформації про абонентів і мережу оператора, а також шахрайство з оператором. Крім того, зловмисник може примусово перевести пристрій абонента в режим 3G – і здійснювати подальші атаки на менш захищену систему SS7: прослухувати

голосові дзвінки, перехоплювати СМС і здійснювати шахрайські схеми проти абонентів .

Так, для мереж на основі протоколу сигналу Diameter зловмисник може здійснювати напади з метою:

Розкриття інформації про абонента;

Розкриття інформації про мережу оператора;

Перехоплення абонентського трафіку;

Шахрайства;

Відмови в обслуговуванні;

На рис. 1.23 представлено аналіз реалізації загроз на мережах 3G (SS7) та 4G (Diameter).

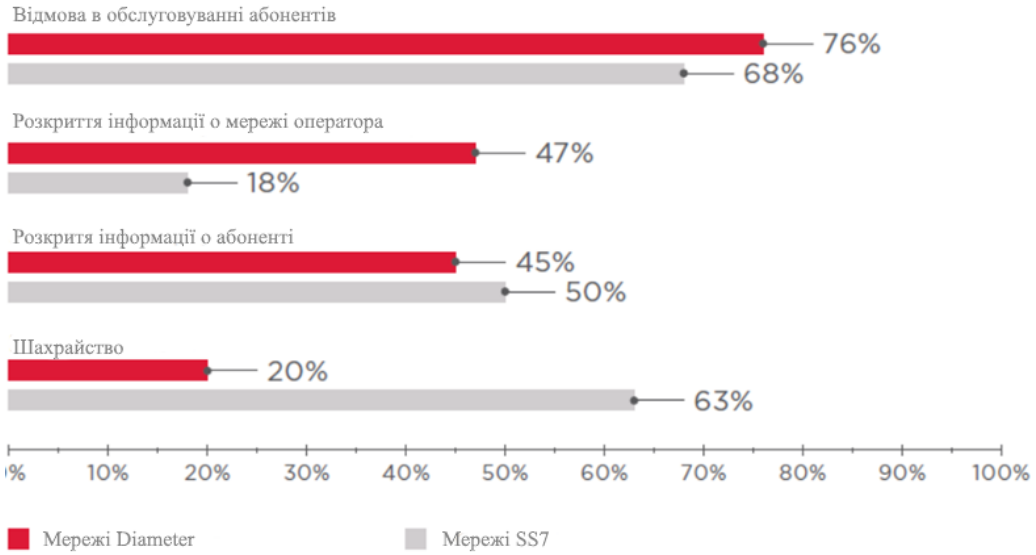

Рисунок 1.23 – Частка успішних атак за типами загроз

На рис. 1.24, 1.25 представлені результати аналізу витоку інформації про клієнта. У всіх випадках IMSI було розкрито за допомогою повідомлення Sh UDR (User-Data-Request), яке використовується сервером додатків для запиту різних абонентських даних з HSS (Home Subscriber Server), або з використанням S6a AIR (Authentication-Information-Request) – повідомлення, призначеного для отримання ключів аутентифікації абонента. Це повідомлення відправляє MME, в зоні дії которого абонент є в роумінгу. Використовуючи дані з векторів аутентифікації, зловмисник може видати свою підроблену базову станцію як легітимну та

здійснювати подальші атаки: збирати інформацію про абонентів, перехоплювати SMS і вихідні голосові дзвінки, викликати відмову в обслуговуванні абонентів.

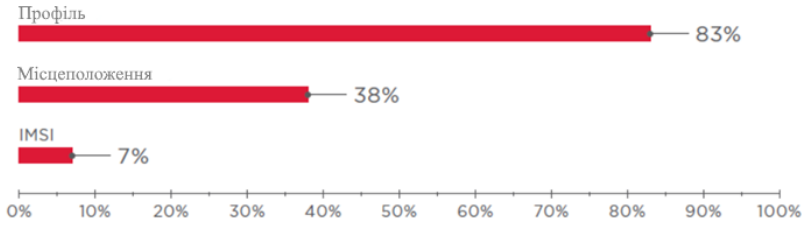

Рисунок 1.24 – Розкрита абонентська інформація (частка успішних атак)

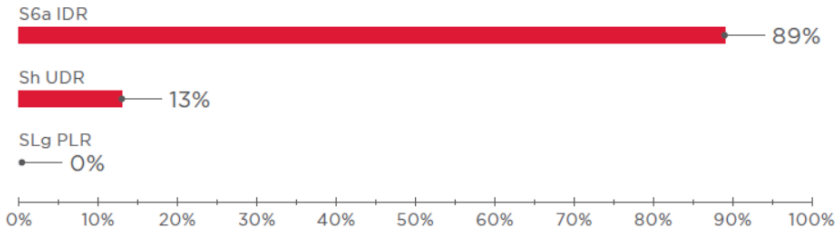

Рисунок 1.25 – Методи розкриття місцезнаходження абонента (частка успішних атак)

Таким чином, зловмисник практично повністю “контролює” місцезнаходження “жертви”, що дозволяє з урахуванням методів соціальної інженерії модифікувати загрози та практично отримувати доступ до конфіденційної інформації та/або персональних даних користувача. На рисі. 1.26 представлені результати аналізу DoS-атак в мережі на основі протоколу Diameter.

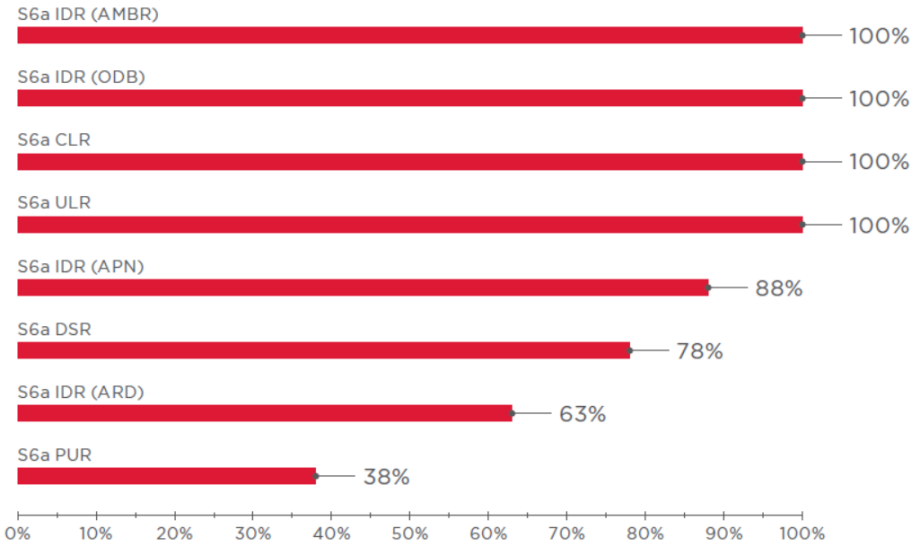

Рисунок 1.26 – Здійснення DoS-атак у мережі на основі протоколу Diameter

Аналіз рис.1.26 демонструє майже повну відсутність захисту від такого типу атаки, що дозволяє зловмиснику примушувати до погроз, отримуючи синергічний ефект від їх використання.

2 СПЕЦИФІКАЦІЯ ВИМОГ ДО МОДУЛЯ (СИСТЕМИ)

2.1 Опис предметної області, визначення цілей та можливих переваг мобільного застосунку.

Не зважаючи на те що потужність сучасних смартфонів можна порівняти з бюджетними комп'ютерами, при розробці мобільного застосунку слід враховувати особливості взаємодії користувача з пристроєм. На відміну від десктопу – смартфон має значно менший екран, некомфортну, для вводу великих обсягів інформації, клавіатури та тач-скрин замість миші як вказувача. Також, смартфон на відміну від десктопу має перевагу постійної доступності та можливості виходу в мережи з будь якої точки. Виходячи з цього, при плануванні набору функціоналу застосунку слід визначити потреби користувача що можна задовольнити надавши компонент з мінімумом необхідний дій для досягнення результату. Визначаючи технічне завдання для розробки застосунку "Мобільний кабінет викладача" я орієнтувався на доступний функціонал веб-порталу "Кабінет викладача ХНЕУ" що розроблюєтеся моєю колегою, а також опитуванням викладачів на предмет дій які їм було зручно виконувати находячись на відстані від своєї робочої станції. На основі зібраних даних було прийняте рішення сфокусуватися на такому функціоналі як:

Зчитування та редагування особистої інформації викладачів – у рамках своєї професійної діяльності, викладачу може знадобитися інформація про свого колегу. Також викладачу може стати у потреби оновити якісь з своїх даних наприклад номер мобільного телефону;

Доступ до публікацій викладачів – якщо в викладача є необхідність ознайомитись з публікацією іншого викладача, він зможе зробити через мобільне застосування, що дозволяє роботи це наприклад у метро або іншому транспорті, у кафе чи парку під час перерви, тощо;

Доступ до розкладу та його редагування. Як студентам так і викладачам час від часу потрібно уточнити розклад. Враховуючи малий об'єм інформації і можливості зручного форматування цієї інформації, найзручнішим способом отримання цієї інформації буде смартфон;

Ведення журналу присутності та успішності студентів. Цей функціонал насамперед було запропоновано одним з викладачів під час опитування та піддержано іншими викладачами. Можливість швидко, однією рукою, ввести данні присутності студентів та їх оцінки прямо на занятті – має все перспективи стати одним з найбільш затребуваних функціоналів;

Також при розробці мобільного застосунку слід провести аналіз бази потенціальних користувачів, операційну систему що вони використовують та її максимальну доступну версію. В наш час існує 2 мобільних операційних системи це iOS та Android, маючи дані щодо відносного розподілу систем серед викладачів – можна зробити висновки щодо доцільності використовування кросс-платформених рішень, або фокусі на той чи іншій системі. Виходячи з даних опитування більшість викладачів ХНЕУ користується смартфонами на базі Android, тому було прийнято рішення сфокусуватись на цієї платформі. Визначивши потрібну систему, особливо коли ця система є системою Android, потрібно встановити мінімальну версію ОС що буде підтримуватись. Така необхідність пояснюється політикою виробників смартфонів, що не випускають нові версії ОС для смартфонів що вони більше не випускають у продаж. З іншого боку у інтересах кожного користувача користуватися застосунком орієнтованим на найбільш сучасну версію, тому що стари версії мають гірші можливості та менш захищені від відомих вразливостей. Виходячи з цього необхідно знайти баланс між доступністю версії та її сучасністю. Компанія Google надає розробникам статистику (рис. 2.1) відносного поширення різних версій ОС.

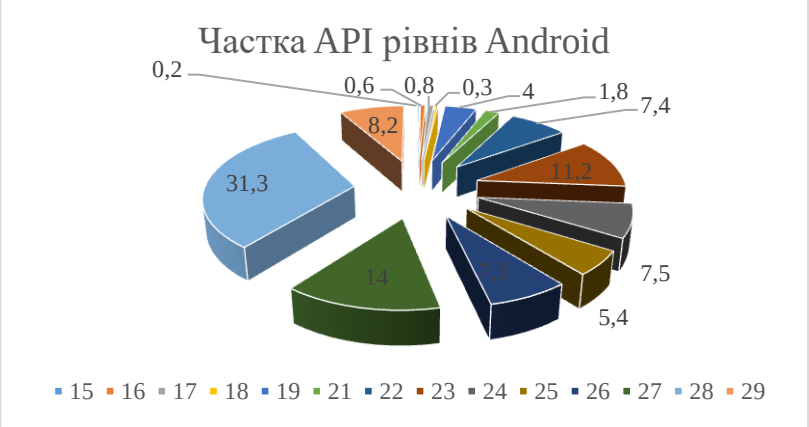

Рисунок – 2.1 Розподіл версій ОС Android

У цьому чарті напроти кожної версії вказаний процент користувачів що зможуть користуватися застосункам при обрані цієї версії як мінімальної. Виходячи з цих даних було прийняте рішення базуватись на версії 5.0 що є значно більш захищеною ніж 4.x версії, надає можливість використовувати усі сучасні інструменти дизайну, та підтримується 94.1% пристроїв.

Словник основних використовуваних термінів, у вигляді глосарію [14], наведений в таблиці 2.1.

Таблиця 2.1 – Глосарій

Термін	Опис терміну
1. Основні поняття та категорії предметної області та проекту	
Планувальник	Система, що розроблена як особистий кабінет викладачів університету
Кафедра	Підрозділ вищого навчального закладу, що проводить навчально – виховну, методичну і наукову діяльність
Індивідуальний план	Основний документ викладача, на підставі якого оцінюється його робота, подається щомісячний рапорт у бухгалтерію про нарахування зарплати, ведеться перевірка КРУ
Google Scholar	Вільна доступна пошукова система, яка індексує повний текст наукових публікацій всіх форматів і дисциплін
Open Researcher and Contributor ID (ORCID)	Некомерційний проект, мета якого створення єдиного, міжнародного реєстру вчених ORCID
Конкурсні роботи студентів	Науково – дослідна робота
Scopus	ID Elsevier бібліографічна і реферативна база даних та інструмент для відстеження цитованої статі, опублікованих в наукових виданнях
Активність	Екземпляр класу що успадковує клас android.app.Activity. Э основним елементом любого застосунку на базі андроїд та кореневим елементом кожного екрану.
Фрагмент	Екземпляр класу що успадковує клас androidx.fragment.app.Fragment. Є додатковим елементом структури застосунку. Являє собою екран що може бути додано у Активність.
Сервіс	Клас що реалізує роботу с даними. У цих класах проходить отримання, відправлення та локальне збереження цих даних.
Об’єкт репозиторію	Об’єкт що надає доступ UI компонентам до моделі даних. Отримує інформацію через сервіси доступу до БД або через мережеві сервіси

Закінчення табл. 2.1

Термін	Опис терміну
2. Користувачі системи	
Керівник навчального відділу	Користувач, котрий має повний доступ до всіх функцій сайту
Викладач	Користувач, котрий має доступ майже до всіх функцій застосування, крім адміністративних
3. Вхідні та вихідні документи	
Розклад	Вхідний документ. Документ що вказує розклад занять та їх розташування.
Відомості про викладачів	Вхідний документ. Інформація про дані викладачів
Список кафедр	Вхідний документ. Список кафедр університету
Список груп по спеціальностях	Вхідний документ. Список груп університету
Список факультетів	Вхідний документ. Список факультетів університету
Список дисциплін	Вхідний документ. Список дисциплін університету
Публікації	Вихідний документ. Оформленні та завантажені до системи публікації викладачів
Розподілене навантаження	Вихідний документ. Сформоване та розподілене навантаження викладача

2.2 Розроблення варіантів використання

2.2.1. Діаграма варіантів використання.

Діаграма варіантів використання, виконана за допомогою онлайн CASE інструмента. Діаграма варіантів використання відображає функціональність, яка буде реалізована в програмному продукті. Основними акторами у даній предметній області є керівник начального відділу та викладач. Перелік функцій кожного можна побачити на рис. 2.2.

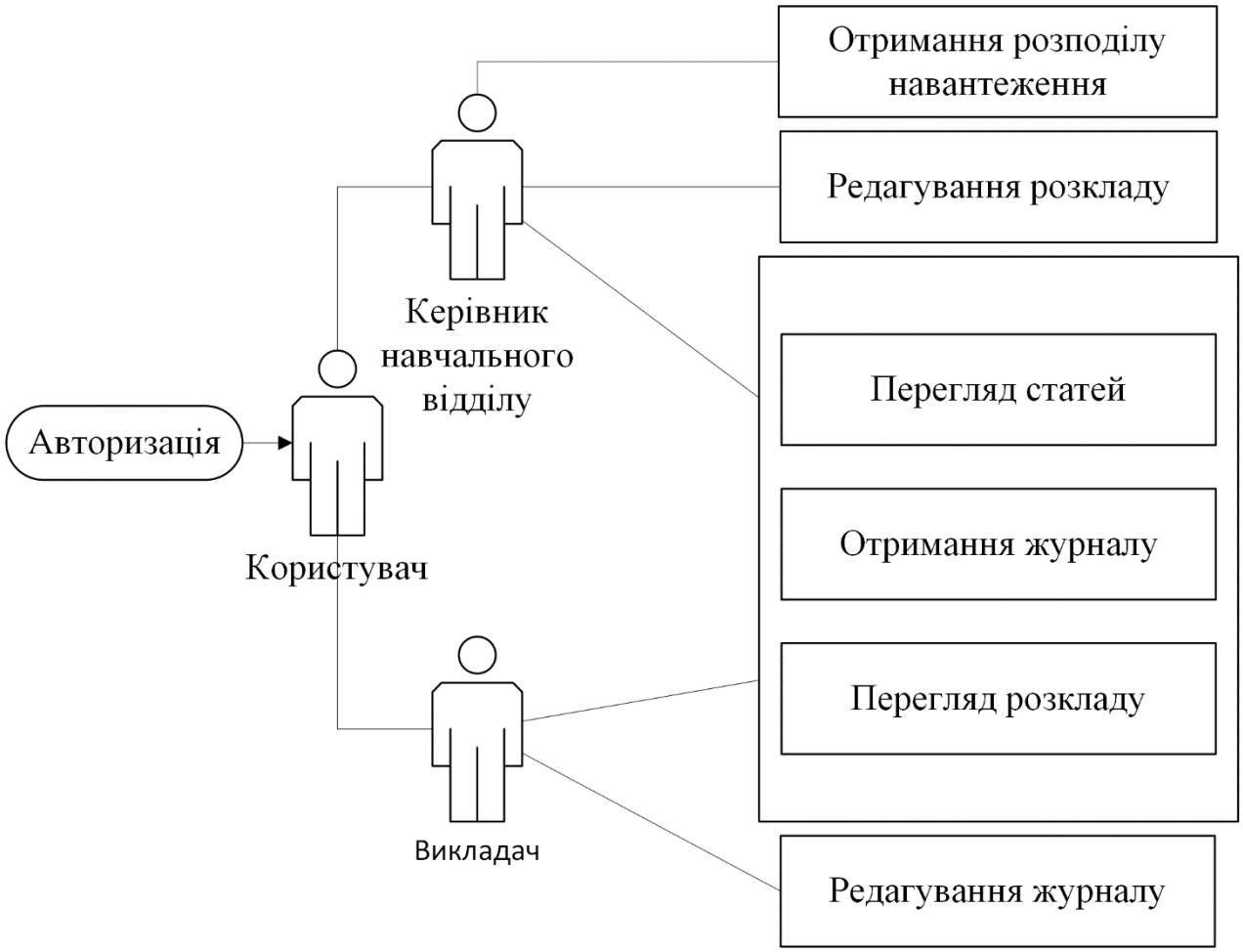

Рисунок 2.2 – Діаграма варіантів використання

2.2.2. Специфікація варіантів використання.

У даному пункті описуються варіанти використання [14] зображені на рис. 2.2. У табл. 2.2 – 2.4 описані основні варіанти використання.

Нижче представлені варіанти використання : виконання поточних завдань та робіт, виконання та складання тестів, виконання лабораторних робіт, використання програм для виконання робіт, формування та підготовка завдань. Ці варіанти використання забезпечують основну функціональність розроблюваного додатку.

Таблиця 2.2 – Варіант використання “Авторизація у систему веб-сервісу”

Характеристика	Значення
1	2
Контекст використання	Авторизація в системі
Дійові особи	Керівник навчального відділу, начальник навчально-дослідницького сектору, викладач
Передумова	Користувач зареєстрований в системі
Тригер	Вхід на веб-сервіс
Сценарій	1 – Введення логіну; 2 – Введення паролю; 3 – Натискання кнопки “Вхід”.
Посту умова	У випадку успішного завершення, відкривається веб-сервіс та користувач отримує доступ до його функціоналу, в іншому випадку отримує повідомлення про некоректний логін чи пароль і програма завершує свою роботу.

Таблиця 2.3 – Варіант використання “Заповнення журналу”

Характеристика	Значення
Контекст використання	Заповнення журналу даними о присутності та успішності студентів
Дійові особи	Викладач
Передумова	Користувач увійшов в систему
Тригер	Початок заняття за розкладом
Сценарій	1. Сортування студентів за наявністю 2. Заповнення оцінок студентів 3. Натискання кнопки зберегти для синхронізації з сервером
Пост умова	У випадку успішного завершення, інформація збережена в ІС; у випадку помилки стан системи залишається незмінним, програма відображає повідомлення, яке містить причину помилки

2.3 Специфікація функціональних та нефункціональних вимог

Специфікація функціональних вимог до програмного забезпечення [14] є опис поведінки продукту, який необхідно розробити. Тобто функціональні вимоги пояснюють, що повинно бути зроблено. Специфікація функціональних вимог наведена в табл. 2.4. До таблиці специфікації, по-перше входить пріоритет, тому що, завдяки пріоритету можемо зрозуміти важливість тої чи іншої вимоги. По-друге, до атрибуту вимог входить складність. Вона показує рівень трудовитрат кожної вимоги. По-третє, також відноситься контакт/виконавець, це поле визначає людину, яка відповідальна за певну вимогу.

Таблиця 2.4 – Специфікація функціональних вимог

Ідентифікатор вимоги	Назва вимоги (варіанту використання)	Атрибут вимог		
		Пріоритет	Трудність	Контакт/ Виконавець
UC – 1	Авторизація	Обов’язковий	Середня	Керівник навчального відділу / Викладач
UC – 2	Перегляд публікацій	Рекомендовано	Низька	Керівник навчального відділу / Викладач
UC – 3	Перегляд розкладу занять	Рекомендовано	Низька	Керівник навчального відділу / Викладач
UC – 4	Редагування розкладу занять	Рекомендовано	Середня	Керівник навчального відділу
UC – 5	Заповнення журналу	Обов’язкова	Висока	Викладач
UC – 6	Перегляд журналу	Рекомендовано	Середня	Керівник навчального відділу / Викладач
UC – 7	Редагування даних користувачів	Обов’язкова	Середня	Керівник навчального відділу / Викладач
UC – 8	Перегляд плану наукової роботи кафедри	Рекомендована	Середня	Керівник навчального відділу

Специфікація нефункціональних вимоги описує характеристику системи і її оточення, а не поведінку системи. Не функціональні вимоги визначають

системні властивості такі як продуктивність, зручність супроводу, розширюваність, надійність. Тут також може бути наведено перелік обмежень, що накладаються на дії і функції, виконувані системою. Вони включають тимчасові обмеження, обмеження на процес розробки системи, стандарти і т.д. Специфікацію нефункціональних вимог зображена у табл. 2.5.

Таблиця 2.5 – Специфікація нефункціональних вимог

Ідентифікатор вимоги	Назва вимоги	Атрибут вимог		
		Пріоритет	Трудність (показник та характеристика)	Контакт
1. Застосовність				
SUPP – 01	Час завантаження системи веб-сервісу – не більше 5 с	Обов’язкове	Середня	Бофанов А.В
SUPP – 02	Швидкість роботи мереже інтернет з’єднання – 100Mbit/s.	Рекомендовано	Низька	Бофанов А.В
SUPP – 03	Зручний та функціональний інтерфейс користувача застосунку.	Обов’язкове	Середня	Бофанов А.В
SUPP – 04	Легкість в користуванні та зручне обслуговування системи.	Обов’язкове	Висока	Бофанов А.В
SUPP – 05	Відгук серверу не більше 15 сек.	Рекомендовано	Середня	Бофанов А.В
Надійність				
SUPP – 06	Не велика кількість збоїв у роботі системи.	Обов’язкове	Висока	Бофанов А.В
SUPP – 07	Стійкість до збоїв, можливість продовжувати роботу з системою у випадку збою.	Рекомендовано	Висока	Бофанов А.В
3. Робочі характеристики				
SUPP – 08	Можливість зручно направити дані у інші застосунки	Рекомендовано	Низька	Бофанов А.В
SUPP – 09	Коректний вхід та вихід в режим сну.	Обов’язкове	Висока	Бофанов А.В

Закінчення табл. 2.5

Ідентифікатор вимоги	Назва вимоги	Атрибут вимог		
		Пріоритет	Трудність (показник та характеристика)	Контакт
3. Експлуатаційна придатність				
SUPP – 10	Дотримання стандартів MVVM при проектуванні системи	Рекомендовано	Середня	Бофанов А.В
5. Проектні обмеження				
SUPP – 11	Технологія Android SDK, мова Java та Kotlin	Обов'язкове	Середня	Бофанов А.В
6. Інтерфейс				
6.1 Інтерфейс користувача				
SUPP – 12	Єдине оформлення усіх сторінок системи	Обов'язкове	Середня	Бофанов А.В
6.2 Апаратні інтерфейси				
SUPP – 13	512 Мбайт ОЗУ та вище	Обов'язкове	Низька	Бофанов А.В
SUPP – 14	256 Мбайт вільного дискового простору	Обов'язкове	Низька	Бофанов А.В
SUPP – 15	Процесор 800МГц та вище	Обов'язкове	Низька	Бофанов А.В
7. Програмні інтерфейси				
SUPP – 16	Наявність офіціальної версії Android з установленими GAPPS	Обов'язкове	Середня	Бофанов А.В
8. Вимоги до ліцензування				
SUPP – 17	Наявність підключення до Internet	Обов'язкове	Середня	Бофанов А.В
9. Вимоги до ліцензування				
SUPP – 18	Використання одної ліцензії на одне робоче місце	Обов'язкове	Середня	Бофанов А.В
10. Застереження щодо питань, пов'язаних з авторськими правами				
SUPP – 19	Авторські права захищені законом	Обов'язкове	Середня	Бофанов А.В

2.4 Проектування інтерфейсу користувача.

Розробка інтерфейсу користувача, це одна з найголовніших вимог до створення нового та актуального застосунку, аби майбутні користувачі не мали складнощів у пошуку необхідної інформації або використанням функцій цього

застосунку. Виходить, що програмний інтерфейс не тільки вирішує нашу проблему взаємодії з додатком, а й робить цю взаємодію максимально комфортною. Важлива наявність інтерфейсу, що дозволяє при меншій кількості зусиль ознайомитися з можливостями програми і зрозуміти основні принципи роботи в ньому.

Для розробки макету інтерфейса було використано веб-сервіс Figma. Для того щоб розробити застосунок, потрібно з самого початку розуміти як він буде виглядати. Саме для цього було розроблено макети, які будуть відображати інтерфейс та працездатність функціоналу. Спочатку розглянем майбутній інтерфейс для сторінки авторизації.

Рисунок 2.3 – Макет сторінки авторизації

На рис. 2.3 наведено макет сторінки авторизації, при заході на екран, користувач побачить лого розташоване по центру, коли усі необхідні систему буде ініційовано, лого від’їде вверх з анімацією а під ним з’явиться блок авторизації. З полями логіну та паролю, кнопкою “вхід” що ініціює вхід до системи та “забули пароль” що відображає інформацію о необхідних діях при втраті паролю.

Після входу, користувачу відкривається головна сторінка застосунку що є стандартною моделлю навігації з навігаційним меню. Більшість екранів виступають як фрагменти розміщені на головному робочому просторі екрану.

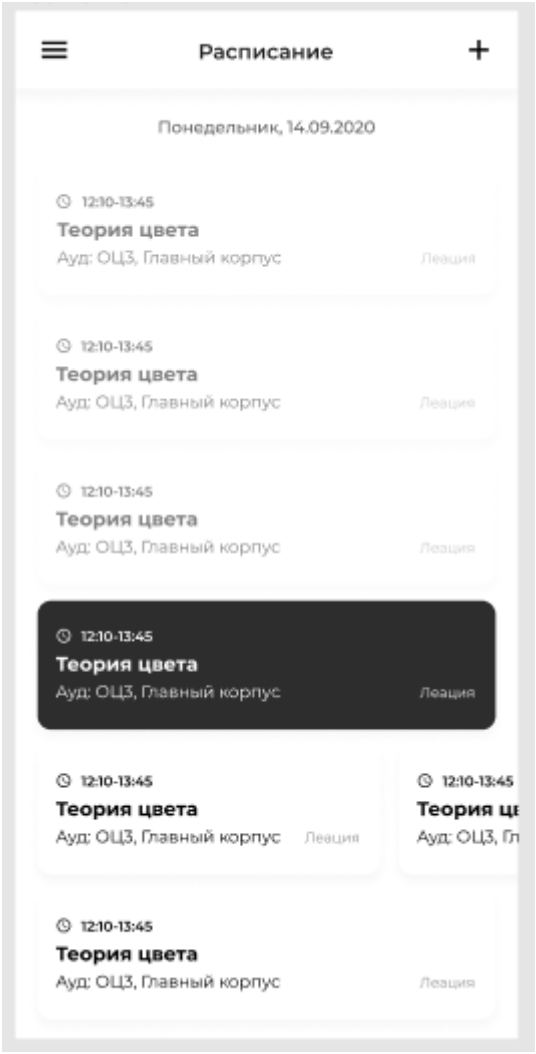

Рисунок 2.4 – Макет екрану розкладу

На рис. 2.4 наведено макет екрану розкладу. Кнопка меню (тут і далі) зліва зверху відкриває навігаційне меню. Кнопка додати справа вверху, відкриває екран додавання розкладу. Зверху під назвою сторінки, розміщене текстове поле дати, що відображає поточну обрану дату (за умовчанням, сьогоднішня дата). Дата може бути змінена горизонтальним свайпом що змінює день на одиницю, або ж натисканням на поле дати що відкриє стандартний календар Android для вибору дати. Одиниця розкладу може бути у трьох станах.

Стандартний стан – чорний текст на білому фоні, відображає майбутні одиниці розкладу.

Поточний стан – білий текст на чорному фоні, відображає заняття що проходить зараз.

Минулий стан – світло чорний текст на білому фоні, відображає заняття що минули.

На одній строчці може бути більш ніж одна одиниця розкладу, у такому випадку одиниці розміщуються горизонтально.

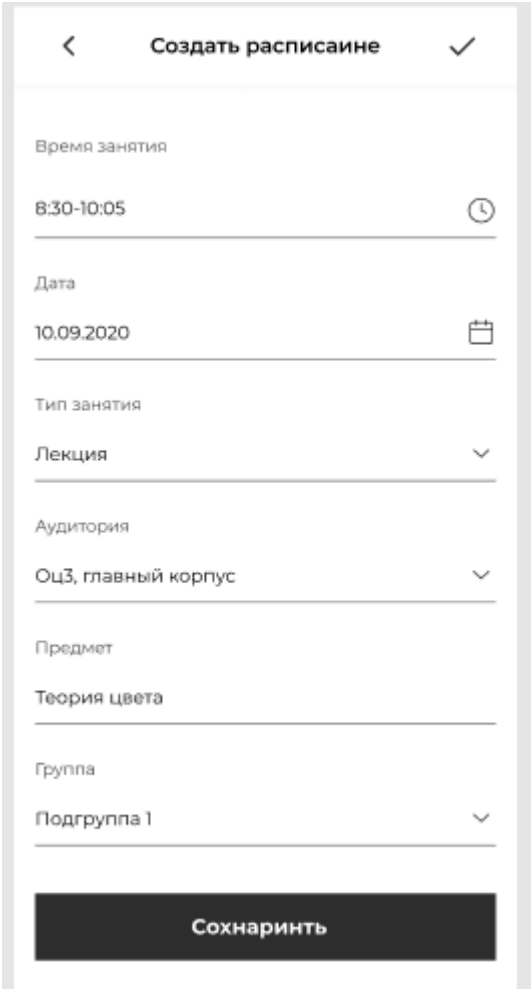

Рисунок 2.5 – Макет сторінки створення одиниці розкладу

На рис. 2.5 наведено макет створення одиниці розкладу. Кнопка меню тут замінена на кнопку “назад” що повертає на основний навігаційний екран. Зверху

справа розташована кнопка “ОК” що зберігає введені дані, також цю кнопку продубльовано знизу. Дані вводяться чотирма способами:

Ввід дати – як і на екрані розкладу використовується системний календар;

Ввід з обранням зі списку – користувач обирає один з наявних елементів списку що розташовані в випадному списку. Елементи випадного списку отримуються з серверу на етапі ініціалізації;

Ввід за авто заповнюванням – користувач починає ввід, на основі введених символів йому пропонуються варіанти зі списку отриманого з серверу;

Екран вводу інформації журналу має два етапи. Насамперед, викладач, вводить дані присутності студентів рис. 2.6. Викладач може робити це свайпом вліво чи вправо, де свайп вправо помічає студента як присутнього а свайп вліво як відсутнього. Опрацьовані студенти переміщуються на кінець списку, в підгрупи “Присутні” та “Відсутні”, де їх також можна свайпнути щоб змінити їх статус. Підгрупи відрізняються заголовком та кольором одиниць списку.

Коли усі студенти були опрацьовані, екран переходить в режим оцінювання рис. 2.7 де студенти також розподілені на підгрупи присутніх і відсутніх але заголовки видаляються залишаючи лише кольорову індикацію.

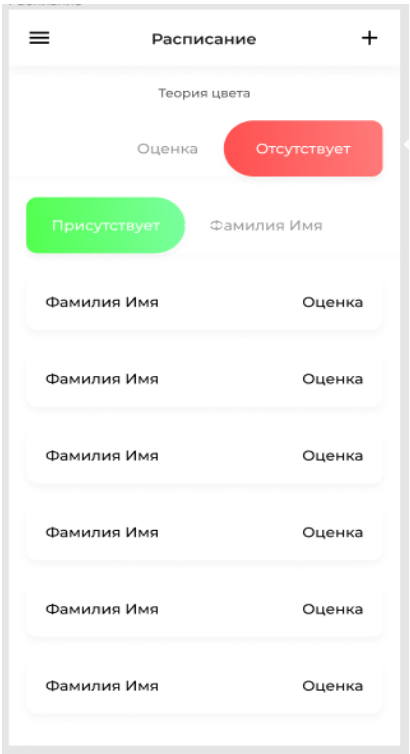

Рисунок 2.6 – Макет екрану присутності студентів

Кожну одиницю можна свайпнути для зміни статусу студента. При натисканні на студента з’являєтеся цифрова системна клавіатура що дозволяє ввести оцінку.

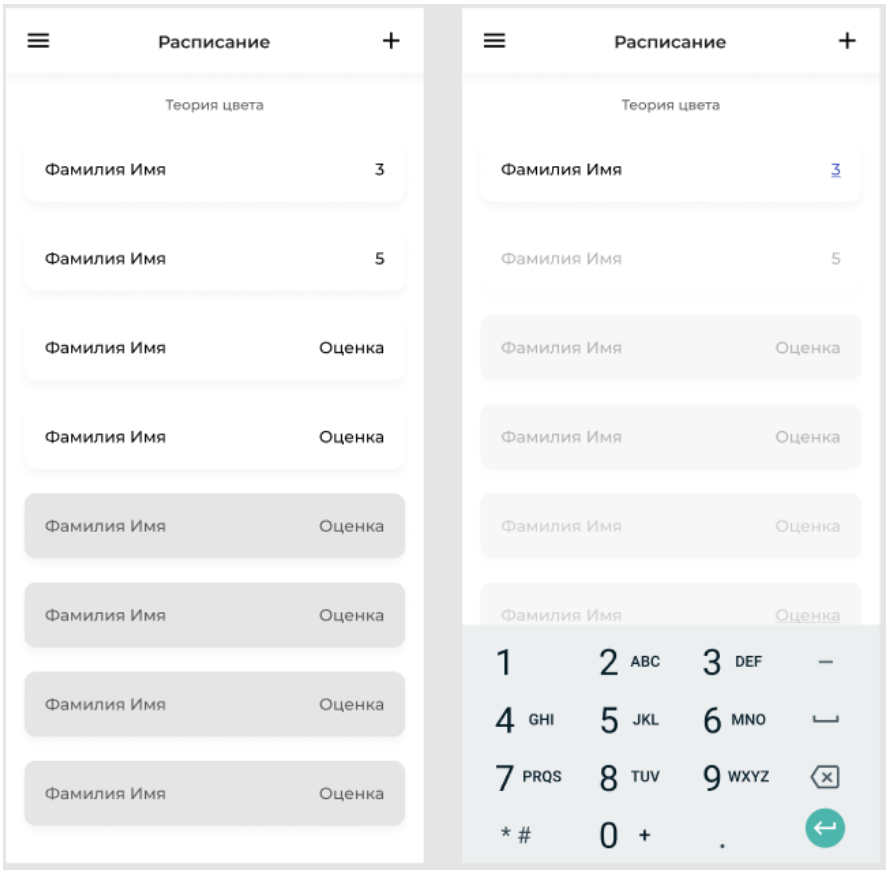

Рисунок 2.7 – Макет екрану оцінювання студентів

2.5 Навігаційна структура проекту.

Вхідною точкою проекту є активність InitialPageActivity. На цьому екрані проходить ініціалізація необхідних компонентів та надається можливість логіну. Після успішного логіну завжди відкривається MainActivity що містить усі основні екрани у вигляді фрагментів. Навігація у цій активності проходить за допомогою реалізації класу com.google.android.material.navigation.NavigationView що створює меню що виїжджає справа та перекриває собою основний екран з контентом. Основний екран являє собою відображення заголовку та контейнер для фрагментів контенту. Клік на елементи меню змінює поточний фрагмент відображений у головному контейнеру. У випадках коли потрібно зібрати

великий об’єм даних, вони збираються у окремій активності. Візуальна структура застосунку представлена рис. 2.8.

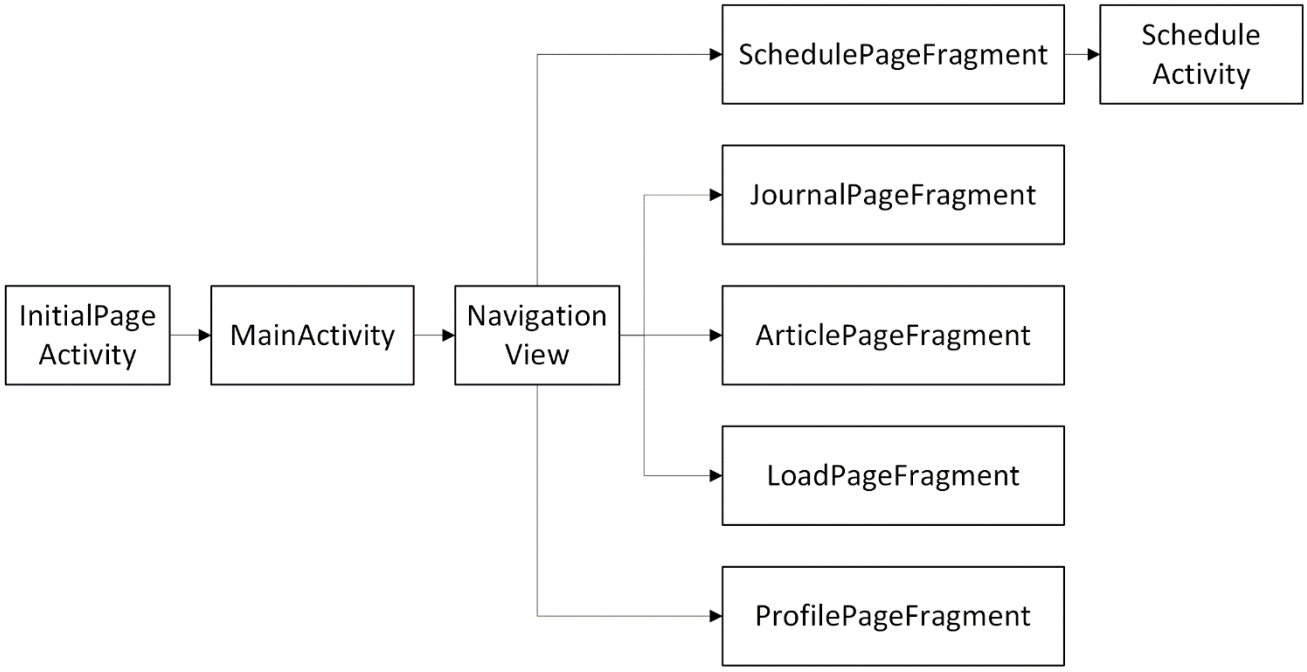

Рисунок 2.8 – Навігаційна структура проекту

2.6 Архітектура проекту.

Архітектура проекту збудована на основі поточного рекомендованого шаблону MVVM (Model–View–ViewModel), що надає змогу збудувати чисту структуру де усі компоненти розділені за призначенням. Це є можливим завдяки розподілу відповідальності що надає цей шаблон:

Розробка користувацького інтерфейсу здійснюється за допомогою технології XML;

Логіка користувацького інтерфейсу реалізується як компонент ViewModel;

Функціональні зв’язки між користувацьким інтерфейсом та ViewModel реалізуються через біндинги (bindings), які, по суті, є правилами типу “якщо кнопка А була натиснута, повинен бути викликаний метод onButtonAClick() з ViewModel”. Біндинги можуть бути написані в коді або визначені декларативним шляхом (Android використовує обидва типи);

Дані, з яких формується ViewModel отримуються з об’єкту репозиторію, який, в свою чергу виходячи з внутрішньої логіки та стану системи (стан життєвого циклу застосунку, наявність підключення до мережі тощо) отримує чи зберігає дані з бази даних або серверу. Но основі принципів шаблону та особливостях системи було створено таку архітектуру:

View – об’єкти, що успадковують клас View, відповідають за відображення інформації.

Activity – базовий компонент, виступає в ролі контролеру якщо не має внутрішніх фрагментів. Fragment – контролер, відповідає за поєднання View та слою даних. ViewModel – відповідає за формування даних для відображення у View, збирає дані що вводить користувач. Repository – об’єкт, що поєднує контролер та ViewModel з даними, використовуючи LocalService або ApiService, LocalService – об’єкт зв’язку з БД, ApiService – об’єкт зв’язку з сервером.

Структура та взаємодія цих елементів показана на рис. 2.9

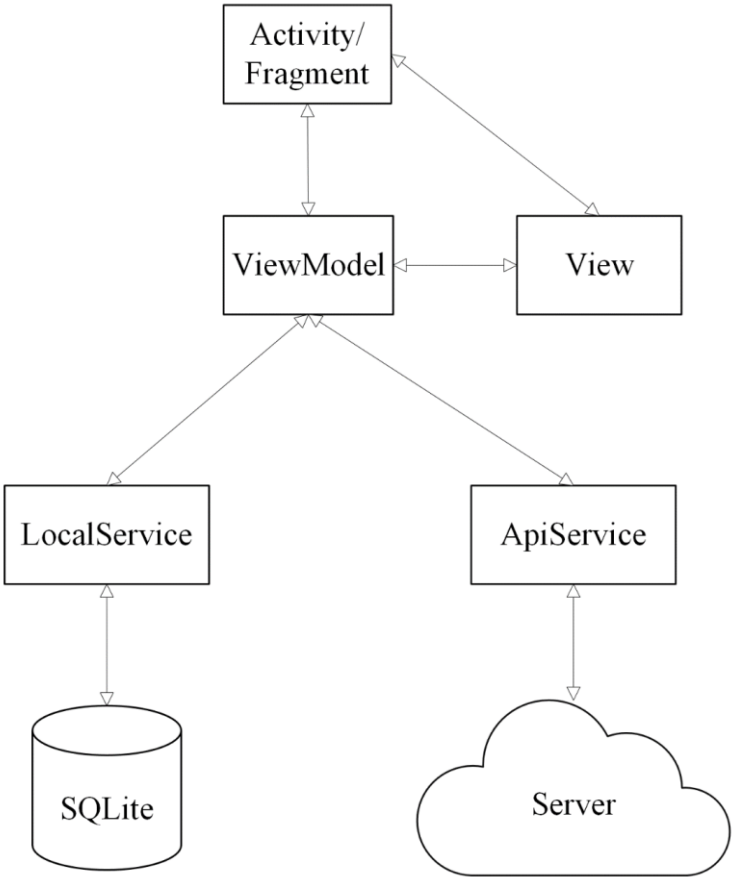

Рисунок 2.9 – Архітектура проекту

Розташування елементів архітектури можна зробити використовуючи одну з двох концепцій, типової або функціональної. Кожна з концепцій має свої переваги та недоліки, тому є доцільним розглянути обидві концепції.

Типова структура проекту представлена на рис. 2.10 пропонує розміщувати класи по їх архітектурному типу, тобто створювати пакти з класами типу Repository, ApiService, ViewModel тощо.

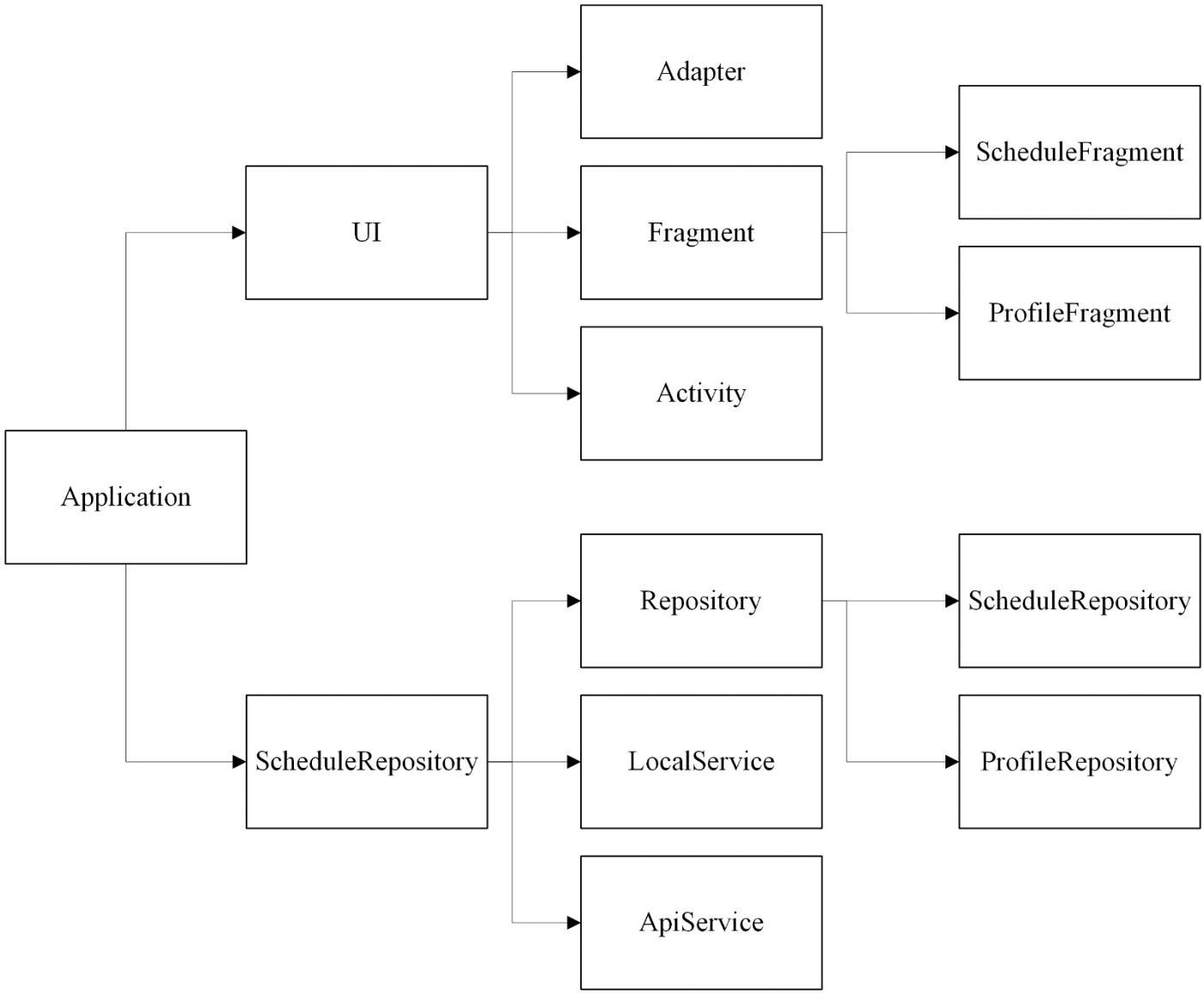

Рисунок 2.10 – Типова структура проекту

Такий підхід має декілька переваг:

Спрощує навігацію по класах за умови їх невеликої кількості;

Надає можливість реалізувати protected методи, для більш чіткого розподілу області видимості;

Є інтуїтивно зрозумілим та не потребує від нового розробника усієї ширини знань о функціоналі та архітектури проекту;

Але, для великих проектів така концепція має 2 суттєвих недоліки:

При великої кількості функціоналу навігація є дуже ускладненою, це може підштовхнути розробника к об’єднанню декількох елементів функціоналу у один клас. Наприклад, об’єднати елементи розкладу, звітності та публікації в один сервіс що може бути названий як “TeacherApiService”. На перший погляд це спрощує як навігацію так і загальну комплексність коду завдяки зменшенню загальної кількості класів та строк, але це також порушує важливий принцип Single Responsibility, що згодом, при підтримки чи розвиненні проекту може створити хаос серед функціоналу.

Коли розробник матиме проблему ускладнення та порушення принципу єдиної відповідальності, він прийде к єдиному можливому рішенню – рефактору коду у функціональну концепцію, але якщо розробник користувався перевагою реалізації області видимості – йому прийдеться витрати велику кількість часу на перерозподіл видимості методів, змінних, та внутрішніх класів. Це викликано тим що protected метод що розповсюджений у типовий концепції – має область видимості на рівні пакету, і не може бути викликаний з іншого пакету.

Виходячи з цього таку концепцію можна використати лише для малих проектів без прогнозованого зростання кількості елементів функціоналу.

Функціональна концепція структурує елементи архітектури за їх приналежністю до елементу функціоналу. Тобто один пакет являє собою репрезентацію частки функціоналу і містить всі кінцеві екземпляри елементів архітектури необхідні для реалізації функціоналу. Для реалізації загального функціоналу такого як ініціалізація бази даних, використовують базові абстрактні класі у базовому пакеті. Приклад такої структури наведено на рис. 2.11.

Концепція є складнішою для зрозуміння новим розробником, але при гідно зробленої документації цей недолік можна виправити. Також недоліком є неможливість в повну міру використовувати всі можливості областей видимості, через це потрібно вводити абстрактні класи що можуть забезпечити базовий

функціонал водночас ховаючи методи базової логіки від успадкованих класів. Таким чином логіку що повторюється в усіх реалізаціях типового елементу архітектури можна винести до базового класу використовуючи Generic class, що являє собою додатковий аргумент типу що може бути вказаний при ініціалізації об’єкту та використаний для внутрішньої типізації.

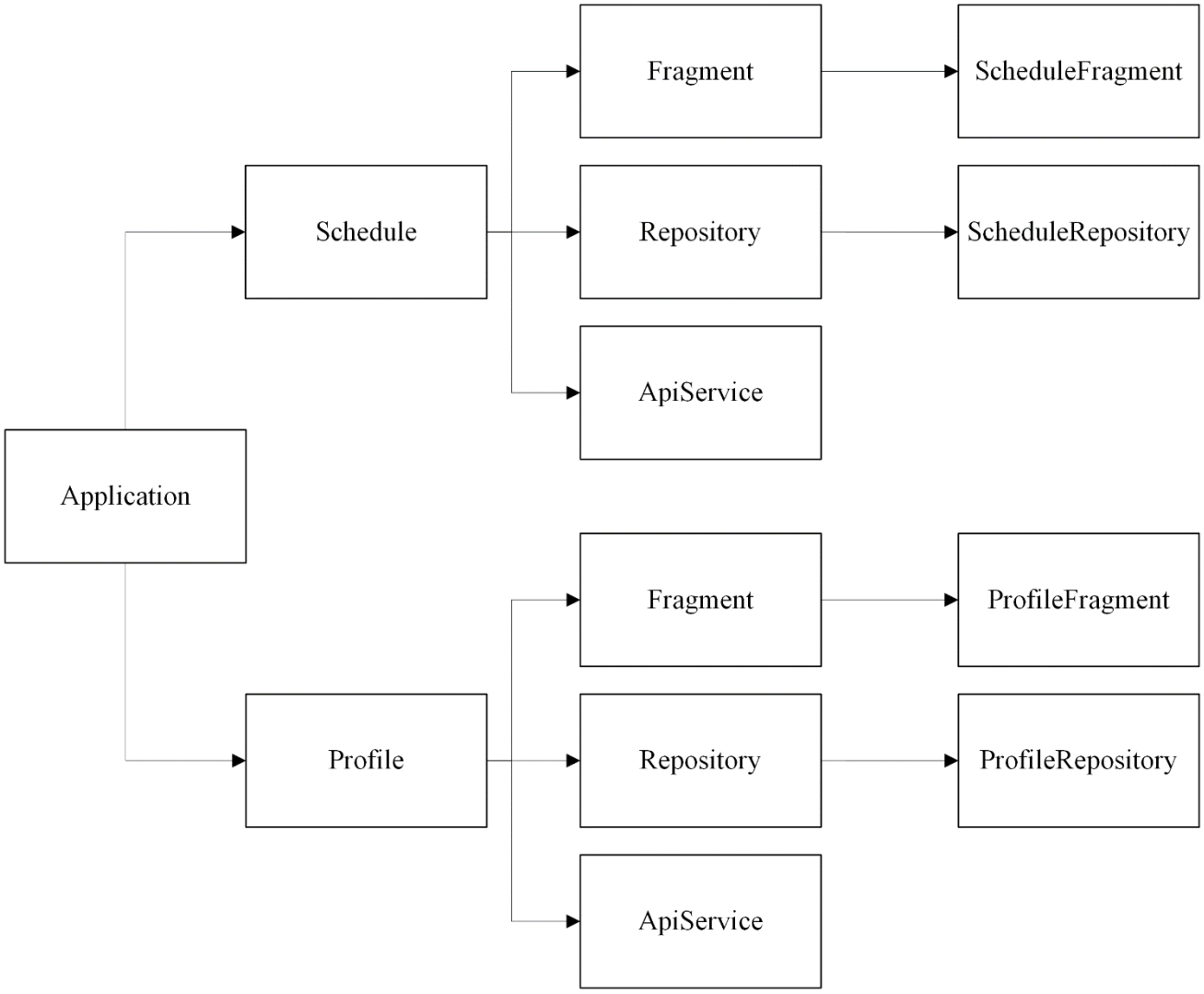

Рисунок 2.11 – Функціональна концепція

На основі цих даних мною було прийняте рішення використати функціональну концепцію структури, не зважаючи на малий розмір проекту. Такий вибір дозволить студентам та науковим співробітникам вдосконалювати застосунок, без потреби постійного рефактору, що буде сприяти розвитку системи інноваційно-активного університету, і мотивувати студентів вдосконалювати її.

3 РОЗРОБКА СИСТЕМИ ЗАХИСТУ

3.1 Опис можливих загроз мобільної платформи, визначення моделі загроз

Результатом дипломної роботи, буде додання до існуючої системи нового за типом елементу – застосунку на базі ОС Android. Новий тип елементу, якщо його не було розроблено з урахуванням загроз властивих цій платформі, може стати слабкою частиною усій системи та скомпрометувати її. Тому суттєвою задачею розробки мобільного застосунку є аналіз можливих загроз застосунків та захист від можливих кібератак. За умови якісної розробки самого застосунку, що робить маловірогідним втрату доступу до інформації через внутрішні помилки, інші загрози доступності, достовірності та кондиційності інформації можна поділити за їх походженням на внутрішні та зовнішні що представлено на рис. 3.1.

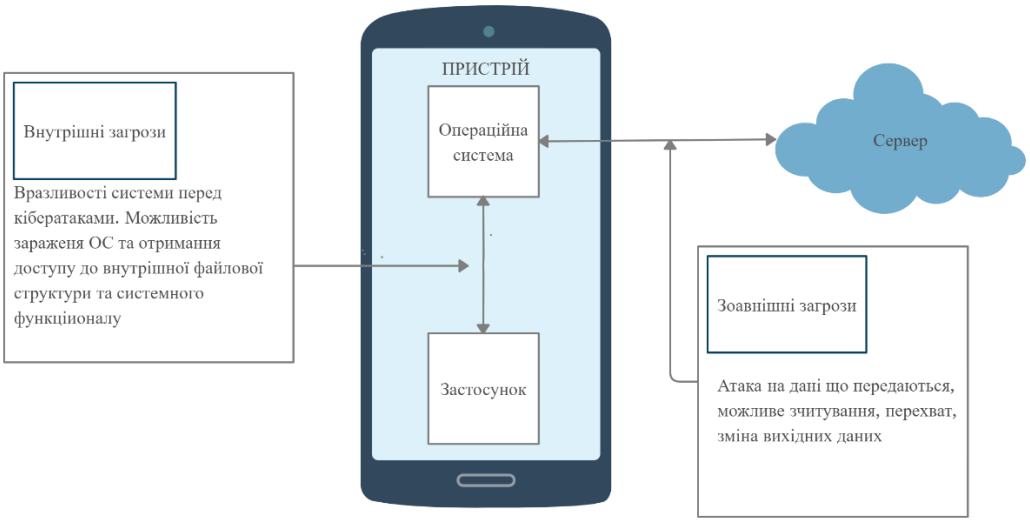

Рисунок 3.1 – Загальні типи загроз мобільного застосунку

Зовнішні загрози використовують мережу задля перехвату або модифікування пакетів даних користувача. Навіть досвідчені користувачі часто ігнорують основні правила мережевої безпеки, такі як підключатися тільки до відомих довірених мереж та не використовувати ресурси з застарілим або неправильнім сертифікатом. Особливою вразливістю мобільних систем є те що на

відміну від десктопу користувач виходить в мережу не через захищений браузер, а через мобільне застосування.

Враховуючи це, уся відповідальність за збереження даних користувача знаходиться в розробника застосування.

Внутрішні загрози є вразливостями системи перед різноманітними кібератаками, враховуючи те що зараження системи може відбутися у інших або навіть системних застосувань, розробнику необхідно не тільки захистити власне застосування від атак але й дані від можливого доступу зараженої системи.

В роботі [1] запропонована синергетична модель ІАУ, яка дозволяє забезпечити оцінку потокового стану інформаційної безпеки (ІБ) та визначити превентивні заходи та механізми захисту.

Для забезпечення оцінки критичних точок інфраструктури ІАУ пропонується використовувати удосконалені модель інфраструктури ІАУ [1]:

$$G^{CIES} = \{\{O^{CIES}\}, \{L^{CIES}\}, \{I_A\}\},$$

де $\{O^{CIES}\}$ це множина об'єктів що представляють елементи інфраструктури та їх зв'язок за рівнями моделі ISO/OSI $\{L^{CIES}\}$ – множини залежності між елементами інфраструктури, що визначається матрицею суміжності. [3]

$$A^{CIES} = \left\| a_{ij}^{CIES} \right\|.$$

$\{I_A\}$ – множина елементів інформаційних активів. Кожний елемент $I_{A_i} \in \{I_A\}$ являє собою вектор $I_{A_i} = \left(Type, A^C, A^I, A^A, A^{Av}\right)$. Де *Type* – це тип інформаційного елементу, що набуває одного з визначених значень *Type = {PlD, StO, OI, YI, PD, SI}*, де *PlD* – платіжні документи, *StO* – статистичні звіти, *Ol* – загальнодоступна інформація, *YI* – нормативна інформація, *PD* – власні дані користувача системи, *SI* – наукова інформація. Подальші елементи вектору являють собою булеві змінні представленні у целочисленному форматі (де 1-true, 0-false) та відображують необхідність властивості що вони репрезентують.

АС – конфіденційність, АІ – цілісність, АА – автентичність, доступність – ААv – безперервність [3]

Кожен елемент $O_l \in \{O^{CIES}\}$, також є вектором що описується як $O_l = \{Y^{CIES}, IO\}$, де Y^{CIES} – рівень ієрархії інформаційної структури що являє собою множину

$Y^{CIES} = \{FL, NL, OSL, DBL, BL\}$, де *FL* – фізичний рівень, *NL* – мережевий рівень, *OSL* –рівень операційної системи, *DBL* – рівень СУБД, *BL* – рівень застосунку. Для вказання типу зв'язку та існуючого відношення *IOR* між інформаційними активами та об'єктами середи, було запропоновано використання правила:

$$IO^R = \left\| IO_{il}^R \right\|$$

де IO_{il}^R це тип зв'язку між інформаційним активом (i) та об'єктом середи (l). При цьому $\forall i \in \{I_A\}$, а $\forall l \in \{O^{CIES}\}$.

Можливі значення [4]

$$IO_{il}^R = \begin{cases} 0, \text{ звязок відсутній} \\ cs, \text{ включає та зберігає} \\ pt, \text{ обробляє або передає} \\ so, \text{ реалізує функціионал} \end{cases}$$

Синергічну модель загроз запропоновано представляти як

$$ThM_{syn}^{CIES} = \{\{DF^{CIES}\}, \{T_{risk}\}, \{T_P\}, \{T_U\}, \{VH\}\},$$

де $DF^{SIES} = \{V^{NS}, V^{AS}\}$ що складається з: V^{NS} – природні загрози, $V^{AS} = \{V^{ACS}, V^{AIS}, V^{ASI}\}$ – антропогені загрози, де V^{ACS} – загрози кібербезпеки, V^{ASI} – загрози безпеки інформації, V^{AIS} – загрози інформаційної безпеки. Далі по

параметрах $ThM_{syn}^{CIES} - T_{risk}$ – якісний показник загрози, T_P множина імовірностей реалізації хоча б однієї з загроз, T_Uмножина збитків від успішної загрози, VH множина деструктивних станів елементів системи, тобто станів елементів що є небажаними або шкідливими та є результатом успішної кібератаки [4.]

Для отримання синергетичного зростання рівня захисту інформації необхідно враховувати комплексування загроз:

$$DF^{CIES} = \{V^{NS}\} \cup \{V^{AS}\} \text{ де } \{V^{AS}\} = \{V^{ACS}\} \cap \{V^{AIS}\} \cap \{V^{ASI}\}$$

Кожен елемент $DF_i \in \{DF^{CIES}\}$ можна представити як вектор значень DF_i $(T, T_p, pr_{ij}, r_{motiv})$, де Т – час успішної реалізації загрози, Тр – імовірність реалізації хоча б однієї загрози (де j – відповідний актив, і – відповідна загроза), $\forall i \in n$, n – кількість загроз, j –актив, $\forall j \in m$, m – кількість активів, r_{motiv} – імовірність мотивації злодія на реалізацію загрози [5].

Імовірність реалізації хоча б однієї загрози для кожного активу запропоновано розраховувати використовуючи формулу:

$$p_{rj} = 1 - \prod_{i=1}^{m} (1 - pr_{ij}),$$

де pr – імовірність реалізації загрози для одного відповідного активам.

Найбільш відомі загрози актуальні для платформи Android представлені на рис. 3.2.

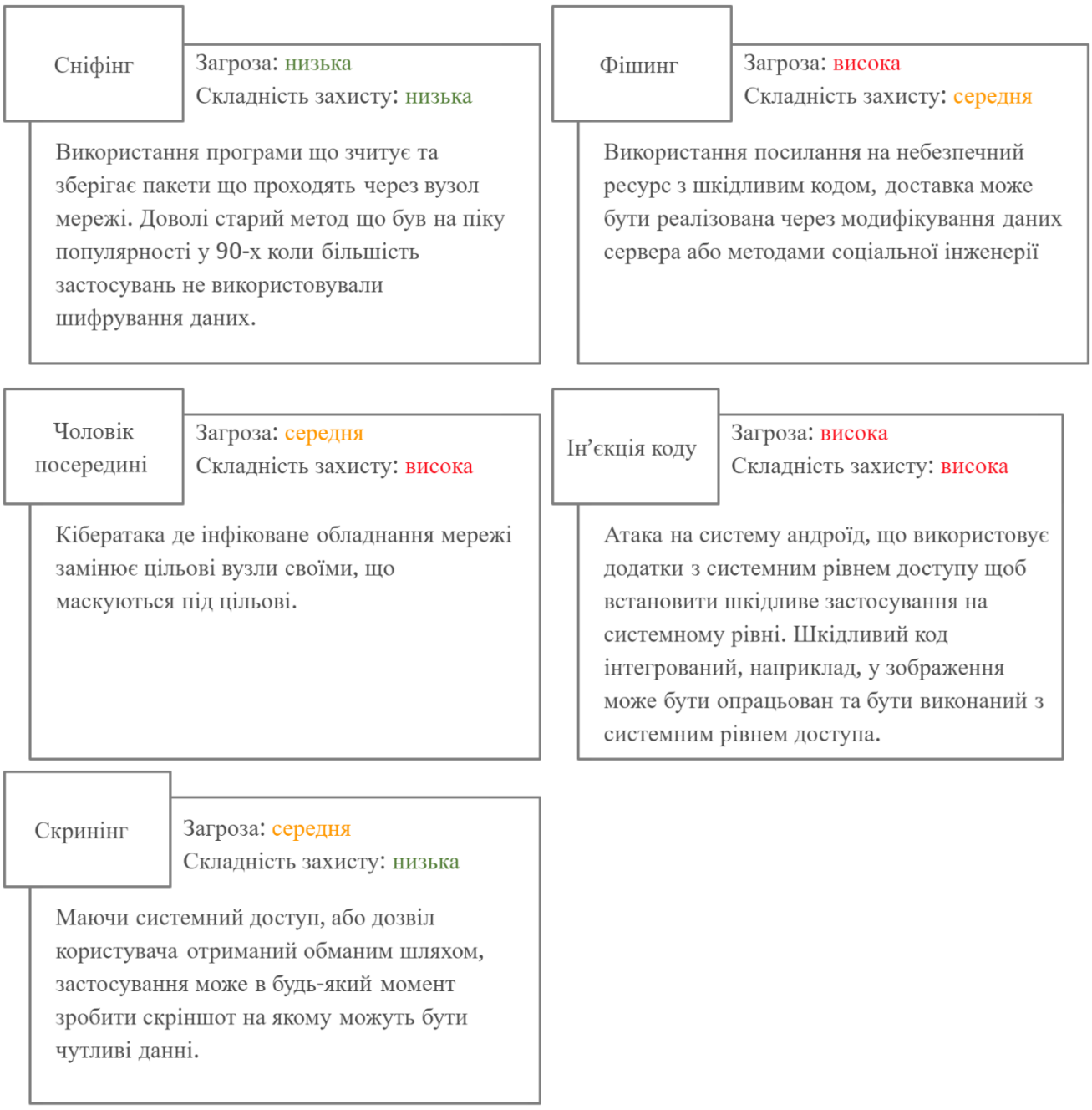

Рисунок – 3.2 Відомі загрози безпеки інформації для Android застосунків

3.2 Розрахування моделі загроз для мобільного застосунку "Кабінет викладача"

Маючи за основу дані о можливих загрозах, та методах їх розрахування ми можемо провести суттєвий аналіз безпеки майбутнього застосунку.

По-перше необхідно виділити типи інформаційних активів що будуть присутніми у застосунку, та визначити необхідні властивості.

У таблиці 3.1:

AC – конфіденційність;

AI – цілісність;

AA – автентичність, доступність;

AAv – безперервність

Таблиця 3.1 – Властивості компонентів

Тип	A^C	A^I	A^A	A^{Av}
SI – Наукова інформація	1	1	1	1
Ol – Загальнодоступна інформація	0	1	1	0
YI – Керуюча інформація	1	1	1	1
PD – Персональні дані	1	1	1	0

0 – послуга не підтримується

1 – послуга підтримується

Коли необхідні властивості виділено, ми маємо описати та виділити рівень зв’язку для кожного з елементів. Для цього потрібно виділити роль кожного елементу системи у функціонуванні застосунку.

Таблиця 3.2 – Рівень зв’язку компонентів.

Тип	Фіз. Рівень	Мережевий Рівень	Рівень ОС	Рівень СУБД	Рівень застосунку
SI – Наукова інформація	pt	pt	so	0	pt
Ol – Загальнодоступна інформація	pt	pt	so	cs	so

Закінчення табл. 3.2

Тип	Фіз. Рівень	Мережевий Рівень	Рівень ОС	Рівень СУБД	Рівень застосунку
YI – Керуюча інформація	pt	pt	so	0	pt
PD – Персональні дані	pt	pt	so	cs	so

де: 0 – зв’язок відсутній;

cs – включає та зберігає;

pt – обробляє чи передає ;

so – забезпечує функціонування;

Таблиця 3.3 – Рівень загроз кібератак для компонентів.

Загроза	Наукова інформація	Загальнодоступна інформація	Керуюча інформація	Персональні дані
Сніфінг	0.05	0.05	0.05	0.05
Ін’єкція коду	0.2	0.152	0.2	0.172
Скринінг	0.2	0.132	0.2	0.134
Фішинг	0.2	0.03	0.2	0.18
Чоловік посередині	0.267	0.152	0.267	0.24

Проаналізувавши ці загрози, можна дійти висновку що найбільш проблематичними загрозами є загрози з високою складністю захисту. Реалізація атаки “Чоловік посередні” може скомпрометувати дані не зважаючи на всі мережеві ступені захисту серверу. Превентивними заходами для захисту від цієї атаки має бути комплекс заходів з шифрування запитів, використання протоколів захищеного каналу зв’язку, та верифікація запитів як зі сторона клієнта так і зі сторони серверу.

Найбільш складною та небезпечною кібератакою є ін’єкція коду. Захист від шкідливого коду що виконується з системним рівнем доступу – неможливий, як і неможливо запобігти зараженню системи якщо в алгоритмах безпеки Android була знайдена вразливість. Тому, єдиним заходом забезпечення безпеки інформації користувача та інфраструктури є пасивний захист цієї інформації методом шифрування, у комплексі з рандомізованою генерацією ключа шифрування та обфускації вихідного коду.

Якщо провести аналіз кіберзагроз що є важливими для системи Android, їх можна поділити на три функціональних типи:

Атака на дані користувача – (ін’єкція коду, зараження системи) атака націлена на отримання даних користувача що зберігаються локально;

Атака на мережу – (сніфінг, фішинг, чоловік посередні) атака націлена на перехват або зміну даних що передаються через мережу;

Атака на систему – (скринінг) атака на дані користувача через уразливості системи;

3.3 Захист від атак на дані користувача

Виходячи з того що система може бути інфікована, єдиним способом захистити дані користувача є їх шифрування. Завдяки структурі MVVM ми можемо не використовувати системний метод onSaveInstanceState для обробки входу/виходу застосунку в режим сну. Замість цього усі локальні дані буде збережено у локальній базі даних, тому все що нам потрібно зробити – це захистити базу даних від несанкціонованого доступу. Це можна зробити за допомогою біблотеки SQLCipher яку необхідно настроїти за допомогою таких команд (приклад наведено для моделі розкладу):

```
final ScheduleDatabase room;


public ScheduleLocalStorage(String passphrase){
   SupportFactory factory = new SupportFactory(passphrase);
```

```
   room =  Room.databaseBuilder(activity, ScheduleDatabase.class,
ScheduleDatabase.NAME)
        .openHelperFactory(factory)
        .build();
}
```

Завдяки цьому ми маємо можливість працювати за БД через бібліотеку Room та зберігати локальні файли у зашифрованому вигляді. Для шифрування БД бібліотека використовує пароль що представлений змінною типу String у конструкторі. Цей пароль генерується за допомогою генератора випадкових чисел підчас першої ініціалізації застосунку та зберігається у шифрованому виді в Android Keystore API.

3.4 Захист від атак на мережу.

Для захисту від атак на мережу можна запровадити такі заходи як:

Використання захищеного сертифікату

Перевірка домену

Прив’язка до домену

Шифрування даних

Застосування використовує бібліотеку Retrofit для обробки запитів до серверу. Як мережевий клієнт використовується стандартна бібліотека OkHttp. Для використання SSL сертифікатів необхідно настроїти бібліотеку для роботи з відповідними протоколами SSL.

```
public void setupSsl(OkHttpClient.Builder builder) {
        ConnectionSpec spec = new
ConnectionSpec.Builder(ConnectionSpec.COMPATIBLE_TLS)
                .tlsVersions(TlsVersion.TLS_1_1, TlsVersion.TLS_1_2)
                .build();
builder.connectionSpecs(Collections.singletonList(spec));
```

Також на цьому етапі ми можемо додати компонент перевірки домену X509HostnameVerifier STRICT_HOSTNAME_VERIFIER що дозволяє використовувати тільки домен вказаний у сертифікаті та запиті. Додаєм цю команду до нашого методу настройки захисту:

```
builder.hostnameVerifier(SSLSocketFactory.STRICT_HOSTNAME_VERIFIER);
```

Наступним кроком буде прив'язка системи до домену та сертифікату що не дозволить серверу (якщо його було зараженно) переадресувати запит на інший домен:

```
CertificatePinner pinner = new CertificatePinner.Builder()
        .add(BuildConfig.PIN_HOST, BuildConfig.PIN_KEY)
        .build();
builder.certificatePinner(pinner);
```

Зараз, застосунок має усі необхідні засоби безпеки для роботи з мережею, але щоб бути певним у захисті даних у разі появи нових вразливостей у SSL протоколах, ми можемо власноруч зашифровати дані що відправляються на сервер, да дешифрувати дані з серверу. Нажаль бібліотека OkHttp не має стандартних зручних методів для цього, тому нам необхідно створити та зареєструвати компонент що буде обробляти запити. Для цього можна використати клас okhttp.Interceptor, в якому ми маємо можливість зашифровати да дешифрувати запити.

```
public class EncryptionInterceptor implements Interceptor {
  @Override
  public Response intercept(Chain chain) throws IOException {
    Request request = chain.request();
    RequestBody oldBody = request.body();
    Buffer buffer = new Buffer();
    oldBody.writeTo(buffer);
    String strOldBody = buffer.readUtf8();
    MediaType mediaType = MediaType.parse("text/plain; charset=utf-8");
```

```
            String strNewBody = encrypt(strOldBody);
            RequestBody body = RequestBody.create(mediaType, strNewBody);
            request = request.newBuilder().header("Content-Type",
body.contentType().toString()).header("Content-Length",
String.valueOf(body.contentLength())).method(request.method(), body).build();
            Response response = chain.proceed(request);
            ResponseBody responseBody = response.body();
            BufferedSource source = null;
            try {
               source = responseBody.source();
               source.request(Long.MAX_VALUE);
            } catch (IOException e) {
               return response;
            }
            Buffer buffer = source.buffer();
            String responseBodyString =
buffer.readString(java.nio.charset.Charset.forName("UTF-8"));
            String decrypredResponseString = decrypt(responseBodyString);
            Response.Builder rb = new Response.Builder();
            rb.body(ResponseBody.create(mediaType,decrypredResponseString));
            return rb.build();
   }
```

3.5 Захист від атак на систему

Самою простою, з точки зору захисту, атакою є скринінг, шкодлива програма що має системний доступ або дозвіл від користувача може зробити скріншот у будь-який момент та відправити його злодію. Система Android

дозволяє заборонити активності робити скріншот. Це робиться за допомогою виклику команди:

```
getWindow() .setFlags
 (LayoutParams.FLAG_SECURE,LayoutParams.FLAG_SECURE);
```

У нашому застосунку, два з трьох кореневих компонентів має приватні дані

InitialPageActivity – має дані о логіні та паролі користувача, і хоча пароль й замасковано компонентом View – під час вводу останній символ є видимим, що дозволяє вкрасти пароль через запис екрану.

MainActivity – фрагменти JournalPageFragment, ProfilePageFragment та LoadPageFragment можуть мати приватні дані викладачів чи студентів або корпоративні дані університету.

Вводячи захисні заходи, треба пам’ятати о зручності користувача. Заборона скріншоту робить складнішою можливість свідомо поділитися даними. Тому, на екранах MainActivity було запроваджено альтернативну опцію “Поділитися”, на екранах ProfilePageFragment, SchedulePageFragment та JournalPageFragment кнопка “Поділитися” формує текстову репрезентацію даних на екрані та дозволяє обрати застосунок для редагування чи відправлення цієї інформації.

3.6 Загальна система захисту

Роблячи підсумки систему захисту застосунку а також ураховуючи загальну структуру проекту можна зробити загальний огляд всієї системи. Увесь проект поділений на 2 групи: базову групу та множину груп функціоналу.

Базова група являє собою базову абстрактну імплементацію усього функціоналу такого як:

Робота з базою даних;

Зв’язок з сервером;

Логіка розподілу та обробки даних;

У рамках цієї реалізації також вбудовані компоненти захисту. Структура взаємодії компонентів захисту з архітектурою застосунку представлена на рис 3.3.

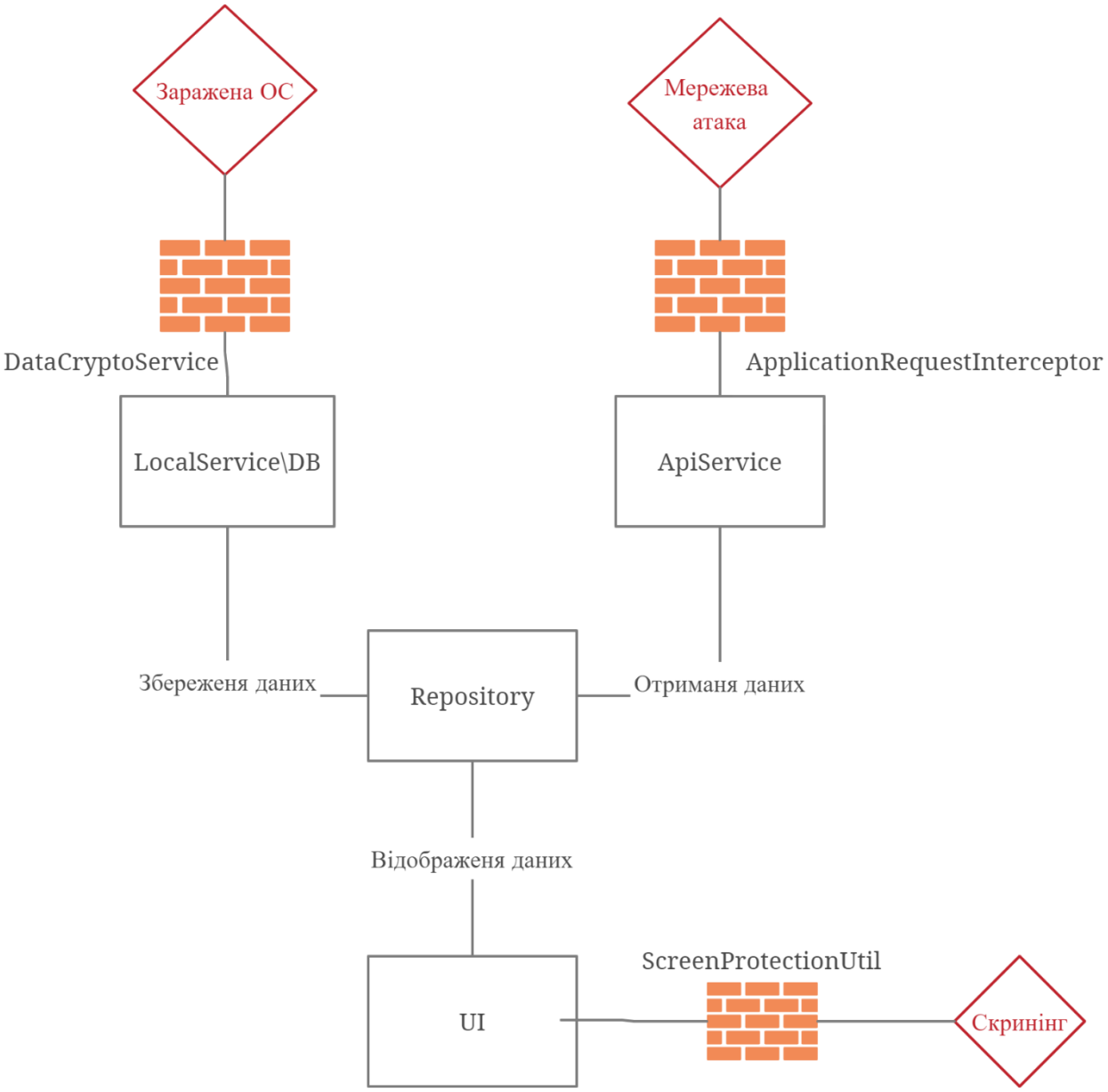

Рисунок 3.3 – Структурна схема системи захисту на основі допоміжних класів

Завдяки винесенню захисної та базової логіки у базовий пакет, та розподілу відповідальності, проект можливо розвивати силами декількох спеціалістів водночас. Спеціаліст з дизайну може змінювати зовнішній вигляд проекту працюючи з XML файлами не змінюючи при цьому логіку. Один чи декілька спеціалістів з програмування можуть вдосконалювати логіку елементів функціоналу без ризику створення нових вразливостей чи компрометування

існуючих систем захисту. У той самий час спеціаліст з кібербезпеки може вдосконалювати існуючи системи захисту, реагувати на нові кібератаки та виявлені вразливості операційної системи, не заважаючи розробці елементів функціоналу.

Така структура проекту може бути використана не тільки при розробці мобільних застосунків але й при розробці веб-застосунків, десктопних рішень та серверних систем.

ВИСНОВКИ

В ході виконання магістерської роботи був практично реалізований застосунок який дозволяє спростити щоденні задачі викладачів та захистити дані викладачів та студентів від можливих кібератак.

При виконанні роботи використовувалися такі інструментальні засоби: Android Studio, Creately

Архітектура система построєна на таких бібліотеках як: AndroidX, Room, Retrofit, OkHttp, SQLChipper, Material.

Архітектура компонентів реалізована на базі сучасної концепції MVVM (Model-View-ViewModel) що дозволяє розподілити логіки за функціональним типом.

У ході розробки застосунку було проведене дослідження для вияви потреб викладачів у мобільних рішень, та необхідні властивості цього рішення. Дослідження було зроблено методом опитування та діалогу з викладачами. Зібрані побажання було проаналізовано та перетворено у технічне завдання, на основі якого було розроблено структуру застосунку та необхідний функціонал, було виведено критерії якості застосунку.

В рамках роботи було проведено аналіз структурної системи інноваційно-активного університету що розроблена у ХНЕУ ім. Семена Кузнеця. Також було виділено п’ять основних загроз властивих для застосунків на базі операційної системи Android. Ці загрози було проаналізовано та розраховано їх ризики. Для усіх вивчених загроз, незалежно від рівня ризику, було розроблено систему заходів безпеки що гарантує цілісність, конфіденційність да доступність даних для авторизованих користувачів.

Відомі загрозу було класифіковано то розподіллено на три типи: системні загрози, загрози даних та мережеві загрози. Системні загрозу було вирішено заходами системних налаштувань унеможливаючими кібератаки на цьому рівні. Мережеві загрози було знешкоджено превентивними заходами з шифрування, верифікаціях та відмово стійкості мережевих компонентів. Загрози рівню даних

було попереджене заходами шифрування бази даних а також даних що зберігаються у системному сховищі.

При розробці застосунку було враховано його подальший розвиток. Структура та архітектура були розроблені таким чином щоб нові спеціалісти не зустрічали труднощів у покращенні та доповнені будь яких елементів системи.

Застосунок виконано з урахуванням усіх сучасних вимог до стилю коду та супровідної документації що дозволить іншим студентам швидко зрозуміти структуру та логіку застосунку, та легко внести зміни до будь якого компоненту. Розподіл логіки між компонентами дозволить вносити зміни студентам різних напрямків, студенти-дизайнери можуть вдосконалювати дизайн, у той самий час коли студенти-програмісти можуть вдосконалювати логіку а студенти з факультету кібербезпеки працювати над алгоритмами захисту.

СПИСОК ДЖЕРЕЛ ІНФОРМАЦІЇ

1 S. Yevseiev, O. Rayevnyeva, V. Ponomarenko, O. Milov, Development of methodological principles for the construction of a corporate information educational system of innovative-active University in the framework of anticorruption activities. Eastern-European Journal of Enterprise Technologies . 2020. 5/2(107). P. 6–28.

2 Грищук Р. В. Основи кібернетичної безпеки: Монографія / Р. В. Грищук, Ю. Г. Даник; за заг. ред. Ю. Г. Данника.–Житомир: ЖНАЕУ, 2016.–636 с.

3 ДСТУ ISO/IEC TR 13335-4:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 4. Вибирання засобів захисту. [Електронний ресурс]. Доступно: http://metrology.com.ua/download/iso-iec-ohsas-i-dr/61-iso/290-dstu-iso-iec-tr-13335-4-2005.

4 ISO/IEC 27006:2015 – Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems [Online]. Available: http://www.iso.org/iso/home/search.htm?qt=ISO%2FIEC+27006%3A2015+&sort=rel&type=simple&published=on. Accessed on: Oct. 7.2020.

5 С. Евсеев, “Синергетическая модель оценки безопасности банковской информации”, Науково-технічний журнал «Інформаційна безпека», № 4 (24), с. 104 – 118, 2016.

6 Бакулін М.Г., Варукіна Л.А., Крейнделін В.В. Технологія MIMO. Принципи і алгоритми. – М.: Гаряча лінія – Телеком – 2014. – 242 с.

7 В.М Вісневський, Портной С.Л., Шахнович І.В. – Енциклопедія 4G, Москва, Техносфера, 2009 – 314 с.

8 Волков Л.Н., Немировський М.С., Сінаков Ю.С. Цифрові радіосистеми. – М.: Екотренди – 2005. 392 с.

9 Миронов, А.Є., Саітов, ІА Планування та побудова цифрових комунікаційних мереж Сигнальні системи / А.Є. Миронов, І.А. Саітов, М.: Посібник з проектування курсів та дипломів. – Орел: Російська академія спеціального зв’язку, 2004. 216 с.

10 Протокол DIAMETR. Технічні матеріали / URL-адреса IBM: http://www.ibm.com/developerworks/ru/library/wi-diameter/ (дата виклику: 20.04.2020).

11 Основні загрози безпеки пакету 4G / URL-адреса: https: https://www.ptsecurity.com/ru-ru/research/analytics/epc-2017/ (дата виклику: 20.04.2020).

12 Діаметр протоколу вразливостей в мережах 4G / URL: https://www.ptsecurity.com/ru-ru/research/analytics/diameter-2018/ (дата виклику: 20.04.2020).

13Путівник по LTE Security // URL:csrc.nist.gov/publications/drafts/80187/sp800_187_draft.pdf. (дата звернення: 01.03.2020).

14 Тихвінський В.О., Терентьєв С.В., Юрчук А.В. – Мобільні мережі LTE: Технології та архітектура, Москва, Еко-тренди, 2010 – 158 с.

15 Sklar B. Цифровий зв'язок. М.: Ред. Будинок Вільямса – 2003. 1100 с.

16 Про затвердження норм часу для планування і обліку навчальної роботи та переліків основних видів методичної, наукової й організаційної роботи педагогічних і науково-педагогічних працівників вищих навчальних закладів: Наказ Міністерства освіти і науки України від 07.08.2002 № 450 // База даних База даних "Міністерства освіти України" / МОН України. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/REG6986.html.

17 Положення "Про рейтингове оцінювання діяльності науково-педагогічних працівників, кафедр і факультетів Харківського національного економічного університету імені Семена Кузнеця". Харків, 2019. URL: https://www.hneu.edu.ua/wp-content/uploads/2019/11/Polozhennya-pro-rejtyng-NPP.pdf (дата звернення: 06.04.2020).

18 Щодо особливостей організації освітнього процесу та формування навчальних планів у 2015/2016 навчальному році: Лист Міністерства освіти і науки України від 13.03.2015 № 1/9-126 // База даних "Міністерства освіти України" / МОН України. URL: http://vnz.org.ua/dokumenty/spysok/7514-lyst-mon-ukrayiny-19-126-vid-13032015r

19 Управління якістю освіти у вищих навчальних закладах [Текст] : навч. посіб. : у 2 ч. Ч. 1: Теоретичні засади формування систем управління якістю надання освітніх послуг / кол. авт. ; за заг. ред. чл.-кор. НАН України В.С. Загорського. Львів: ЛРІДУ НАДУ, 2011. 136с.

20 Шевченко В.М. Особливості формування механізмів державного управління вищими навчальними закладами в умовах євроінтеграції та інноваційного розвитку України // Адміністративне право і адміністративний процес. Дата оновлення: 04.12.2019 URL: www.kbuapa.kharkov.ua/e-book/db/2010-1/doc/5/07.pdf (дата звернення: 06.12.2019).

21 Положення про організацію позанавчальної роботи зі студентами. Харків, 2015. URL: https://www.hneu.edu.ua/wp-content/uploads/2020/02/Polozhennya-pro-organizatsiyu-pozanavchalnoyi-roboty-zi-studentamy.pdf (дата звернення: 06.04.2020).

22 Положення про організацію навчального процесу із використанням технологій дистанційного навчання у Харківському національному економічному університеті імені Семена Кузнеця. Харків, 2019 URL: https://www.hneu.edu.ua/wp-content/uploads/2020/02/Polozhennya-pro-organ-navch-protsesu.pdf (дата звернення: 06.04.2020).

23 Положення про організацію оцінювання результатів навчання та якості вищої освіти із застосуванням дистанційних технологій у Харківському національному економічному університеті імені Семена Кузнеця URL: https://www.hneu.edu.ua/wp-content/uploads/2020/05/Polozhennya-pro-organizatsiyu-otsinyuvannya-rezultativ-navchannya-Dyst.-tehnologiyi.pdf. Харків, 2020 (дата звернення: 06.04.2020).

24 Настройка Active Directory. Windows Server 2008 / Holme Dan [и др.]. Москва: Русская редакция, 2011. URL: https://www.litmir.me/bd/?b=182195 (дата обращения 19.04.2020)

25 Адресная книга LDAP за пять минут [Електронний ресурс]: библиотека Линуксцентра URL: http://www.linuxcenter.ru/lib/articles/soft/address_book_ldap.phtml (дата обращения: 04.05.2020).

26 Web-сторінка кафедри кібербезпеки та інформаційних систем ХНЕУ ім. С. Кузнеця [Електронний ресурс]: практика та загальні відомості. Дата оновлення: 15.02.2020. URL: http://www.kafcbit.hneu.edu.ua/ (дата звернення: 16.02.2020).

27 Web-сторінка сайту з синатаксисом протоколу LDAP для Active Directory. Дата оновлення: 28.03.2020. URL: https://social.technet.microsoft.com/wiki/contents/articles/5392.active-directory-ldap-syntax-filters.aspx (дата звернення: 06.04.2020).

28 Web-сторінка довідника ldapsearch. Дата оновлення: 28.03.2020. URL: https://linux.die.net/man/1/ldapsearch (дата звернення: 06.04.2020).

29 Основы технологий баз данных: учеб. пособ. / Б.А. Новиков [та ін.] Москва: ДМК Пресс, 2016. 240с.

30 Web-сторінка довідника Android Documentary. URL: https://developer.android.com/reference/android/view/WindowManager.LayoutParams.html#FLAG_SECURE (дата звернення: 06.11.2020).

31 Н. А. Молдовян, А. А. Молдовян, и М. А Еремеев Криптография: от примитивов к синтезу алгоритмов, СПб.: БХВ, Петербург, 2004.

32 С. Э. Остапов, С. П. Евсеев, и О. Г. Король Технологии защиты информации, Черновцы: Издательский дом «РОДОВИД», 2014.

33 В. Столлингс Криптография и защита сетей: принципы и практика[Пер. с англ.]; 2-е изд.М. : ИД «Вильямс», 2001.

34 С. П. Євсеєв, С. Е. Остапов, Х. Н. Рзаєв, та В. І. Ніколаєнко, Оцінка обміну даними в глобальних обчислювальних мережах на основі комплексного показника якості обслуговування мережі, Науковий журнал Радіоелектроніка, інформатика, управління, № 1(40), с. 115 – 128, 2017.

35 S. Yevseiev, V. Ponomarenko, O. Rayevnyeva Assessment of functional efficiency of a corporate scientificeducational network based on the comprehensive indicators of quality of service, Eastern-European Journal of Enterprise Technologies ISSN 1729-3774 6/2 (90) 2017.