Міністерство освіти і науки України
Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра комп’ютерних наук

Пояснювальна записка

до магістерської кваліфікаційної роботи

на тему: «Інформаційна технологія захисту абонента мобільного зв’язку»

Виконав: студент 2 курсу,
групи 2КН-18м
Спеціальності 122 «Комп'ютерні науки»
Верхось Д.О.

Керівник: PhD, проф. Савчук Т.О.

Рецензент:к.т.н.,доц.
Коваленко О.О.

м. Вінниця – 2019 рік

ЗАТВЕРДЖУЮ

Завідувач кафедри____КН____
д.т.н., проф.. Яровий А.А.

_____
(підпис)
“____” _____2019 року

ЗАВДАННЯ

на магістерську кваліфікаційну роботу на здобуття кваліфікації магістра зі спеціальності: 122 – «Комп'ютерні науки»

08-22.МКР.025.18.000.ПЗ

Магістранта групи 2КН-18м Верхося Дмитра Олександровича

Тема магістерської кваліфікаційної роботи: «Інформаційна технологія захисту абонента мобільного зв‘язку»

Вихідні дані до роботі: мова програмування – об’єктно-орієнтована, кількість абонентів, що мають доступ до персональних даних рольового абонента – необмежене, можливість коригувати доступ до персональних даних - можливе, кількість рівнів QRn доступу до персональних даних - не менше 5.

Короткий зміст частин магістерської кваліфікаційної роботи:

1. Зміст пояснювальної записки: Вступ. 1 сучасний стан розвитку технологій забезпечення захисту абонента мобільного зв’язку. Розробка моделі захистуабонента мобільного зв’язку, Розробка методу захистуабонента мобільного зв’язку, Розробка інформаційної технології захисту абонента мобільного зв’язку, Економічний розділ. Висновки.

2. Перелік графічного матеріалу: UML-діаграма прецедентів інформаційної технології захисту абонентів мобільного зв’язку, UML-діаграма роботи інформаційної технології захисту абонентів мобільного зв’язку, Схема взаємодії вузлів інформаційної технології захисту абонентів мобільного зв’язку, Загальна модель захисту абонентів мобільного зв’язку, Графічна схема інтерфейсу сторінки користувача для управління доступом, Структурна схема інтерфейсу інформаційної системи захисту абонентів мобільного зв’язку.

КАЛЕНДАРНИЙ ПЛАН ВИКОНАННЯ МКР

№ етапу	Назва етапу	Термін виконання		Очікувані результати
		початок	кінець	
1	Аналіз сучасного стану розвитку технологій забезпечення захисту абонентів мобільного зв'язу.			Аналітичний огляд літературних джерел, задачі досліджень, розділ 1 ПЗ
2	Порівняльний аналіз моделей, методів захмсту абонентів мобільного зв'язку.			Метод, інформаційна технологія, розділ 2,3
3	Проектування програмних засобів інформаційної технології захисту абонентів мобльного зв'язку			Програмне забезпечення, розділ 4
4	Підготовка економічної частини			розділ 5
5	Апробація та/або впровадження результатів дослідження			тези доповідей/акт впровадження
6	Оформлення пояснювальної записки, графічного матеріалу та презентації			Пояснювальна записка, графічний матеріал, презентація

Консультанти з окремих розділів магістерської кваліфікаційної роботи

1. Науковий керівник _____ PhD, професор кафедри КН
(підпис) наук. ступінь, вчене звання (посада)
"____" _____20___ р. Т.О. Савчук
ініціали та прізвище

2. Економічна частина _____ канд. екон. наук, доц. кафедри ЕПВМ
(підпис) наук. ступінь, вчене звання (посада)
М. В. Бальзан
ініціали та прізвище

"____" _____20___ р.

Дата попереднього захисту роботи "____" _____20___ р.

Рецензент _____ канд. техн. наук, доц. кафедри ПЗ
(підпис) наук. ступінь, вчене звання (посада)
к.т.н.,доц.О.О. Коваленко
ініціали та прізвище

Завдання видав
науковий керівник _____ PhD, професор кафедри КН
(підпис) наук. ступінь, вчене звання (посада)
Т.О. Савчук
ініціали та прізвище

"____" _____20___ р.

Завдання отримав магістрант _____ _____ Д.О. Верхось
(підпис) ініціали та прізвище

"____" _____20___ р.

АНОТАЦІЯ

Магістерську кваліфікаційну роботу присвячено інформаційній технології захисту абонента мобільного зв’язку. Удосконалено модоль і метод з урахуванням поставлених критеріїв та розроблено програмне забезпечення для захисту персональних даних абонента мобільного зв’язку.

Програмна реалізація інформаційної технології захисту даних абонентів мобільного зв’язку написана мовою програмування ASP.NET C# та бібліотеку React для реалізації інтерфейсу користувача.

Тестування інформаційної технології захисту абонентів мобільного зв’язку виконано у середовищах розробці Microsoft Visual Studio, Microsoft Visual Studio Code та експерментальним методом.

ANNOTATION

The master's qualification is devoted to information technology of protection of the subscriber of mobile communication. Improved the criteria-based model and method and software for protecting the personal information of a mobile subscriber.

The software implementation of mobile data protection information technology is written in ASP NET C # programming language and React library for user interface implementation.

Mobile telephony security information technology testing was performed in the Microsoft Visual Studio, Microsoft Visual Studio Code development environments and experimentally.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Захист персональних даних у сучасному технологічному світі відіграє важливу роль у діяльності не тільки кожної окремої людини, а й має вагоме значення на державному рівні [1]. Різні по важливості документи і дані мають різний ступінь захищеності. У інтернеті існують тисячі баз даних з номерами абонентів та персональними даними, якими можуть користуватися різні користувачі. Таким чином, постає актуальна задача у створенні засобів, що сприятимуть захисту персональних даних через мобільний зв‘язок за рахунок аналізу кожного абонента, що отримав доступ до них. Комп'ютерні та обчислювальні технології в 21 столітті безперервно удосконалюються і модернізуються. Те, що було немислимо 10 років тому, зараз є невід'ємною частиною сучасного життя. У зв'язку з цим, нові технології розробляються для більш мобільної та інтерактивної взаємодії людини з навколишнім світом. Вони спрощують процес виконання монотонної роботи і скорочують багато часу, який витрачається на процеси, котрі можуть бути виконані обчислювальними системами за лічені секунди.

Крім того, в сучасному світі зберігається дуже багато інформації про все і виникає потреба в швидкому пошуку та обробці цієї інформації. Прогрес у цій області в значній мірі визначається розвитком відповідних технологій.

Таким чином з кожним роком кількість інформації, що оброблюється і аналізується кожною окремою людиною збільшується у геометричній прогресії. Такою ситуацією користуються зловмисники і шахраї, котрі маніпулюють інформацією. Через це звичайній людині тяжко, а інколи навіть небезпечно користуватися новітніми технологіями [2].

Особливу увагу необхідно приділяти абонентам мобільного зв‘язку. У сучасному світі звичайний абонент не завжди розуміє, що передаючи свій абонентський номер телефону іншій людині чи організації, він частково передає частину своїх персональних даних, а це може стати причиною подальшої передачі персональних даних і в кінці кінців абонент, котрий

передав свої персональні дані не відповідальній особі, може почати отримувати «спам» повідомлення.

Захист абонентів мобільного зв‘язку забезпечують мобільні оператори але навіть вони не завжди відносяться до захисту персональних даних цілком відповідально. Таким чином, люди ненавмисно стають жертвами мобільних шахраїв, часто надаючи усю необхідну інформацію прямісінько до рук зловмисників.

Тому актуальною є розробка інформаційної технології захисту абонента мобільного зв‘язку, яка допоможе кожному абоненту забезпечити захист персональних даних та надасть змогу відслідковувати та керувати активність абонентів, котрим було надано доступ до своїх персональних даних.

Зв'язок роботи з науковими програмами, планами, темами. Магістерська робота виконана відповідно до напрямку наукових досліджень кафедри комп’ютерних наук Вінницького національного технічного університету 22 К1 «Моделі, методи, технології та пристрої інтелектуальних інформаційних систем управління, економіки, навчання та комунікацій» та плану наукової та навчально-методичної роботи кафедри.

Мета та завдання дослідження. Метою дослідження є підвищення рівня захисту даних абонента мобільного звязку.

Для досягнення поставленої мети необхідно вирішити такі задачі:

- проаналізувати особливості існуючих моделей і методів захисту абонентів мобільного зв’язку;

- удосконалити існуючі моделі і методи, використовуючи сучасні технології;

- розробити інформаційну технологію, що базується на удосконалених моделях і методах захисту абонентів мобільного зв’язку.

Об'єкт дослідження – це процес захисту абонентів мобільного зв’язку.

Предмет дослідження – це моделі і методи захисту абонентів мобільного зв’язку.

Наукова новизна одержаних результатів полягає в наступному:

− уперше запропоновано інформаційну технологію захисту абонента мобільнго зв’язку, яка підвищує рівень захиста даних абонента мобільного зв’язку надаючи ролі та повноваження кожному абоненту.

− удосконалено модель захисту абонента мобільного зв’язку, яка використовує QR-кодування для пришвидшення аналізу доступу до даних абонента.

− удосконалено метод захисту абонента мобільного зв’язку, який записує кожнового абонента мобільної мережі до структури даних і присвоює унікальний ідентифікатор кожному абоненту, це дозволить підвищити рівень захисту даних абонента мобільного звязку.

Практичне значення одержаних результатів полягає у наступному:

1. Розроблено узагальнений алгоритм захисту даних абонента мобільного зв’язку з використанням QR - кодування.

2. Розроблено систему захисту абонента мобільного зв’язку.

Достовірність теоретичних положень магістерської кваліфікаційної роботи підтверджується строгістю постановки задач, коректним застосуванням математичних методів під час доведення наукових положень, строгим виведенням аналітичних співвідношень, порівнянням результатів з відомими, та збіжністю результатів математичного моделювання з результатами, що отримані під час впровадження розроблених програмних засобів.

Апробація результатів роботи Результати дослідження позитивно апробовані на конференції «Молодь в науці: дослідження, проблеми, перспективи» та на XLVIII Науково-технічній конференції факультету інформаційних технологій та комп'ютерної інженерії (м. Вінниця, Україна, 2019 р.) та опубліковані у збірниках даних конференцій.

Публікації За результатами досліджень подано заявку на реєстрацію авторського права на твір (комп'ютерну програму) “Інформаційна технологія захисту абонентів мобільного зв’язку” (номер реєстрації заявки АПС/10094-18), а також опубліковано 2 тез доповіді з науково-технічних конференцій.

1 СУЧАСНИЙ СТАН РОЗВИТКУ ТЕХНОЛОГІЙ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ АБОНЕНТА МОБІЛЬНОГО ЗВ’ЯЗКУ

1.1 Аналіз моделей і методів захисту абонента мобільного зв’язку

У сучасному світі з кожним роком збільшується кількість роботи, яку люди роблять перед екранами своїх комп’ютерів та телефонів, це необхідно для того, аби збільшити швидкість виконання роботи та зменшити кількість помилок, котрі можуть бути виникненні через людський фактор. Окрім цього швидкість виконання завдань значно пришвидшується. За один і той самий час людина здатна виконати у рази більше роботи не витрачаючи на це більше зусилля. З використанням сучасних технологій ми можемо підписувати офіційні документи, здійснювати перекази коштів у будь-яку частину світу, купувати будь-що. Таким чином, людям необхідно бути дуже уважними і обережними використовуючи новітні засоби зв’язку і комунікації. Окрім плюсів використання новітніх технологій є ще й мінуси – це захищеність персональних даних і атаки шахраїв.

Разом з сучасними технологіями розвиваються і сучасні шахраї, котрі модернізують і використовують нові способи обману. Одним із таких є сховані у рекламних повідомленнях шкідливі програми, котрі здатні причинити шкоду кожному, хто випадковим чином завантажить їх. Оскільки рекламні повідомлення, сильно відрізняються від звичайної кореспонденції, існують різні моделі боротьби з ними [3]. Розглянемо існуючі моделі боротьби із небажаними повідомленнями:

- профілактика;
- фільтри «чорного списку»;
- фільтри «білого списку»;
- фільтри «сірого списку»;
- обмеження можливостей поштового сервісу;
- платний E-mail.

Оскільки, одним із най незахищених процесів комунікації є мобільний зв’язок – надалі будемо розглядати моделі, які використовуються для подолання спам повідомлень, саме на мобільних пристроях. Поширеним моделлю боротьби зі спамом стало фільтрування його з вхідного потоку повідомлень. На даний час ця модель - основна і найбільш широко використовується.

Існує мобільне програмне забезпечення для автоматичного пошуку спаму, так звані спам-фільтри. Воно може бути призначене для кінцевих користувачів або для використання на серверах. Це програмне мобільне забезпечення використовує два основні методи. Перший полягає у тому, що аналізується зміст повідомлення і робиться висновок, спам це чи ні. Повідомлення, класифіковане як спам, відокремлюється від іншої кореспонденції: воно може бути позначено, переміщено в іншу папку, видалено. Таке програмне забезпечення може працювати як на сервері, так і на комп'ютері клієнта. В останньому випадку користувач не бачить відфільтрованого спаму, але продовжує нести витрати, пов'язані з його прийомом, тому що фільтруюче програмне забезпечення отримує кожне повідомлення і тільки потім вирішує, показувати його чи ні. З іншого боку, якщо програмне забезпечення працює на сервері, користувач не несе витрат з передачі його на свій телефон [4].

Другий підхід полягає в тому, щоб, застосовуючи різні методи, визначити відправника як спамера, не заглядаючи в текст листа. Це програмне забезпечення може працювати тільки на сервері, який безпосередньо приймає повідомлення. При такому підході додатковий трафік витрачається тільки сервером на спілкування із спамерськими повідомленнями програмами (тобто на відмови приймати повідомлення) і звертання до інших серверів (якщо такі потрібні) при перевірці.

Програми автоматичної фільтрації використовують статистичний аналіз змісту листа для прийняття рішення, чи є воно спамом. Найбільшого успіху вдалося досягти за допомогою алгоритмів, заснованих на теоремі Байеса. Для

роботи цих методів потрібно попереднє –навчання– фільтрів шляхом передачі йому розсортованих вручну листів для виявлення статистичних особливостей нормальних листів і спаму. Метод дуже добре працює при сортуванні текстових повідомлень (в т.ч. HTML). Після навчання на досить великій вибірці вдається відсікти до 95-97% спаму. Для уникнення таких фільтрів спамери іноді поміщають змістовну частину в картинку, вкладену в лист, текст же або відсутній, або випадковий, що не дозволяє фільтру скласти статистику для розпізнавання таких повідомлень. У цьому випадку необхідно користуватися програмами розпізнавання тексту, або використовувати інші методи [5].

Запорука надійної роботи Байєсівського методу - постійне донавчання фільтра і вказівки йому на вчинені помилки. У поштових програмах для цього вводиться можливість ручної позначки повідомлення –спам / не спам–, а в поштових сервісах в мережі Інтернет - кнопка –поскаржитися на спам. Багато програм і поштових сервісів в мережі Інтернет дозволяють користувачеві задавати власні фільтри. Такі фільтри можуть складатися зі слів або, рідше, регулярних виразів, в залежності від наявності або відсутності яких повідомлення потрапляє або не потрапляє в сміттєвий ящик. Однак така фільтрація трудомістка і негнучка, крім того, вимагає від користувача певної міри знайомства з комп'ютерами. З іншого боку, вона дозволяє ефективно відсіяти частину спаму, і користувач точно знає, які повідомлення будуть відсіяні і чому [6].

Чорні списки Realtime Blackhole List (RBL) - величезна база даних з відкритих поштових серверів (relay). Під словом –відкритий– у даному випадку розуміється відсутність адекватного адміністрування сервера, що призводить до неконтрольованих розсилок спаму через такі сервера. Конкретно, відкритість виражається в тому, що сервер приймає повідомлення від кого завгодно і відправляє її далі, теж для кого завгодно, а не тільки для своїх користувачів. Якщо з будь-якої номера постійно розсилається спам і адміністрація сервера, через який здійснюється розсилка, не приймає ніяких заходів, можна повідомити про спамерів у RBL. Спамера занесуть у базу даних і всі

провайдери, які приєдналися до проекту RBL, та й просто усі системи будуть автоматично забороняти прийом повідомлень з цього поштового сервера. Також використовується технологія DNSBL - список номерів, що динамічно оновлюється, за допомогою яких вироблялися розсилки незапитаних повідомлень. Існує безліч різноманітних DNSBL, що розрізняються як політикою внесення та видалення номерів, так і оперативністю роботи. Їх використання відсікає помітну частину непрошеної пошти. Проте, працює це тільки в тому випадку, якщо сервер, що знаходиться в списку, розсилає повідомлення прямо на ваш сервер [7].

Сірі списки Метод сірих списків заснований на тому, що «поведінка» програмного забезпечення, призначеного для розсилки спаму, відрізняється від поведінки звичайних серверів, а саме, спамерські програми не намагаються повторно відправити повідомлення при виникненні тимчасової помилки, як того вимагає протокол SMTP. Точніше, намагаючись обійти захист, при подальших спробах вони використовують іншу зворотній номер, тому це виглядає для приймаючої сторони як спроби відправки різних повідомлень. Найпростіша версія сірих списків працює наступним чином. Всі раніше невідомі SMTP-сервера записуються до «сірого» списку. Пошта з таких серверів не приймається, але й не відхиляється зовсім - їм повертається код тимчасової помилки («приходьте пізніше»). У випадку, якщо сервер-відправник повторює свою спробу не менш ніж через деякий час (цей час називається затримкою), сервер вноситься в білий список, а повідомлення приймається. Тому звичайні повідомлення (не спам) не втрачаються, а тільки затримується їхня доставка (вони залишаються в черзі на сервері відправника і доставляються після однієї або декількох невдалих спроб). Програми-спамери або не вміють повторно відправляти повідомлення, або використовуються ними номери встигають за час затримки потрапити в чорні списки DNSBL. Цей метод на даний час дозволяє відсіяти до 90% спаму практично без ризику втратити важливі повідомлення. Проте його теж не можна назвати бездоганним

за наступними причинами: – Можуть помилково відсіюватися листи з серверів, що не виконують рекомендації протоколу SMTP, наприклад, розсилки з сайтів новин. Сервера з такою поведінкою по можливості заносяться до білих списків. Білі списки - це ще один метод по боротьбі з шкідливими програмами або спамом. Замість того, щоб шукати тільки відомі шкідливі програми, це технологія запобігає виконанню всіх комп'ютерних кодів за винятком тих, які були раніше позначені системним адміністратором як безпечні. Вибравши цей параметр відмови за умовчанням, можна уникнути обмежень, характерних для оновлення сигнатур вірусі [8].

До того ж, ті застосування на комп'ютері, які системний адміністратор не хоче встановлювати, не виконуються, тому що їх немає в «білому списку». Таким самим чином адміністратор може створити список абонентів мобільного зв’язку, котрим буде надано дозвіл на вхідні дзвінки і повідомлення, керувати ним, постійно вносячи коригування. Цей метод є достатньо надійним, тому що забороняє надходження будь-яких повідомлень від абонентів, яких мнемає у списку, а отже зникає можливість випадкової помилки.

У таблиці 1.1 відображено порівняльну характеристику методів захисту абонента мобільного зв’язку.

Таблиця 1.1 - Порівняльна характеристика методів захисту абонента мобільного зв’язку

Характеристики	Білі списки	Сірі списки	Чорні списки
Отримання повідомлень від невідомих контактів	-	+	+
Масшабованість	+	+	-
Швидкодія	-	-	+
Визначення Спам повідомлень	-	+	-
Відправка повідомлень	+	+	+

Аналіз сучасних методів і моделей передбачає створення сучасної інформаційної системи захисту абонента мобільного зв’язку, яка надасть повну захищеність користувачу від небажаної пошти і задовільнить абонента зв'язку своїм сучасним функціоналом, швидкодією [9].

Отже, проаналізувавши всі методи та моделі захисту абонента мобільного зв’язку, можна зробити висновок, що для реалізації усіх поставлених завдань може підійти удосконалена модель білих списків. Удосконалення мають збільшити швидкодію виконання даного методу та полегшити маштабованість даного метода.

1.2 Аналіз технологій захисту абонента мобільного зв’язку

Захист даних в телекомунікаційно-інформаційних системах це один із основних сегментів національної програми концепції технічного захисту інформації в Україні [10]. Триває розвиток нових методів захисту інформації та удосконалення відомих засобів забезпечення безпеки телекомунікаційних систем. Зокрема, в літературі розглянуто принципи побудови систем зв’язку, стандарти та загрози інформаційній безпеці. В роботі запропоновано методику систематизації та представлення експертних знань про комплексні системи захисту інформації, яка забезпечує оцінювання захищеності інформаційних систем та забезпечення рівнів безпеки.

В роботі представлено принципи створення захищених мереж стільникового зв’язку, розглянуто заходи та засоби забезпечення якості передавання інформації. З метою забезпечення цілісної безпеки структури “система – канал зв’язку– система” розглянемо інформаційну модель захисту даних в технологіях голосової телефонії та передавання даних, зображено на рисунку 1.1. Модель створена на основі принципів системного аналізу – ієрархічності, багатоаспектності, цілісності і характеризує безпеку технологій

GSM, PSTN, VoIP, ADSL, Wi-Fi на рівні системи “об’єкт – загроза – захист”. На основі інформаційної моделі формується комплекс уніфікованих методів і засобів забезпечення безпеки даних в технологіях зв’язку відповідно до нормативного забезпечення.

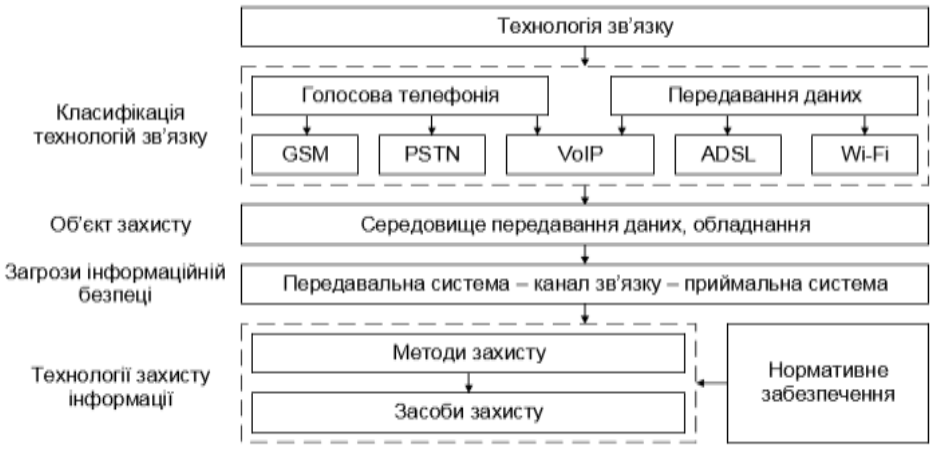

Рисунок 1.1 - Інформаційна модель захисту даних в технологіях зв'язку

Технологія GSM: характеристика системи “об’єкт – загроза – захист”. Технологія GSM (Global System for Mobile Communications) – глобальний цифровий стандарт для мобільного стільникового зв'язку з розділенням частотного каналу за принципом TDMA та середнім ступенем безпеки. Технологія GSM відноситься до мереж 2-го покоління (2G – цифровий стільниковий зв'язок), хоча з 2010 р. умовно знаходилась у фазі 2.75G завдяки численним розширенням. Технологія GSM функціонує в чотирьох частотних діапазонах: 850 МГц, 900 МГц, 1800 МГц, 1900 МГц. Загальна архітектура технології GSM представлена на рисунку 1.2 [11].

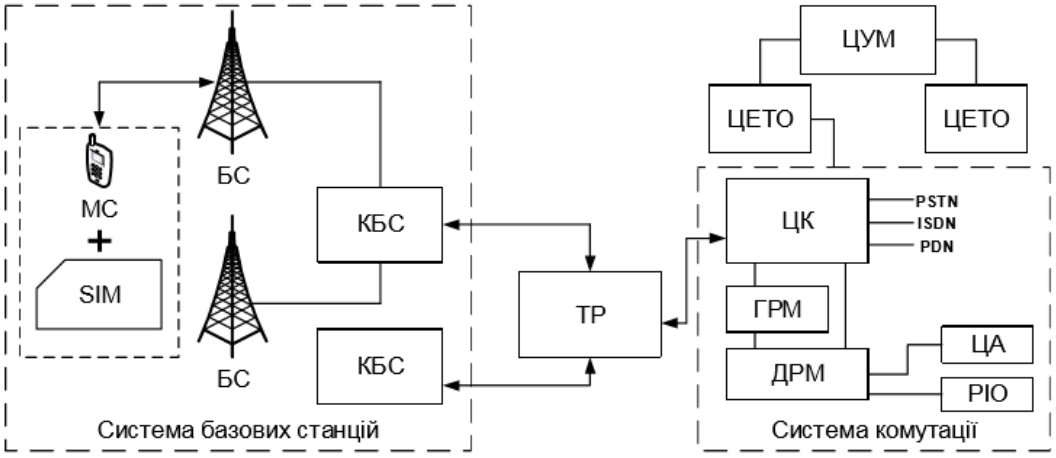

Рисунок 1.2 - Загальна архітектура технології GSM

Мобільна станція (МС) із мікропроцесорною картою SIM (Subscriber Identify Modul), в яку занесені унікальні дані для обміну інформацією між абонентами. Контролери базових станцій (КБС) – здійснюють керування базовими станціями (БС) і в подальшому формують з'єднання з центром комутації (ЦК), за допомогою якого можна створити канал передавання даних між двома абонентами. Транскодер (ТР), як проміжна ланка між БС та системою комутації, забезпечує перетворення вихідних сигналів каналу передавання мовного сигналу і даних (64 Кбіт/с) до виду, що відповідає рекомендаціям GSM по радіоінтерфейсу (13 Кбіт/с). В домашньому реєстрі місцезнаходження (ДРМ) зберігається інформація про місцезнаходження будь-якої МС, яка дозволяє центру комутації реалізувати виклик до цієї станції. Загалом ДРМ представляє базу даних (БД), в якій зберігається службова інформація про абонента. Гостьовий реєстр місцезнаходження (ГРМ) – це тимчасова БД абонентів, які знаходяться в зоні дії відповідного центру комутації. У кожного ЦК є лише один гостьовий реєстр місцезнаходження. В ГРМ зберігається та ж інформація

що і в ДРМ, але лише до того часу допоки МС знаходиться в зоні дії цього ГРМ. Центр автентифікації (ЦА) – це сервіс, за допомогою якого перевіряється право на доступ абонента до мережі, зокрема формуються ключі та алгоритми автентифікації. В ЦА зберігаються: унікальні номери абонента,

індивідуальний ключ, алгоритм автентифікації. Реєстр ідентифікації обладнання (РІО) – сервіс, в якому знаходиться централізована БД для підтвердження міжнародного ідентифікаційного номеру МС (IMEI). Центр експлуатації технічного обслуговування (ЦЕТО) – забезпечує контроль і керування іншими компонентами мережі та контроль якості її роботи. Центр управління мережею (ЦУМ) – дозволяє забезпечити раціональне ієрархічне управління мережею GSM та відповідає за експлуатацію і технічне обслуговування. В GSM використовується дві смуги частот: uplink (трансмісія вгору) 890 – 915 МГц, яка призначена для передавання даних від МС до БС; downlink (трансмісія вниз) 935 – 960 МГц відповідно для передавання інформації від БС до МС. Кожна із смуг дозволяє організувати по 124 симплексних канали із частотним рознесенням між каналами до 200 кГц. Враховуючи архітектуру, функціонування та особливості технології GSM розглянемо характеристику системи “об’єкт – загроза – захист” згідно інформаційної моделі, зображено на рисунку 1.3 та таблиці 1.2 [12]

Таблиця 1.2 - Технологія GSM та її характеристики

GSM	Характеристики системи "об'єкт-загроза-захист"	
Об’єкт: середовище передавання даних, обладнання	Ефір: − Мобільна станція − Базові (передавально-приймальні) станції − Провідне середовище, або ефір: − Контролер базових станцій − Транскодер − Центр автентифікації − Регістр ідентифікації обладнання − Центр управління мережею	
Загрози інформаційній безпеці	− Знищення або викривлення логічної структури даних − Несанкціоноване отримання інформації та її модифікація − Зашумлення каналу зв’язку	
Захист інформації: технології	Методи	− Шифрування даних в радіоканалі − Автентифікація повідомлень − Автентифікація користувача − Перепризначення TMSI − Ідентифікація обладнання

Продовженя таблиці 1.2

Захист інформації: технології	Засоби	– Скремблери – Криптофони – Інвертори спектру – SIM-карти – Шифратори – Ідентифікаційний номер рухомого терміналу (IMEI)

Рисунок 1.3 - Загальна архітектура технології VoIP

При передаванні даних в IP-мережах використовуються різні алгоритми стискання мовної інформації, наприклад стискання голосового потоку у 8 і більше разів, а деякі з них практично залишають сигнал на рівні імпульсно-кодової модуляції (64 кбіт/с). На основі інформаційної моделі, зображено на рисунку 1.4, розглянемо характеристику системи “об’єкт – загроза – захист” для технології VoIP, враховуючи її особливості відображено у таблиці 1.3.

Таблиця 1.3 - Технологія VoIP та її характеристики

VoIP	Характеристики системи "об'єкт-загроза-захист"

Об’єкт: середовище передавання даних, обладнання	Провідне середовище:
	– Мережеві пристрої
	  – Маршрутизатор
	  – VoIP шлюз
	– Пристрої клієнти
	  – VoIP телефон / ПК з VoIP програмним забезпеченням

Загрози інформаційній безпеці	– Відмова в обслуговуванні (DoS) – Крадіжка реєстраційних даних і маніпуляція ними – Атаки на систему автентифікації – Підміна (спуфінг) Caller ID – Атаки типу "man in the middle" – Атаки типу "Vlan hopping"

Продовження таблиці 1.3

Загрози інформаційній безпеці		− Спам через Інтернет-телефонію (SPIT) − VoIP фішинг (Vishing)
	Методи	− Ідентифікація/ авторизація користувачів − Перевірка обладнання на право доступу до мережі − Шифрування даних − Забезпечення цілісності − Контроль авторизованих абонентів − Окремий Інтернет-канал для VoIP
	Засоби	− Системи виявлення/ запобігання атак − Віртуальні приватні мережі − Брандмауер VoIP − Захищені мережеві протоколи − Міжмережеві екрани − Системи контролю цілісності

Технологія Wi-Fi: система “об’єкт – загроза – захист”, Технологія WI-FI (Wireless Fidelity) – технологія об'єднує декілька протоколів і ґрунтується на системі стандартів IEEE 802.11. На практиці широко використовується протокол IEEE 802.11n, який визначає принцип функціонування безпровідних мереж, зображено на рисунку 1.4.

Рисунок 1.4 - Загальна архітектура технології Wi-Fi

Функціонування технології Wi-Fi полягає у підключенні мобільного пристрою до точки доступу, роль якої може виконувати як окремий пристрій, так і мобільний, при правильному налаштуванні. Точка доступу розповсюджує

свій ідентифікатор (SSID) в ефір за допомогою спеціальних сигналів (“маячків”). На сьогодні в Україні функціонують стандарти: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n,; впроваджується IEEE 802.11ac. На основі інформаційної моделі, зображено на рисунку 1.4, розглянемо характеристику системи “об’єкт – загроза – захист” для технології Wi-Fi [13], враховуючи її особливості відображено у таблиці 1.4.

Таблиця 1.4 - Технологія Wi-Fi та її характеристики

<table>
<tr><th>Wi-Fi</th><th colspan="2">Характеристики системи "об'єкт-загроза-захист"</th></tr>
<tr><td>Об’єкт: середовище передавання даних, обладнання</td><td colspan="2">− Ефір:
− Базова станція
− Маршрутизатор / безпровідна точка доступу
− Клієнтські пристрої
− Мобільний пристрій з модулем Wi-Fi</td></tr>
<tr><td>Загрози у інформаційній безпеці</td><td colspan="2">− Відмова в обслуговування (DoS)
− Крадіжка реєстраційних даних і маніпуляція ними
− Атаки на систему автентифікації
− Спуфінг
− Атаки типу "man in the middle"
− Несанкціоноване отримання інформації та її модифікація.
− Відмова в обслуговування (DoS)
− Крадіжка реєстраційних даних і маніпуляція ними
− Атаки на систему автентифікації
− Спуфінг
− Атаки типу "man in the middle"
− Несанкціоноване отримання інформації та її модифікація.</td></tr>
<tr><td rowspan="2"></td><td>Методи</td><td>− Ідентифікація/авторизація користувачів
− Перевірка обладнання на право доступу до мережі
− Приховування ідентифікатора мережі
− Шифрування даних WPA
− Забезпечення цілісності
− Обмеження доступу до центрального вузла
− Контроль авторизованих абонентів</td></tr>
<tr><td>Засоби</td><td>− Брандмауери
− Базові системи автентифікації
− Протоколи шифрування
− Системи виявлення/запобігання атак
− Системи контролю цілісності</td></tr>
</table>

Технологія VoIP: система “об’єкт – загроза – захист”, Технологія VoIP (Voice over IP) – технологія передавання медіа-даних в режимі реального часу за допомогою системи протоколів TCP/IP. В технології VoIP аналоговий мовний сигнал від одного абонента дискретизується (кодується), здійснюється компресія та передавання цифровими каналами зв'язку до іншого абонента, де проводиться зворотна операція – декомпресія, декодування і відтворення аналогового сигналу. У випадку, якщо дзвінок надходить на іншу технологію, наприклад PSTN чи GSM, то сигнал проходить через IP-шлюз, який перетворює цифровий (VoIP) сигнал в аналоговий. Для передавання голосу через IPмережу відбувається процедура стискання сигналу спеціальною програмою-кодеком. Це здійснюється для збільшення швидкості передавання даних відповідно для підвищення якості зв'язку. Рівень безпеки передавання мовної інформації підвищує процедура шифрування даних. Зв'язок між двома VoIP-терміналами можливий лише за умови сумісних кодеків. З’єднання двох VoIP-терміналів між собою в мережі забезпечується підтримкою однакового протоколу комутації, наприклад SIP [14], зображено на рисунку 1.2.

Отже серед запропонованих інформаційних технологій захисту даних зв’язку на рівні системи “об’єкт – загроза – захист” для передавально-приймального тракту “система – канал зв’язку – система”, що є методологічною основою для застосування уніфікованих методів і засобів захисту інформації згідно діючих стандартів у сфері інформаційно-комунікаційних технологій найбільш вдалим і концетуально розширюваним э технологія Wi-Fi [15].

1.3 Аналіз засобів захисту абонента мобільного зв’язку

Додаток «SMS Анти спам online» покликаний швидко і ефективно блокувати небажані SMS. При цьому дистрибутив програми важить буквально кілобайти, а це значить, що рішення зовсім не навантажує систему. Розробник запевняє, що в Мережу відправляються тільки SHA-256-відбитки ваших SMS від відправників, яких немає у вашому списку контактів, тому конфіденційність зберігається на рівні.

Основні функції:

- чорний / білий список;
- блокування всіх відправників, яких немає в списку контактів;
- перегляд контактів;
- прийом SMS;
- Відправлення SMS-повідомлень.

Для роботи програми необхідно завантажити додаток з офіційного сайту розробника і зробити її програмою по замовчуванню для роботи з SMS. Тільки після цих дій можливо використовувати анти спам блокування.

Інтерфейс програми чотирьох-віконний. Доступні для роботи наступні вікна: SMS, Заборонити, Дозволити, Історія. Функціонал у програми обмежений, можливе часткове або повне блокування SMS. Блокування здійснюється за допомогою звірення абонента котрий надіслав повідомлення зі списком контактів у телефоні. У разі відсутності даних про відправника у існуючій контактній книзі – дане SMS повідомлення вважається спам повідомленням і блокується. Даний метод є діючим але малоефективним. Отримання нових SMS повідомлень від абонентів, котрих немає у базі даних - неможлива. Блокування небажаних телефонних дзвінків – неможливе. Доступний лише перегляд усіх SMS (додаються автоматично), перегляд чорного і білого списків, а також історія, де буде показано список нещодавно блокованих абонентів. Наявна також платна версія програми. За додаткову

плату можна призначити пароль, активувати резервне копіювання, відновлення і видаляти історію по витіканню двох тижнів [16].

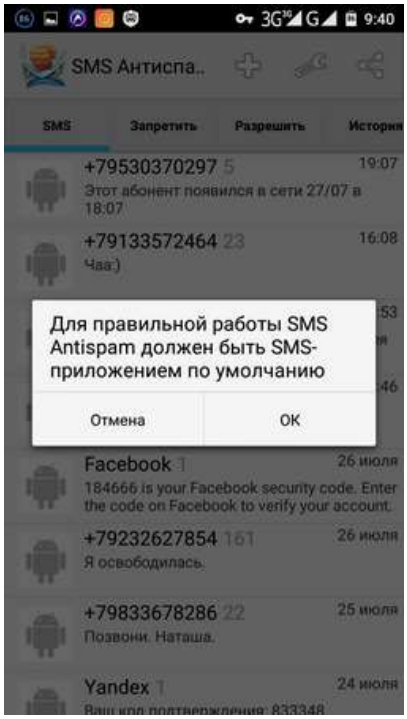

Рисунок 1.5 - Вікно програми

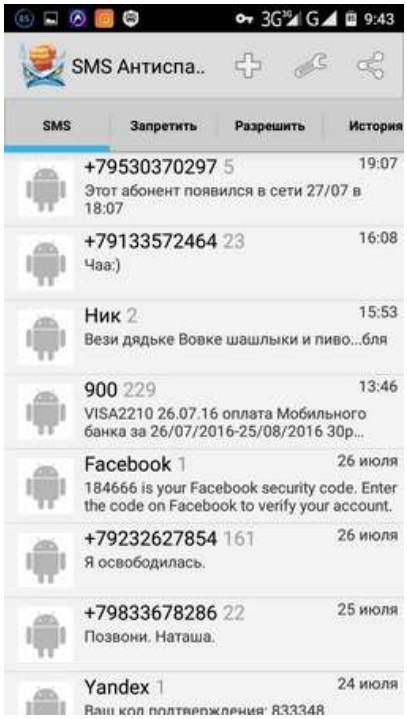

Рисунок 1.6 - Головне вікно програми

Програмний засіб працює коректно, мінусом є сам алгоритм блокування спам повідомлень, який може окрім спам повідомлень заблокувати звичайні повідомлення від абонентів, котрих немає у контактній книзі.

Додаток «Anti SMS Spam & Private Box» розроблений для активного блокування SMS повідомлень на усіх версіях Android. Дистрибутив програми маленький, це дозволяє їй працювати швидко і не перевантажувати мобільний пристрій, як зазначено в описі. Програма має можливість захисту паролем і можливість налаштування SMS-шаблонів.

Основні функції:

- чорний список ключових слів;
- блок невідомих відправників;

- відновлення в папку «Вхідні»;
- захист паролем;
- імпорт номера з журналу викликів, SMS і телефонної книги;
- перегляд контактів;
- зміна контактів;
- відправлення SMS-повідомлень;
- прийом SMS;
- перенаправлення вихідних дзвінків;
- здійснення телефонних викликів;
- перегляд журналу викликів;
- зміна журналу викликів.

При першому завантаженні і встановленні додатку виявлено програму шкідника це свідчить про те, що розробники програмного забезпечення невідповідально ставляться до захисту даних у мережі. Для користування програмою, необхідно прийняти угоду користувача.

Дана програма працює не тільки з наявною базою даних контактів, а й надає можливість блокувати повідомлення за ключовими словами і номером телефону, при цьому номер можна вбити вручну або додати з журналу дзвінків, SMS-повідомлень, телефонної книги або вбити перші цифри спам абонента.

Для коректної роботи програми її необхідно зробити програмою по замовчуванню для роботи з SMS, що є неможливим на пристроях з Android 4.4 або вище [17].

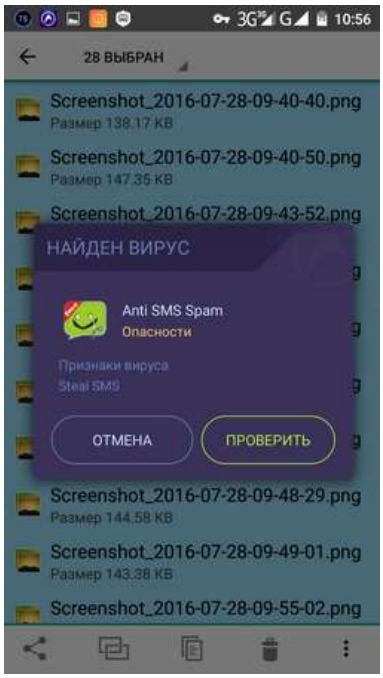

Рисунок 1.7 – Вікно програми

Програма працює коректно тільки на новій версії програмного забезпечення, хоча була розроблена для роботи на усіх пристроях. Окрім цього програма блокує усі повідомлення, що надходять з невідомих номерів, що може спричинити незручності у роботі. Виробник програмного забезпечення розповсюджує неякісне програмне забезпечення зі шкідливими програмами. Тому користуватися ним недоцільно.

Додаток «#1 SMS Blocker» Програмний засіб створений для швидкого блокування SMS-спама і небажаних повідомлень. Даний засіб працює за алгоритмом порівняння номера абонента, від якого надійшло повідомлення, з наявною базою даних контактів. У наявній версії програми перебачений додатковий функціонал.

Досить просте рішення, яке має більший функціонал аніж «SMS Анти спам online»

У платній версії програми можна налаштувати автоматичне видалення історії блокувань через день, тиждень або місяць, установку спеціального сигналу для підозрілого SMS, а також установку пароля на програму.

Основні функції:

- автоматичне блокування SMS-спаму;
- фільтр по номеру телефону, відправнику або фразі в повідомленні;
- заблоковані SMS переміщаються в окрему папку;
- експорт SMS в txt-формат;
- настроюваний автовідповідь;
- створення резервних копій та відновлення;
- захист паролем;
- прийом SMS;
- прийом MMS;
- відправлення SMS-повідомлень.

Програма працює коректно, але для повноцінної роботи необхідно завантажити платну версію. Мінусами є те, що програмний засіб блокує усі повідомлення, що надходять на мобільний пристрій від невідомих номерів, що є недосить правильно і зручно [18].

Порівняння оглянутих програмних засобів відображено у таблиці 5

Таблиця 5 - Порівняльна таблиця оглянутих програмних засобів для захиста абонента мобільного зв’язку.

Функціональність	**SMS Антиспам online**	**Anti SMS Spam & Private Box**	**#1 SMS Blocker**
Інтерфейс	декілька екранів	одновіконний інтерфейс	одно віконний
Можливість особистого налаштування	Так	Ні	Так
Ефективність анти спаму	Так	Ні	Так
Чорни і білий списки	Так	Так	Так
Реклама	Ні	Так	Так
QR сканування	Ні	Ні	Ні

1.4 Доцільність використання QR - кодування для захисту абонента мобільного зв’язку

Вже багато років по всьому світі успішно використовується технологія стиснення інформації та її збереження у невеликому матричному штрих-коді, що має вже загальновідому назву QR-код [19].

QR-код може містити в собі абсолютно різноманітну інформацію: цифри, літери, двійковий код та навіть ієрогліфи. Його можна використовувати в різноманітних сферах діяльності завдяки його універсальності.

QR-коди стали поширеними у використанні у 2010р. Зазвичай смартфон використовується як сканер QR-коду, відображаючи код і перетворюючи його в якусь корисну форму (наприклад, стандартну URL-адресу для веб-сайту, тим самим позбавляючи потреби користувача вводити його у веб-браузер). QR-код став центром рекламної стратегії, оскільки він забезпечує спосіб швидшого доступу до веб-сайту бренду, ніж через ручне введення URL-адреси [20].

Вони також можуть бути використані для зберігання особистої інформації для використання організаціями. Прикладом цього є Національне бюро розслідувань Філіппін (NBI), де дозволи NBI тепер поставляються із QR-кодом. Багато з цих програм орієнтовані на користувачів мобільних телефонів (за допомогою тегів на мобільних пристроях). Користувачі можуть отримати текст, додати контакт vCard на свій пристрій, відкрити URL-адресу або скласти електронне повідомлення або текстове повідомлення після сканування QR-кодів. Вони можуть генерувати та друкувати власні QR-коди для сканування та використання інших, відвідавши один із декількох сайтів чи додатків, що генерують QR-код [21].

Таким чином задача збереження конфіденційності кожної окремої фізичної особи може бути вирішена за допомогою ведення аналізу передачі ідентифікаційних даних між фізичними особами. Одним із способів вирішення цієї задачі є присвоєння унікального QR – коду кожному окремому абоненту мобільного зв’язку, врезультаті чого, з’являється можливість відслідкувати

факт передачі персональних даних, використовуючи двовимірний штрих-код. Саме за допомогою цього коду є можливість зберігати потрібну інформацію для аналізу часткової передачі персональних даних, зашифрувати усю необхідну інформацію та послатись на віддалений сервер, тим самим підвищивши захищеність абонента мобільного зв'язку.

1.5 Постановка задачі

Нехай, A – рольовий абонент мобільної мережі, дані якого необхідно захистити,

$X = \{x_1, x_2, x_z \dots, x_n\}$ – множина абонентів мобільного зв'язку, де x_z – z-й абонент мобільного зв'язку, у якого є доступ до персональних даних рольового абонента A, де $z = \overline{1,n}$, n – потужність абонентів мобільнго зв'язку.

$I = \{i_{1k}, i_{2k}, i_{jk}, \dots, i_{lr}\}$ – множина первинних абонентів мобільного зв'язку, де i_{jk} – j-й абонент мобільного зв'язку, де $j = \overline{1,\text{l}}$, у якого є повноваження додати k абонентів мобільного зв'язку, де $k = \overline{1,r}$,

$D = \{d_{1v}, d_{2v}, d_{ev} \dots, d_{mb}\}$ – множина вторинних абонентів мобільного зв'язку, де d_{ev} – e-й абонент мобільного зв'язку, де $e = \overline{1,m}$ у якого є повноваження додати v абонентів мобільного зв'язку, де $v = \overline{1,b}$,

$G = \{g_1, g_2, \dots, g_q\}$ – множина нових абонентів мобільної мережі, які піддаються аналізу, котрі отримали доступ до персональних даних абонента A, але не мають на це дозвіл.

Тоді, задачею захисту абонента мобільного зв'язку будемо вважати задачу забезпечення достатнього рівня захисту даних абоента мобільного зв'язку з урахуванням виявлених нових абоненітів G які не мають права на доступ до персональних даних рольового абонента A.

$$Y = F(X(I, D), G).$$

2 РОЗРОБКА МОДЕЛІ ЗАХИСТУ АБОНЕНТА МОБІЛЬНОГО ЗВ’ЯЗКУ

2.1 Розробка моделі захисту абонента мобільного зв’язку

З метою забезпечення захисту абонентів мобільного зв’язку розробимо сучасну модель захисту персональних даних базуючись на вже існуючу модель «Білих списків». Модель створена на основі принципів структурованої бази даних користувачів, доступом яких керує власник персональних даних і забезпечує повний контроль факту передачі власних персональних даних.

Головними принципами розроблюваної моделі захисту є:

- цілісність;
- конфіденційність;
- доступність.

Дані принципи необхідні для забезпечення захисту персональних даних у мобільних мережах, швидкою можливістю аналізу і коригування персональними даними.

Розроблювана модель представляє собою своєрідну модель дискреційного моделювання, тому що правом керувати доступом у ній реалізується як на основі матриці прав доступ до ролей, так і за допомогою правил, рольового абонента мобільної мережі. У даній моделі класичне поняття суб'єкта замінюється поняттями користувача та ролі. На рисунку 2.1 зображена загальна модель захисту абонентів мобільного зв’язку.

Для забезпечення захисту персональними даними кожному новому абоненту мобільного зв’язку присвоюється певна роль.

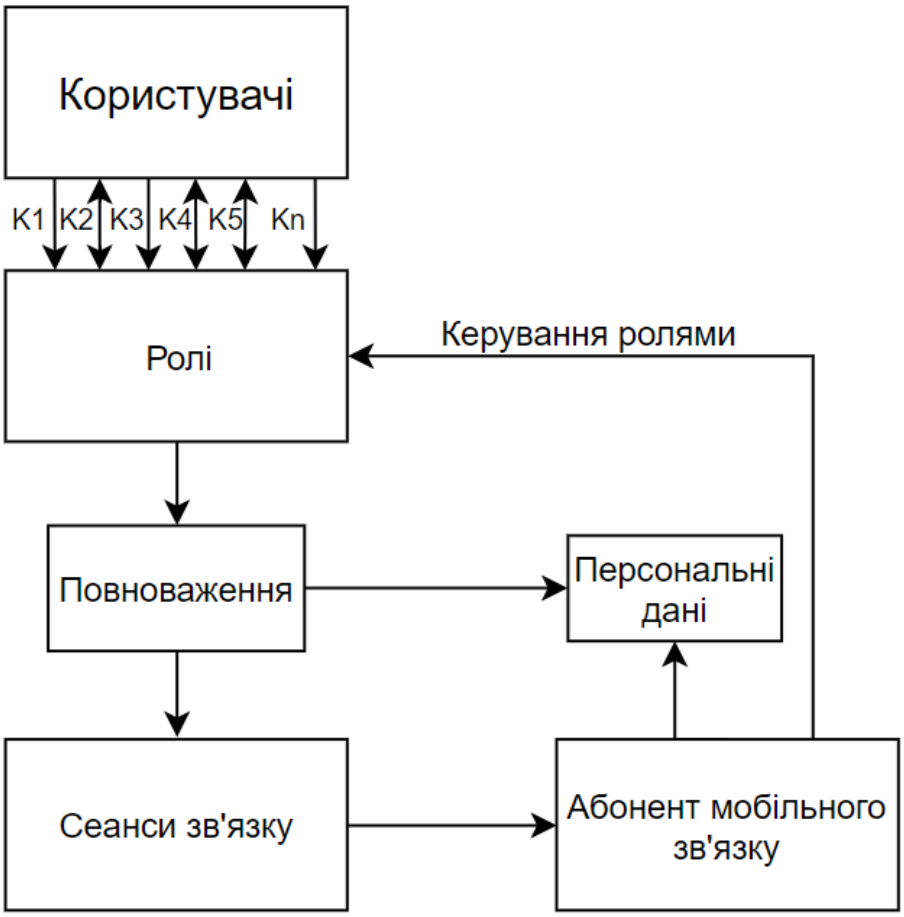

Рисунок 2.1 - Загальна модель захисту абонентів мобільного зв’язку.

Роль - це активно діюча в системі абстрактна сутність, з якою пов'язаний обмежений, логічно зв'язаний набір повноважень, необхідних для здійснення певної діяльності. Абоненти мобільної мережі, що використовують систему, діють не від свого власного імені, замість цього використовується абстрактне поняття роль, яка аж ніяк не пов'язана з їх особистістю.

Ролі бувають трьох типів: Первинні $I = \{i_{1k}, i_{2k}, i_{jk}, \dots, i_{lk}\}$ – множина первинних абонентів мобільного зв’язку, Вторинні $D = \{d_{1v}, d_{2v}, d_{ev} \dots, d_{mb}\}$ – множина вторинних абонентів мобільного зв’язку, Нові $G = \{g_1, g_2, \dots, g_q\}$ – множина нових абонентів мобільного зв’язку. На рисунку 2.2 зображено ролі абонентів мобільного зв’язку.

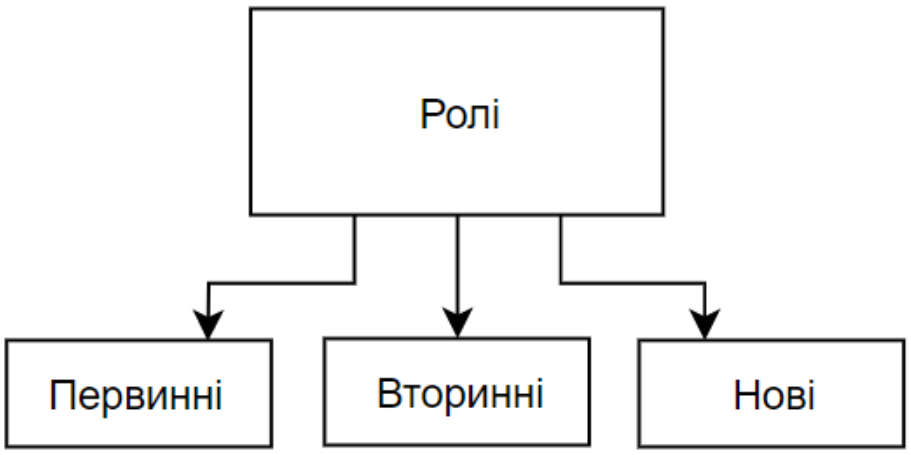

Рисунок 2.2 - Ролі абонентів мобільного зв’язку

Відповідно до своєї ролі кожний абонент отримує повноваження на доступ до персональних даних. Дані повноваження повністю розроблюються і контролюються рольовим абонентом мобільного зв’язку. Для j-го первинного абонента i_{jl} існує коефіцієнт l – кількість абонентів, яким він може передати доступ до даних рольового абонента A, для e-го вторинного абонента d_{ev} існує коефіцієнт v – кількість абонентів, яким він може передати доступ до даних рольового абонента A, аналізуючи потреби рольовий абонент надає повноваження кожному абоненту і у кожен момент часу може змінити дані повноваження. Контролюючи доступ до персональних даних. На рисунку 2.3 зображено можливі повноваження абонентів мобільного зв’язку.

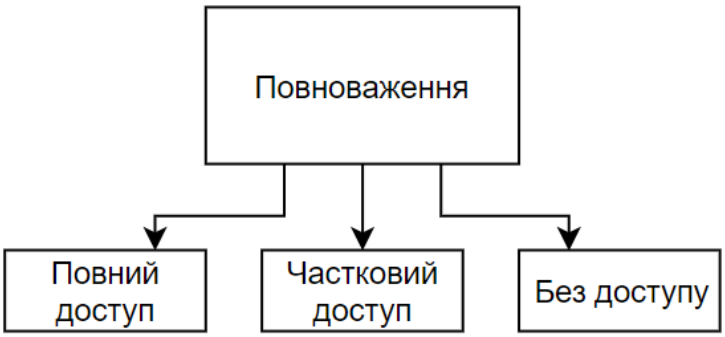

Рисунок 2.3 - Повноваження абонентів мобільного зв’язку

Доцільно забезпечити можливість керування доступом і призначення повноваженн не реальним користувачам, а абстрактним ролям, які представляють учасників певного процесу обробки інформації. Такий підхід до захисту абонентів мобільного зв’язку дозволяє врахувати розподіл обов'язків і повноважень між учасниками прикладного інформаційного процесу, оскільки з точки зору розроблювальної моделі, має значення не особистість користувача, що здійснює доступ до інформації, а те, які повноваження йому необхідні для виконання цих дій.

Відповідно до повноважень користувачів вони можуть отримувати доступ до персональних даних, повний, частковий, або ж взагалі не мати доступу. Ці повноваження повністю контролює рольовий абонент. Таким чином, отримуючи доступ до персональних даних користувачі системи, можуть створювати сеанси зв’язку.

Таким чином, задачею захисту абонента мобільної мережі є знаходження нових абонентів мобільної мережі G, у яких не було права отримувати доступ до персональниз даних рольового абонента A і забтрати доступ у цих абонентів до персональниз даних рольового абонента.

2.2 Висновок

У даному розділі розроблено модель захисту абонентів мобільного зв’язку з урахуванням виявлених нових абоненітів G, які не мають права на доступ до персональних даних рольового абонента A.

3 УДОСКОНАЛЕННЯ МЕТОДУ ЗАХИСТУ АБОНЕНТІВ МОБІЛЬНОГО ЗВ’ЯЗКУ

3.1 Узагальнений алгоритм захисту абонентів мобільного зв’язку

Захист абонентів мобільного зв’язку відбувається із залученям серверів мобільного операртора. Сформований вихідний виклик шифрується на телефоні вихідного абонента мобільної мережі і передається на найближчу мобільну вишку оператора мобільної мережі у радіусі дії. У той саме час сигнал відправляється на сервери мобільного оператора, де опрацьовуються процеси виклику, ведеться аналіз і контроль передачі вихідного виклику між супутниками і мобільними вишками мобільного оператора. Після отримання інформації супутником мобільного оператора відбувається пошук найближчої із необхідних телефоних вишок, куди перенаправляється вихідний виклик. Останнім кроком для здійснення виклику є переадресація цифрового сигналу на телефон вхідного абонента мобільного зв’язку, де відбувається дешифрування вхідного дзвінка і оцифрування голосового сигналу із цифрового потоку інформації.

Під час такого методу з’єднання, персональні дані захищаються мобільним оператором вхідного і вихідного абонентів мобільного зв’язку . Для цього використовуються різні методи шифування інформації і збереження даних про виклики на серверах мобільного оператора. Такий метод є не цілком захищеним, адже використовуючи різні спеціальні прилади можливий перехват сигналу і дешифрування його злочинцями.

Персональні дані можуть бути передані під час передачі даних між мобільною вишкою і телефоном вхідного абонента, цей етап є уразливішим і потребує доопрацювання.

З метою удосконалення даного методу запропоновано використовувати QR-кодування для можливості аналізу передачі персональних даних і

моніторингу факту передавання прав доступу до них факту передання прав доступу до персональних даних.

На рисунку 3.1 зображено узагальнений алгоритм захисту абонентів мобільного зв’язку.

Рисунок 3.1 - Загальний алгоритм захисту абонентів мобільного зв’язку

3.2 Розробка алгоритму генерації унікальних QR-кодів

З урахуванням запропонованих удосконалень, алгоритм захисту абонентів мобільного зв'язку включатиме додаткові етапи. Розглянемо кожний етап окремо.

На першому етапі абонент мобільного зв'язку повинен додати новий контакт до існуючого списку своїх контактів. У розроблюваній інформаційній технології для цього використовується технологія QR-кодування.

Абонент мобільного зв'язку використовує для цього унікальний, згенерований QR-код. Алгоритм генерації QR-кодів зображено на риску 3.2

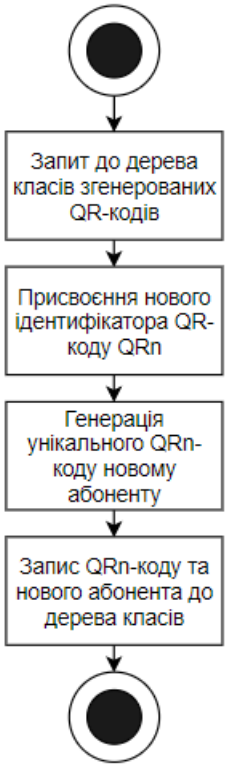

Рисунок 3.2 – UML-діаграма генерації унікальних QR-кодів

Після сканування QR-коду власника персональних даних, мобільний пристрій нового абонента мобільного зв'язку генерує запит, який обробляється у хмарі. Спочатку виконується запит до дерева класів згенерованих QR-кодів,

після обробки усієї інформації, новому абоненту мобільного зв’язку присвоюється унікальний ідентифікатор QRn, після чого даний унікальний ідентифікатор записується до журналу ідентифікаторів для правильності побудови структури. Після чого новий абонент мобільного зв’язку отримує доступ до персональних даних власника абонентського номера, та можливість до відправлення повідомлень та дзвінків. Окрім цього, у разі потреби передачі цих даних іншому абоненту мобільного зв’язку, він має змогу згенерувати свій унікальний QRn-код власника персональних даних, у якому збережена інформація про актуальний статус доступу та його унікальний ідентифікатор QRn.

Алгоритм присвоєння унікальних даних представлено на рисунку 3.3

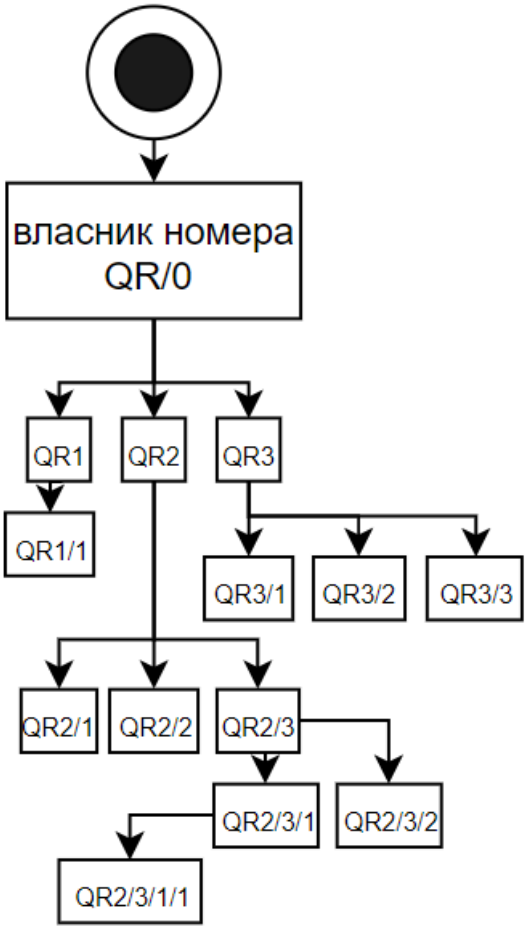

Рисунок 3.3 - UML діаграма присвоєння унікальних QR-кодів

Абонент мобільної мережі, власник персональних даних по замовчуванню має унікальний номер QR-коду – 0. Переходячи на кожен нижчій рівень дерева класів до його коду додається унікальний ідентифікатор. Дані ідентифікатори присвоюються з певною закономірністю.

Для n-го абонента, котрий просканував QR-код власника персональних даних ідентифікатор додається за наступною формулою

$$n = QRn.$$

Для n-го абонента, котрий просканував QR-код у абонента мобільного зв'язку, якому надано доступ до персональних даних ідентифікатор додається за наступною формулою:

$$n = QRn/+n.$$

Таким чином, будується структуроване дерево абонентів мобільного зв'язку у якому у кожного абонента є унікальний ідентифікатор.

Використовуючи дані ідентифікатори, абонент власник персональних даних може відслідкувати факт передачі персональних даних і вносити зміни у дану структуру, якщо є така необхідність.

3.3 Розробка алгоритму аналізу і коригування доступу абонентів мобільного зв'язку

Одним із розроблюваних методів є метод аналізу і коригування доступу абонентів до персональних даних. За допомогою даного методу абонент власник персональних даних має змогу вносити особисті корективи, до доступу абонентів мобільної мережі, відслідковувати факт передачі персональних даних та отримувати оперативні, зведені дані про актуальний стан доступу до персональних даних.

Даний метод працює за таким алгоритмом:

Якщо абонент мобільної мережі вирішив забрати доступ до персональних даних якогось окремого абонента мобільної мережі, йому необхідно використовуючи інтерфейс інформаційної технології видалити даного абонента із списку контактів. Після чого створюється вхідний запит на сервер обробітку інформації, де відбуваються коригування у структурі даних використовуючи метод аналізу і коригування доступу абонентів мобільної мережі. Роботу даного метода зображено на рисунку 3.4 .

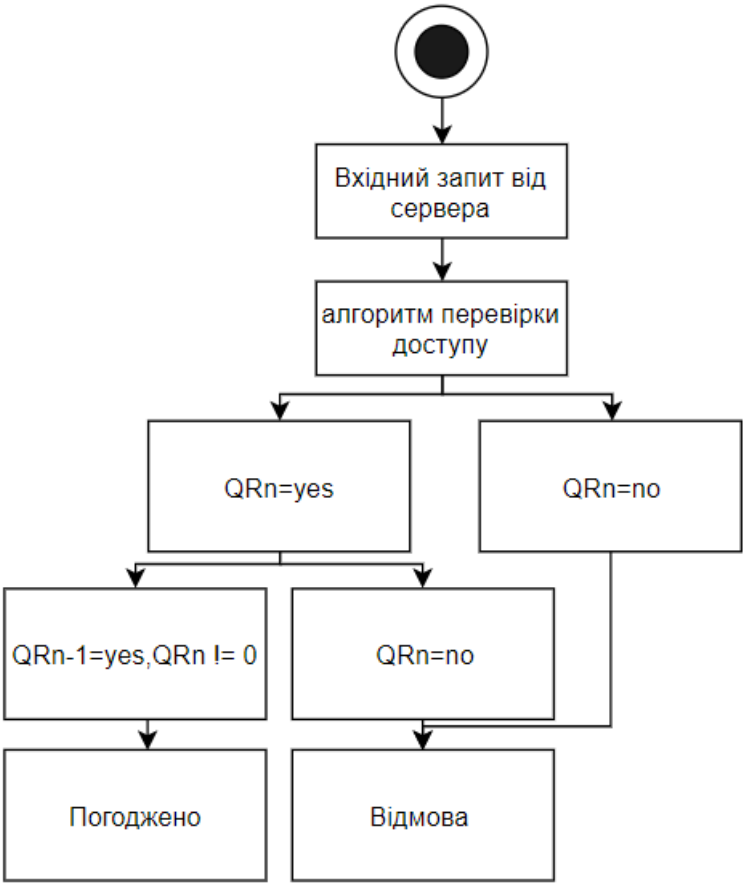

Рисунок 3.4 – UML-діаграма перевірки абонентів мобільного зв’язку на доступ до персональних даних

З алгоритму перевірки абонентів мобільного зв’язку видно, що після коригування абонентом власником доступу до персональних даних, створюється вхідний запит, який направляється до алгоритму перевірки доступу. Під час перевірки значення доступу кожного окремо взятого абонента може бути або *yes,* або *no,* відповідно до чого йде первірка гілки дерева структури даних, до якої належав абонент мобільної мережі, якому забрали доступ до персональних даних. У випадку , якщо абонент мобільного зв’язку надавав доступ до персональних даних власника, іншим абонентам, то виконується перевірка кожного, наступного абонента. Таким чином перевіряються унікальні ідентифікатор абонентів мобільного зв’язку *QRn,* якщо

$$QRn = yes.$$

Виконується перевірка на доступ минулого абонента. У цей час абонент власник персональних даних отримує сповіщеня про підтвердження актуального доступу кожного абонента. Дана перевірка триває до тих пір, поки

$$QRn\ -1\ yes,\ QRn!=0.$$

Поки *QRn-1* не буде відповідати унікальному ідентифікатору абонента власника персональних даних. Роботу даного методу можна побачити на прикладі структурованих абонентів мобільного зв’язку на рисунку 3.5.

Загальну структуру методу перевірки абонента мобільного зв’язку можна подати, як показано на рисунку 3.6.

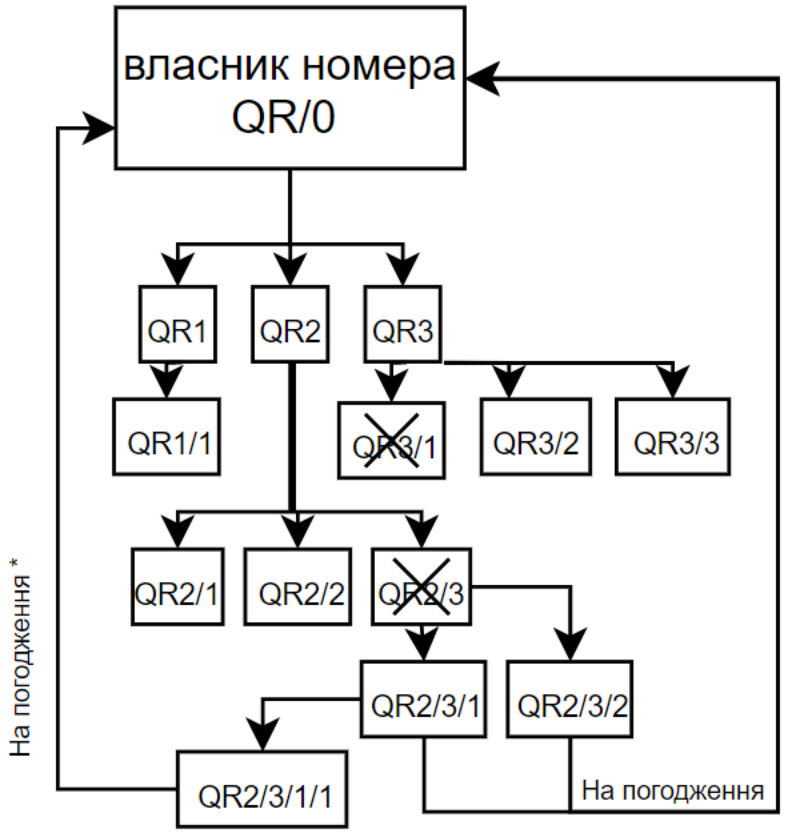

Рисунок 3.5 - Метод перевірки абонентів мобільного зв’язку

На даній загальній структурній схемі можна побачити метод аналізу коригування доступу абонентів мобільного зв’язку.

Дані із сервера направляються на хмарний сервер, де йде обробка інформації. У хмарі виконуються наступні дії:

– алгоритм обробки вхідних запитів оброблює отриману інформацію і записує отримані дані у базу даних;

– отримані дані необхідні для аналізу доступу абонентів мобільного зв’язку до персональних даних рольового абонента рольовий абонент вносить коригування у доступ до своїх конфіденційних даних, забираючи право доступу до персональних даних іншим абонентам мобільного зв’язку.

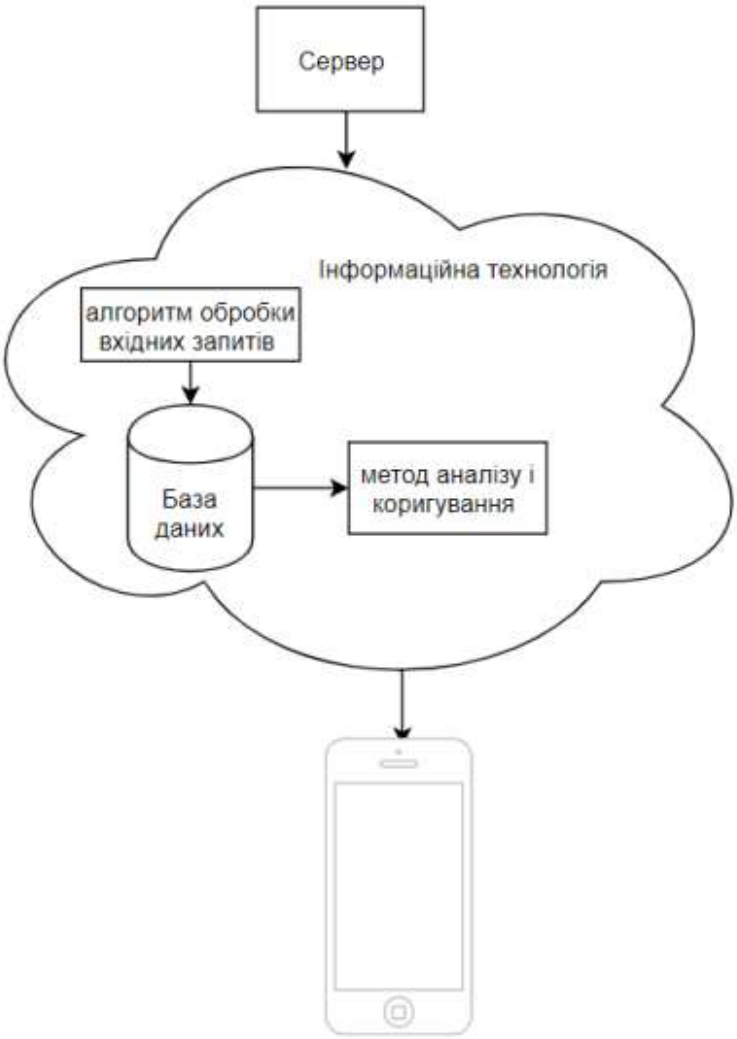

Рисунок 3.6 - Загальна структура методу аналізу коригування доступу абонентів мобільного зв’язку

3.4 Висновок

Отже, удосконалено метод захисту абонентів мобільного зв’язку з використанням QR-кодування, що дозволяє покращити аналіз доступу до персональних даних абонента мобільного зв’язку, вносити корективи у структури даних, тим самим забезпечуючи захист передачі власних персональних даних.

4 РОЗРОБКА ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ЗАХИСТУ АБОНЕНТА МОБІЛЬНОГО ЗВ’ЯЗКУ

4.1 Розробка структури інформаційної технології захисту абонентів мобільного зв’язку

Задача забезпечення захисту кожного окремого абонента мобільного зв’язку може бути вирішена за допомогою ведення аналізу передачі ідентифікаційних даних між фізичними особами. Такий аналіз дає можливість побудувати дерево відношень (зв’язний граф), де першим вузлом буде абонент мобільного зв’язку – власник персональних даних, а усі інші вузли у графі - абонентами, котрі отримали персональну інформацію від власника, чи інших фізичних осіб, котрі мають доступ до цієї інформації. Таким чином, з’являється можливість відслідкувати факт передачі персональних даних.

Запропоновано використовувати двовимірний штрих-код, а саме QR-код, присвоєний кожному окремому номеру. Саме за допомогою цього коду є можливість зберігати потрібну інформацію для аналізу часткової передачі персональних даних, зашифрувати усю необхідну інформацію та послатись на віддалений сервер, тим самим підвищивши захищеність даного методу. Запропонований аналіз базується на теорії графів. Мережу можна уявити як геометричну конфігурацію, яка складається з точок (фізичних і юридичних осіб, котрі мають доступ до персональних даних), сполучених лініями (факт передачі частини персональних даних та зв’язок між абонентами). Таким чином можна відслідковувати, аналізувати та керувати доступом до інформації абонентів, котрі мають доступ до персональної інформації. Використання означеної QR-технології сприяє підвищенню ефективності та швидкодії аналізу зв’язків між абонентами мобільної мережі. На рисунку 3.1 зображено загальний алгоритм інформаційної технології захисту абонентів мобільного зв’язку. Усю технологію можна розділити на 3 основні етапи:

− додання нового абонента та його запис до дерева класів усіх абонентів;

− генерація унікальних QR кодів для кожного нового абонента та структуризація усіх даних;

− перевірка алгоритмом відповідності при вхідному виклику чи повідомленні.

Розглянемо дані етапи та розробимо більш детальну структуру методу захисту абонентів мобільного зв’язку. Додавання нового абонента здійснюється за допомогою сканування унікального QR-коду, після чого створюється запит до хмарного серверу, де аналізуються дані та створюється унікальний ідентифікатор для нового абонента мобільного зв’язку. Тоді дані про нового абонента записуються до дерева класів. Після чого новий абонент мобільного зв’язку отримує власний унікальний ідентифікатор у вигляді QR-коду, яким може поділитися з іншими абонентами мобільного зв’язку.

Отже, остаточна структура методу буде складатись з таких етапів:

− створення інформації про нового абонента мобільної мережі;

− генерація QR-коду для передачі персональних даних нового абонента;

− запит (сканування) створеного коду іншим абонентом мобільної мережі або додатком для роботи з QR-кодом;

− формування створеного запиту іншого абоненту мобільної мережі або додатку до серверу;

− аналіз отриманих даних про нового абонента сервером;

− збереження отриманих даних про нового абонента на сервері та додавання нового абонента в дереві класів для подальшого аналізу та корегування даних власником персональних даних;

− відповідь від сервера іншим абонентам мобільної мережі або додаткам, які зробили запит на отримання персональних даних власника.

Генерація QR-коду абонента мобільної мережі, котрий має доступ до персональних даних, у разі подальшої передачі даних іншим абонентам.

Інформаційна технологія захисту абонентів мобільного зв’язку - це складна система, яка включатиме у себе чотири типи користувачів, щоб

задовільно використовувати усі можливості та функції захисту персональних даних абонентів мобільного зв’язку.

– рольовий абонент мобільного зв’язку;
– первинний тип абонентів;
– вторинний тип абонентів;
– новий тип абонентів.

Кожна група користувачів інформаційної технології має свої права та можливості у комунікації, та обміном персональних даних, відповідно до своєї ролі і повноважень, тобто кожен має різний рівень доступу до системи.

Зрозуміло, що звичайні абоненти мобільного зв’язку не можуть керувати доступом до персональних даних рольового абонента мобільного зв’язк, це недоцільно, тому було розроблено спеціальні міри для запобіганню таких ситуацій.

Рольовий абонент мобільного зв’язку

– присвоювати ролі;
– присвоювати повноваження;
– надавати доступ;
– створювати сеанси зв’язку;
– коригувати персональні дані.

Первині абоненти мобільного зв’язку;

– надавати доступ вторинним абонентам;
– створювати сеанси зв’язку з рольовим абонентом.

Вторинні абоненти мобільного зв’язку

– надавати доступ новим абонентам;
– створювати сеанси зв’язку з рольовим абонентом.

Нові абоненти мобільного зв’язку

– надсилати запит на доступ.

Первинний і вторинний абонент мобільного зв’язку відрізняються тим, що первинним абонентам надав доступ до персональних даних саме рольовий абонент і він їм цілком довіряє.

Загальна структура інформаційної технології захисту абонентів мобільного зв’язкузображена на рисунку 4.1

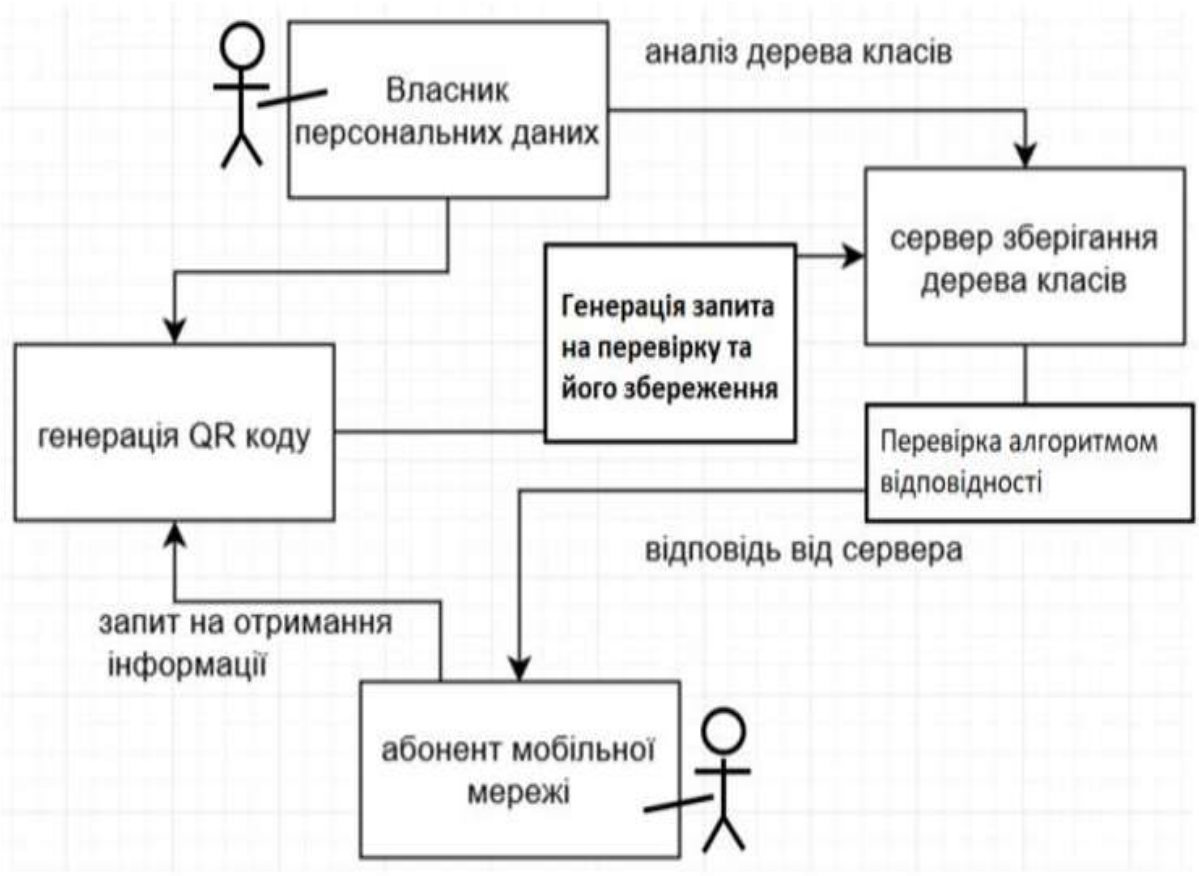

Рисунок 4.1 – Загальна структура інформаційної технології захисту абонентів мобільного зв’язку

Діаграма прецедентів інформаційної технології захисту абонентів мобільного зв’язку зображена на рисунку 4.2.

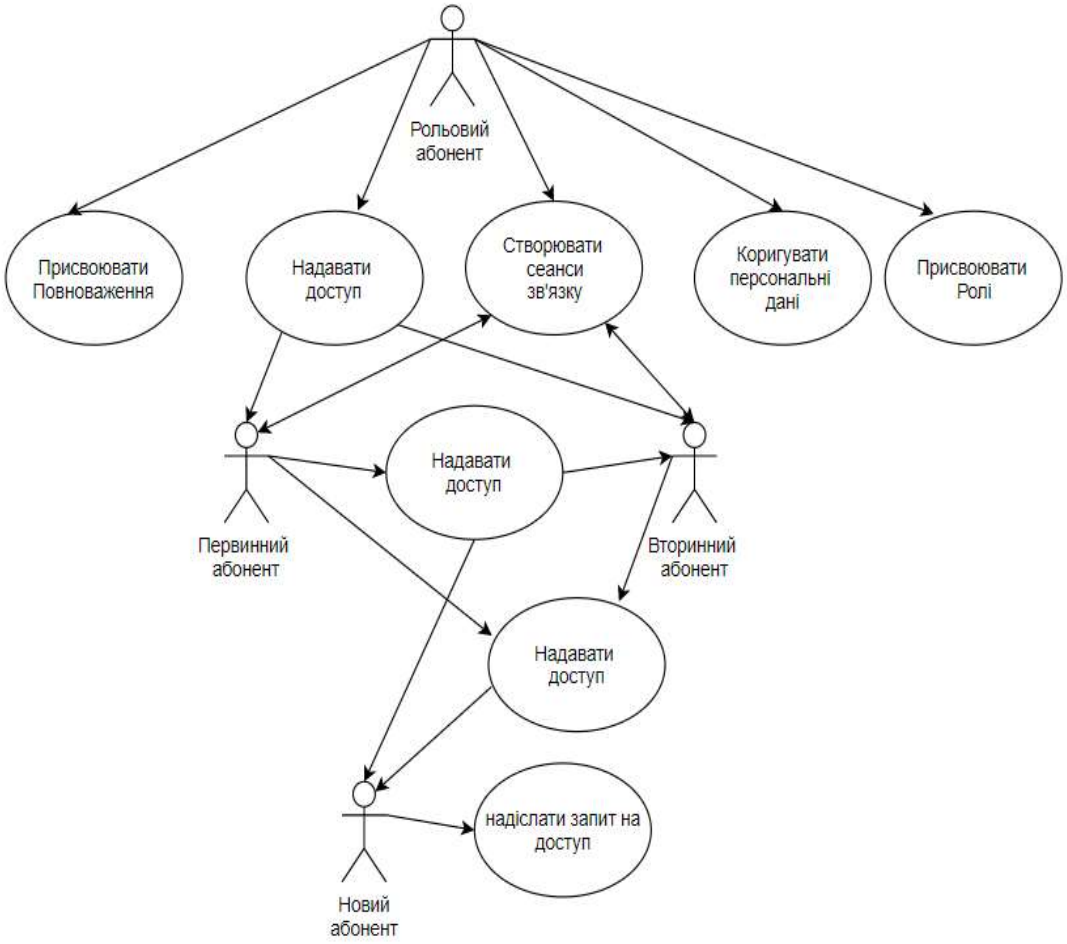

Рисунок 4.2 - UML-діаграма прецедентів інформаційної технології захисту абонентів мобільного зв’язку

Для повної взаємодії та функціонування інформаційної технології захисту абонентів мобільного зв’язку мають бути присутні всі вузли системи:

- вузол інтерфейсу користувачів;
- вузол бази даних;
- вузол надання доступу;
- вузол аналізу ролей і повноважень;
- вузол створення сеансу зв’язку.

Розроблена загальна структурна схема взаємодії вузлів інформаційної технології захисту абонентів мобільного зв’язку завдань зображена на рисунку 4.3

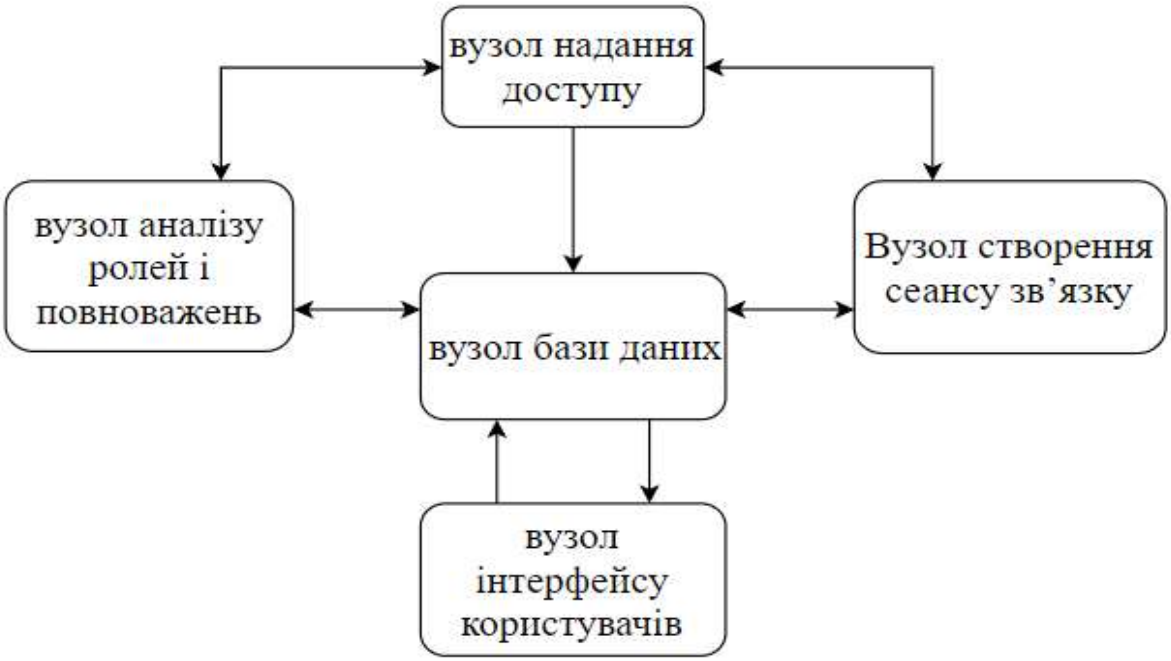

Рисунок 4.3 – Схема взаємодії вузлів інформаційної технології захисту абонентів мобільного зв'язку

Отже, взаємодія вузлів інформаційної технології забезпечує виконання задачі захисту абонентів мобільного зв'язку у повному обсязі.

4.2 Вибір середовища програмування та мови програмування

У даному розділ виконано порівняння перспективних мов програмування, таких як: C++, C#, PHP та Java для успішної реалізації інформаційної технології захисту абонентів мобільного зв'язку.

C# працює з використанням .NET Framework, яка надає можливість працювати з великою кількістю бібліотек, що містять класи, які використовуються для виконання загальних завдань, таких як робота з масивами, відображення вікон або редагування файлів. На відміну від інших мов програмування немає необхідності у виборі декількох бібліотек для реалізації невеликого завдання [21].

C# є об’єктно-орієнтованою мовою програмування та підтримує деякі функції, які зазвичай зустрічаються у функціональних мовах, такі як делегати та анонімні класи.

C# найкращий вибір для прикладних програм під управлінням операційної системи Windows. При використані .NET Core, C# є універсальною мовою, яка надає можливість запускатися додатку на будь-якій операційній системі.

C# – об'єктно-орієнтована мова програмування з безпечною системою типізації для платформи .NET. Розроблена Андерсом Гейлсбергом, Скотом Вілтамутом та Пітером Гольде під егідою Microsoft Research (при фірмі Microsoft).

Синтаксис C# близький до C++ і Java. Мова має строгу статичну типізацію, підтримує поліморфізм, перевантаження операторів, вказівники на функції-члени класів, атрибути, події, властивості, винятки, коментарі у форматі XML. Перейнявши багато що від своїх попередників — мов C++, Delphi, Модула і Smalltalk – C#, спираючись на практику їхнього використання, виключає деякі моделі, що зарекомендували себе як проблематичні при розробці програмних систем, наприклад множинне спадкування класів (на відміну від C++).

C# розроблялась як мова програмування прикладного рівня для CLR і тому вона залежить, перш за все, від можливостей самої CLR. Це стосується, перш за все, системи типів C# [22-23]. Присутність або відсутність тих або інших виразних особливостей мови диктується тим, чи може конкретна мовна особливість бути трансльована у відповідні конструкції CLR. Так, з розвитком CLR від версії 1.1 до 2.0 значно збагатився і сам C#. CLR надає C#, як і всім іншим .NET-орієнтованим мовам, багато можливостей, яких позбавлені «класичні» мови програмування. Наприклад, збірка сміття не реалізована в самому C#, а проводиться CLR для програм, написаних на C# точно так, як і це робиться для програм на VB.NET, J# тощо.

Переваги мови C# у порівнянні з C++:

- класи можуть бути визначені всередині класів;
- можливості відображення;
- не потрібно турбуватися про заголовні файли “.h”;
- визначення класів і функцій можуть бути зроблені в будь-якому порядку;
- автоматичний збір сміття;
- немає глобальних функцій або змінних, все належить до класу;
- всі змінні ініціалізуються значеннями за замовчуванням, перш ніж використовувати (це автоматично, за замовчуванням, але може бути зроблено вручну, використовуючи статичні конструктори);
- не можна використовувати не логічні змінні, як умови;
- більш чисте управління подіями (за допомогою делегатів);

Переваги C# в порівнянні з Java:

- має більш примітивні типи (типи значень).

Порівняння мов C++, Java і C# зображено в таблиці 4.1.

Враховуючи всі переваги і недоліки, була вибрана мова C#.

Таблиця 4.1 – Порівняння мов програмування C++, Java і C#

Ознака порівняння	C++	Java	C#
ООП мова	Так	Так	Так
Наявність контейнерів	Ні	Так	Так
Перевантаження операторів	Так	Ні	Так
Автоматичний збір сміття	Ні	Так	Так
Висока продуктивність коду	Так	Ні	Ні
Зручність налагодження	Ні	Так	Так
Безкоштовне використання	Так	Так	Ні

Для реалізації інтерфейсної частини порівнюються такі фреймворки та бібліотеки, як React, Vue та Angular.

React — відкрита JavaScript бібліотека для створення інтерфейсів користувача, яка покликана вирішувати проблеми часткового оновлення вмісту веб-сторінки, з якими стикаються в розробці односторінкових застосунків. React дозволяє розробникам створювати великі веб-застосунки, які використовують дані, котрі змінюються з часом, без перезавантаження сторінки. Його мета полягає в тому, щоб бути швидким, простим, масштабованим. React обробляє тільки користувацький інтерфейс у застосунках [24].

Vue.js — JavaScript-фреймворк що використовує шаблон MVVM для створення інтерфейсів користувача на основі моделей даних, через реактивне зв'язування даних. Vue використовує синтаксис шаблонів на основі HTML, що дозволяє декларативно зв'язувати рендеринг DOM з основними екземплярами даних в Vue. Всі Vue шаблони валідні HTML, і можуть бути розпарсені браузерами та HTML парсерами. Всередині Vue компілює шаблони в рендерингові функції віртуального DOM. В поєднанні з реактивною системою, Vue здатний розумно обчислити кількість компонентів для ре-рендингу та застосувати мінімальну кількість маніпуляцій з DOM, коли стан застосунку зміниться.

AngularJS — JavaScript-фреймворк з відкритим програмним кодом, який розробляє Google. Призначений для розробки односторінкових додатків, що складаються з одної HTML сторінки з CSS і JavaScript. Його мета — розширення браузерних застосунків на основі шаблону Модель-вид-контролер (MVC), а також спрощення їх тестування та розробки. Фреймворк працює зі сторінкою HTML [25], що містить додаткові атрибути і пов'язує області вводу або виводу сторінки з моделлю, яка є звичайними змінними JavaScript. Значення цих змінних задаються вручну або отримуються зі статичних або динамічних JSON-даних.

Порівняння фреймворків Angular, Vue та бібліотеки React зображено в Таблиці 4.2.

Таблиця 4.2 – Порівняння фреймворків Vue, Angular і біоліотеки React.

Ознака порівняння	Vue	Angular	React
Рендеринг	Так	Так	Так
Наявність архітектури компонентів	Так	Так	Ні
Зворотня сумістність	Ні	Ні	Так
Висока продуктивність коду	Так	Так	Так
Зручність налагодження	Так	Ні	Так
Легковагі	Так	НІ	Так

Проаналізувавши мови програмування та фреймворки було обрано технологію ASP NET C# для реалізації програмної частини і бібліотеку React для реалізації інтерфейсу користувача.

4.3 Реалізація складових інформаційної технології захисту абонентів мобільного

Для реалізації інформаційної технології захисту абонентів мобільного зв’язку були реалізовані такі складові, як інтерфейс користувача, сервіс надання ролей, повноважень, створення сеансів зв’язку та аналіз алгоритмом відповідності.

У магістерській кваліфікаційній дипломній роботі виконується реалізація інформаційної технології захисту абонентів мобільного зв’язку у середовищі Visual Studio з використанням мови розробки – C# та бібліотеки для інтерфейсу користувача React. Для роботи основного компонента реалізовано групу класів, які знаходяться в бібліотеці NotificationBot.Core.

Основі класи та методи інформаійної технології захисту абонентів мобільного зв’язку QR-Generation, NewContactAdd, MessageCheck, Tokens, Users, TimeOfAnalis.

Представлення класів та методів буде представлано нижче з їх коротким описом.

QR-Generation – клас, якиий дозволяє використовувати технологію QR-кодування для генерації унікальних QR-кодів для кожного нового абонента мобільного зв’язку, у якому зберігається уся персональна інформація, а також дозволяє сканувати сканувати QR-код під час обміну інформацією.

NewContactAdd – клас, який дозволяє додавати нового абонента до структури даних та записувати дані у базу даних.

AccessTokens – клас, який відповідає за присвоєння повноважень і контролює передачі даних між двома користувачами.

TokensGroup – клас, який призначений для присвоєння первинних і вторинних ролей абонентів.

Users – клас, який дозволяє створювати нового користувача у даній системі захисту абонентів мобільного зв’язку, відображає і зберігає персональні дані абонентів мобільної мережі.

TimeOfCall – клас, у якому реалізовано точний час, коли було створено сеанс зв’язку з рольовим абонентом.

public private<Bitmap> GetStrings(Bitmap text) – метод для виділення вхідних дзвінків.

public private List<Bitmap> GetStringNotification (Bitmap str) – метод вхідного дзвінка.

public private List <Bitmap> GetNotJs(Bitmap text) – метод передаваня персональних даних.

public private Bitmap TrimBitmap(Bitmap bmp) – метод обрізання неточностей серед qr-кодування.

public void Notification (Bitmap b, int classindex) – метод відправки оповіщення про використання кодування.

public string Users(Bitmap b) – метод створення користувачів у контактній книзі.

public void Friends() – метод добавлення користувачів у список друзів.

public void DeserializeParams() – метод читання параметрів групи друзів у контактній книзі.

public static SchedulerExclodes (Bitmap b, Size sz) – метод, який показує коли і хто добавив користувача у список друзів.

public static Tokens Inverse Tokens (Bitmap b) – метод видалення користувачів з групи контактів.

public static Give Comment Status (Bitmap b) – метод створення привілегій для інших користувачів.

Для реалізації інформаційної технології захисту абонента мобільного зв’язку використовуються також інші вузли, реалізація яких наведена у додатку Б.

Інтерфейс користувача – графічний інтерфейс, який надає змогу керувати системною за допомогою графічних об’єктів і дій над ними.

Для проектування інформаційної системи необхідним є створення графічних схем інтерфейсу. Структурну схему інтерфейсу інформаційної системи захисту абонентів мобільного зв’язку зображено на рисунку 4.3

Інтерфейс користувача інформаційної системи захисту абонентів мобільного зв’язку складається з таких сторінок:

– сторінка для сканування QR-коду;
– сторінка для погодження доступу;
– сторінка для присвоєння ролі користувача;
– сторінка для присвоєння повноваження;
– сторінка «користувачі».

Графічна схема інтерфейсу сторінки для авторизації зображено на рисунку 4.4

Сторінка для аналізу абонентів:

- погодження доступу нового абонента;
- поле для введення персональних даних;
- поле для сканування QR-коду;
- кнопка «присвоєння повноважень».

Рисунок 4.4 Структурна схема інтерфейсу інформаційної системи захисту абонентів мобільного зв’язку

На даній сторінці є можливість просканувати QR-код рольового абонента мобільного зв’язку. Сторінка для управління доступом складається з таких елементів:

- навігаційне меню;
- текст «погодити доступ»;
- текст «відмовити у доступі»;
- персональні дані користувача;
- перегляд вхідних викликів;
- кнопка персональних даних;
- присвоєння повноважень абоненту;
- кнопка отримання інформації;
- поле сканування QR-коду.

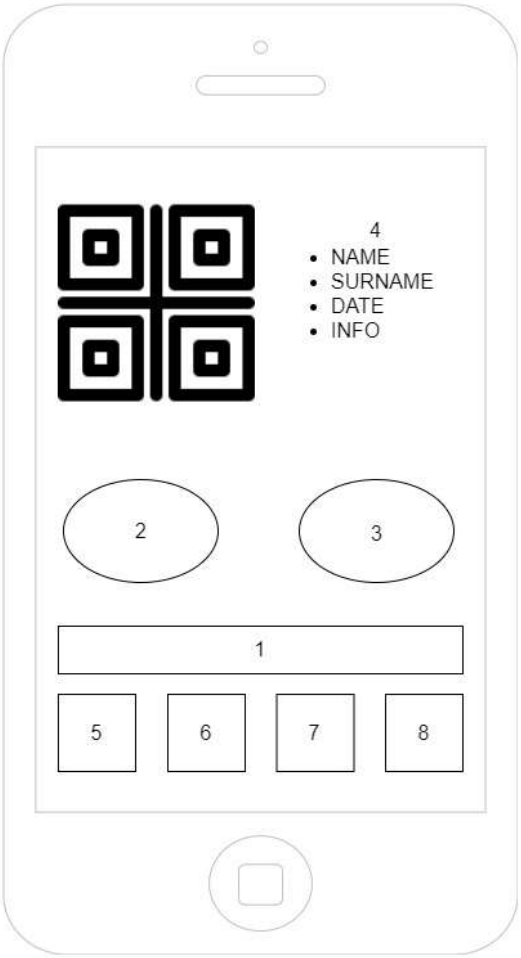

Рисунок 4.5 – Графічна схема інтерфейсу сторінки користувача для управління доступом

Ключовим кроком інформаційної технології захисту абонентів мобільного зв’язку є проектування загального алгоритму роботи. UML-діаграма алгоритму роботи інформаційної системи захисту абонентів мобільного зв’язку зображено на рисунку 4.5 Основними кроками алгоритму є:

1. Початок роботи інформаційної системи захисту абонентів мобільного зв’язку (ініціалізація всіх вузлів).
2. Пвторизація користувача.
3. Запит на доступ від абонента мобільної мережі до рольового абонента.
4. Якщо у доступі відмовлено, то виконується наступна дія.
   4.1. Запис до історії запсів і структури даних.
   4.2. Закриття доступу і вихід з алгоритму.
5. Якщо доступ погоджено, то виконується наступні дії алгоритму.
   5.1 Генерація QR-коду новому абоненту мобільної мережі.
   5.2 Запис до історії записів і структури даних.
   5.3 Запис до Бази даних персональних даних нового абонену.
   5.4 Присвоєння ролі нового абонента мобільної мережі.
   5.5 Присвоєння повноважень новому абоненту.

Після чого виконується вихід із алгоритму.

UML-діаграма функціонування інформаційної технології захисту абонентів мобільного зв’язку зображена на рисунку 4.6.

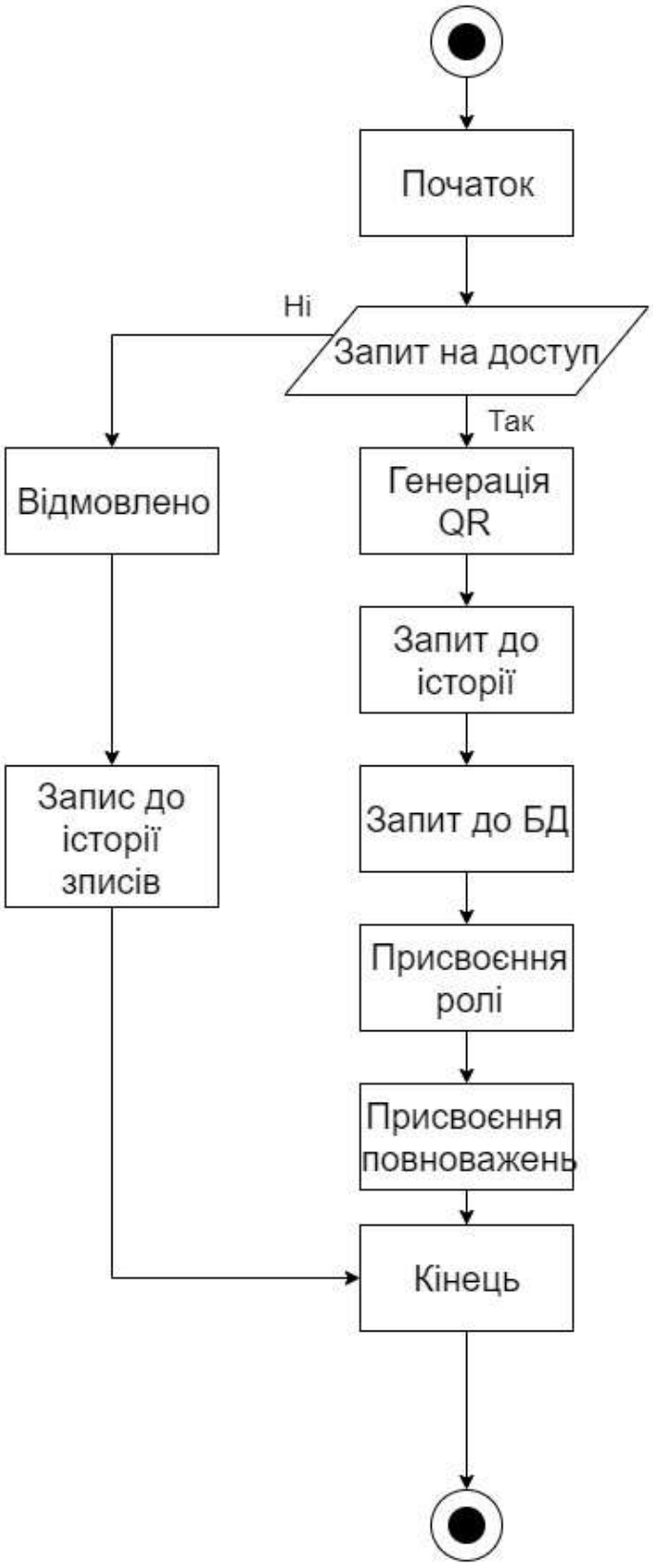

Рисунок 4.6 - UML-діаграма функціонування інформаційної технології захисту абонентів мобільного зв’язку

4.5 Аналіз роботи інформаційної технології захисту абонентів мобільного зв’язку

Тестування розроблюваного засобу є одним із найважливіших методів перевірки виконання поставлених задач і контролю якості, так зване (Quality Control). Тестування засобу включає у себе планування, складання тестів, безпосередньо виконання тестування і аналіз отриманих результатів.

Важливо пам’ятати, що тестування розроблюваного засобу – це не лише теставання ПЗ, а й багато інших пов’язаних дій з для забезпечення процесу якості:

- аналіз і планування;
- написання звітів;
- проведення статичного аналізу;
- розробку тестових сценаріїв;
- оцінку критеріїв закінчення тестування;
- рецензування документації (в тому числі і вихідного коду).

Розглянемо неступниі методи тестування розроблюваної технології:

- метод «Біла скринька;
- метод «Чорна скринька».

Метод тестування «біла скринька» виконується розробником (так як необхідно знати внутрішні принципи роботи програми) для перевірки внутрішньої структури програмного засобу. Об’єктом тестування є дані, отримані шляхом аналізу логіки програми. Перевіряється коректність побудови всіх елементів програми та правильність їхньої взаємодії один з одним. Зазвичай аналізуються керуючі зв'язки елементів, рідше – інформаційні зв'язки. Тестування за принципом «білої скриньки» характеризується ступенем, в якому тести виконують або покривають логіку (вихідний текст) програми. Зазвичай тестування «білої скриньки» засноване на аналізі керуючої структури програми. Програма вважається повністю перевіреною, якщо проведено вичерпне тестування маршрутів (шляхів) її графа управління.

Принцип «білої скриньки» дозволяє врахувати особливості програмних помилок:

1. Попередні припущення про ймовірність потоку керування або даних у програмі часто бувають некоректними. У результаті типовим може стати маршрут, модель обчислень за яким опрацьована слабо.

2. Кількість помилок мінімально в «центрі» і максимально на «периферії» програми.

3. Деякі результати в програмі залежать не від вихідних даних, а від внутрішніх станів програми.

4. При записі алгоритму програмного забезпечення у вигляді тексту на мові програмування можливе внесення типових помилок трансляції (синтаксичних та семантичних).

Метод тестування «чорна скринька» використовується, коли тестувальнику не потрібно знати внутрішні властивості програми. При тестуванні «чорної скриньки» розглядаються системні характеристики програм, ігнорується їхня внутрішня логічна структура. Вичерпне тестування, як правило, неможливе. Тестування «чорної скриньки» не реагує на багато особливостей програмних помилок.

Тести демонструють:

- як виконуються функції програми;
- як приймаються вихідні дані;
- як виробляються результати;
- як зберігається цілісність зовнішньої інформації.

Тестування «чорної скриньки» (функціональне тестування) дозволяє отримати комбінації вхідних даних, які забезпечують повну перевірку всіх функціональних вимог до програми. Програмний виріб тут розглядається як «чорна скринька», чию поведінку можна визначити тільки дослідженням його входів та відповідних виходів. Принцип «чорної скриньки» – не

альтернативний принципу «білої скриньки». Скоріше це доповнює підхід, який виявляє інший клас помилок.

Тестування «чорної скриньки» забезпечує пошук наступних категорій помилок:

1. Некоректних чи відсутніх функцій.
2. Помилок інтерфейсу.
3. Помилок у зовнішніх структурах даних або в доступі до зовнішньої бази даних.
4. Помилок характеристик (необхідна ємність пам'яті і т. д.).
5. Помилок ініціалізації та завершення.

Існує метод тестування «сіра скринька», яка створена на основі розглянутих методів. При роботі з даним методом тестувальник має доступ до коду програми, проте тестування проводить з точки зору кінцевого користувача. Суть даних методів не є складною, проте ефективність тестування за допомогою кожного з них вимагає хороших знань та навичок. В результаті, обрано метод тестування «чорна скринька», оскільки за даним методом тестуються лише вхідні/вихідні дані.

Для перевірки працездатності розроблено інформаційну систему, що базується на запропонованій інформаційній технології.

Нехай, кількість первинних абонентів мобільної мережі – I з повноваженням по можливості надання доступу до персональних даних рольового абонента – *l*, кількість вторинних абонентів - D з повноваженням по можливості надання доступу до персональних даних рольового абонента – *v*. Порівняємо загальну кількість можливості передачі персональних даних рольового абонента з кількістю усіх абонентів, які отримали доступ до персональних даних. Для порівняння необхідно від загальної кількості абоненітів, що отримали доступ до перснальних даних рольового абонента відняти загально можливу кількість можливих передач прав доступу до

персональних даних рольового абонента мобільної мережі. Результати порівняння зображені у таблиці 4.3.

Таблиця 4.3 - аналіз захищеності персональних даних рольового абонента

Кількість первинних абонентів I	Повноваження надати доступ k абонентам	Кількість вторинних абонентів D	Повноваження надати доступ v абонентам	Можлива кількість передачі доступу до персональних даних G	Загальна кількість абонентів, що отримали доступ X
4	2	6	1	15	30
2	3	3	3	15	20
15	3	10	2	65	50
10	4	8	2	56	71
8	7	4	4	72	93
7	10	4	2	78	120
5	4	18	2	56	58

Для аналізу працездатності розробленого програмного забезпечення було відмовлено у доступі абоннетам мобльного звязку, які отримали доступ до персональних даних рольового абонента мобільної мережі і порахавано у відсотковому співвідношенні, на скільки відсотків краще вдалося забезпечити захист персональних даних рольового абонента. Створена інформаційна технологія захисту абонентів мобільного зв’язку порівнювалась з програмним продуктом SMS Анти спам online. Дослідження були проведені при зміні до 1000 потужностей представлених у таблиці, зменшення неконтрольованих передач даних, відносно кількості усіх нових абонентів, які отримали доступ до персональних даних.

Результати захисту абонентів мобільного зв’язку виконання завдань зображені у таблиці 4.4.

Таблиця 4.4 – результати захисту абонентів мобільного зв’язку

% забезпеченя захисту	% забезпеченя захисту програми аналога	% Покращення відносно програми аналога
35	20	17,5
85	53	16,03
33,3	27	12,3
23,07	29,4	-7,9
26,78	20,7	12,8
29,16	29,1	1
53,84	39,8	13,5
13,57	3	25,2
29,05	7,2	20,2
25,7	18,3	14,04
73	70,1	4,03
29,5	33,7	-8,9
43,1	38,5	11,1
10,5	7	30
15,5	15	3,33
32,3	21,3	20
66,6	60	11,1
56,7	45,5	29,7

Як видно з таблиці 4.4, підвищення рівня захисту даних абонента мобільного зв’язку виконано на високому рівні, рівень доступу до персональних даних було зменшено, у середньому, на 15,7%.

Дане дослідження показало, що програмний засіб SMS Анти спам online негативно справився з захистом персональних даних при доданні доступу до персональних даних та доданні нових абонентів, а також програмний засіб SMS Анти спам online, не дає можливості аналізувати доступ до персональних даних.

На рисунку 4.7. зображена початкова активність при вході до інформаційної технології захисту абонентів мобільного зв’язку. Після входу система перевіряє актуальних стан персональних даних і актуалізує графічний вигляд абонентів мобільного зв’язку. Якщо зявляється заявка на додання нового абонента, то користувач повинен відповісти на заявку, якщо користувач погодив додання, то новий абонент отримує доступ до персональних даних, у іншому випадку операція записується до історії додавань і новий абонент не може отримати доступ до персональних даних.

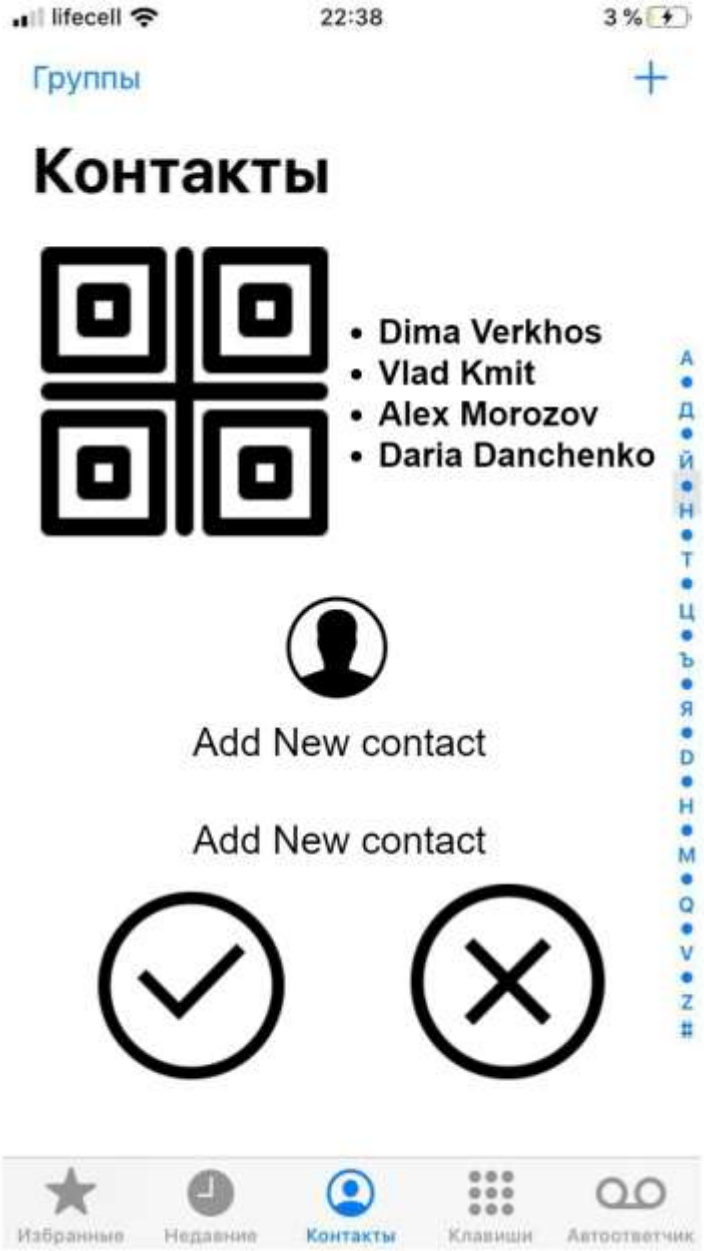

Рисунок 4.7 - Початковий екран мобільного додатку захисту абонента

4.6 Висновок

Отже, запропонована реалізація інформаційної технології цілком відповідає заявленим критеріям і захищає абонента мобільного зв’язку.

5 ЕКОНОМІЧНА ЧАСТИНА

5.1 Оцінювання комерційного потенціалу розробки

Метою проведення технологічного аудиту є оцінювання комерційного потенціалу розробки. Для проведення технологічного аудиту було залучено 2-х незалежних експертів. Такими експертами будуть Коваленко О.О. та Озеранський В.С.

Здійснюємо оцінювання комерційного потенціалу розробки за 12-ма критеріями за 5-ти бальною шкалою.

Результати оцінювання комерційного потенціалу розробки наведено в таблиці 5.1.

Таблиця 5.1 – Результати оцінювання комерційного потенціалу розробки

Критерії	Прізвище, ініціали, посада експерта	
	1. Експерт 1	2. Експерт 2
	Бали, виставлені експертами:	
1	4	4
2	3	3
3	3	4
4	4	3
5	3	3
6	4	4
7	4	3
8	4	4
9	3	3
10	4	3
11	3	4
12	3	4
Сума балів	$СБ_1 = 43$	$СБ_2 = 42$
Середньоарифметична сума балів $\overline{СБ}$	$\overline{СБ} = \frac{\sum_{1}^{3} СБ_i}{2} = 42{,}5$	

Отже, з отриманих даних таблиці 5.1 видно, що нова розробка має високий рівень комерційного потенціалу.

5.2 Прогнозування витрат на виконання науково-дослідної роботи та конструкторсько–технологічної роботи.

Для розробки нового програмного продукту необхідні такі витрати.

Основна заробітна плата для розробників визначається за формулою (5.1):

$$З_о = \frac{М}{Т_р} \cdot t, \quad (5.1)$$

де М- місячний посадовий оклад конкретного розробника;

$Т_р$ - кількість робочих днів у місяці, $Т_р$ = 21 день;

t - число днів роботи розробника, t = 40 днів.

Розрахунки заробітних плат для керівника і програміста наведені в таблиці 5.2.

Таблиця 5.2 – Розрахунки основної заробітної плати

Працівник	Оклад М, грн.	Оплата за робочий день, грн.	Число днів роботи, t	Витрати на оплату праці, грн.
Науковий керівник	6200	295,23	5	1476,15
Інженер-програміст	4000	190,46	40	7618,4
Всього:				9094,55

Розрахуємо додаткову заробітну плату:

$$З_{дод} = 0,1 \cdot 9094,55 = 909,45 \text{ (грн.)}$$

Нарахування на заробітну плату операторів НЗП розраховується як 37,5…40% від суми їхньої основної та додаткової заробітної плати:

$$Н_{зп} = (З_о + З_р) \cdot \frac{\beta}{100}, \quad (5.2)$$

$$Н_{зп} = (9094,55+909,45) \cdot \frac{36,3}{100} = 3631,45 \text{ (грн.)}.$$

Розрахунок амортизаційних витрат для програмного забезпечення виконується за такою формулою:

$$А=\frac{Ц \cdot Н_а}{100} \cdot \frac{Т}{12}, \quad (5.3)$$

де Ц – балансова вартість обладнання, грн;

$Н_а$ – річна норма амортизаційних відрахувань % (для програмного забезпечення 25%);

Т – Термін використання (Т=3 міс.).

Таблиця 5.3 – Розрахунок амортизаційних відрахувань

Найменування програмного забезпечення	Балансова вартість, грн.	Норма амортизації, %	Термін використання, міс.	Величина амортизаційних відрахувань,грн
Персональний комп'ютер	10000	25	3	625
Всього:				625

Розрахуємо витрати на комплектуючі. Витрати на комплектуючі розрахуємо за формулою:

$$K = \sum_1^n Н_і \cdot Ц_і \cdot К_і, \quad (5.4)$$

де n – кількість комплектуючих;

Ні - кількість комплектуючих і-го виду;

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

Кі – коефіцієнт транспортних витрат (приймемо Кі = 1,1).

Таблиця 5.4 - Витрати на комплектуючі, що були використані для розробки ПЗ.

Найменування матеріалу	Одиниці виміру	Ціна, грн.	Витрачено	Вартість витрачених матеріалів, грн.
Флешка	шт.	180	1	180
Пачка паперу	уп.	120	1	120
Ручка	шт.	10	1	10
Всього з урахуванням транспортних витрат				341

Витрати на силову електроенергію розраховуються за формулою:

$$В_е=В\cdot П\cdot Ф\cdot К_п\ ; \quad (5.5)$$

де В – вартість 1кВт-години електроенергії (В=1,7 грн/кВт);

П – установлена потужність комп'ютера (П=0,6кВт);

Ф – фактична кількість годин роботи комп'ютера (Ф=185 год.);

$К_п$ – коефіцієнт використання потужності ($К_п< 1$, $К_п = 0,7$).

$$В_е= 1,7 \cdot 0,6 \cdot 185 \cdot 0,7 = 132,09 \text{ (грн.)}$$

Розрахуємо інші витрати $В_{ін}$.

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

$$В_{ін} = (\mathbf{1}..\mathbf{3}) \cdot (З_о + З_р). \quad \mathbf{(5.6)}$$

Отже, розрахуємо інші витрати:

$$В_{ін} = \mathbf{1} * (\mathbf{9094,55} + \mathbf{909,45}) = \mathbf{10004} \text{ (грн).}$$

Сума всіх попередніх статей витрат дає витрати на виконання даної частини роботи:

$$В = З_о + З_д + Н_{зп} + А + К + В_е + І_в$$

В = 9094,55+909,45+3631,45+132,09+625+341+10004= 24737,54 (грн.)

Розрахуємо загальну вартість наукової роботи $B_{заг}$ за формулою:

$$В_{заг} = \frac{В_{ін}}{\alpha} \quad \textbf{(5.7)}$$

де α – частка витрат, які безпосередньо здійснює виконавець даного етапу роботи, у відн. одиницях = 1.

$$В_{заг} = \frac{\mathbf{24737,54}}{\mathbf{1}} = \mathbf{24737,54}$$

Прогнозування загальних витрат ЗВ на виконання та впровадження результатів виконаної наукової роботи здійснюється за формулою:

$$ЗВ = \frac{В_{заг}}{\beta} \quad (5.8)$$

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

Отже, розрахуємо загальні витрати:

$$ЗВ = \frac{\mathbf{24737,54}}{\mathbf{0,9}} = \mathbf{27486,15} \text{ (грн.)}$$

5.3 Прогнозування комерційних ефектів від реалізації результатів розробки.

Спрогнозуємо отримання прибутку від реалізації результатів нашої розробки. Зростання чистого прибутку можна оцінити у теперішній вартості грошей. Це забезпечить підприємству (організації) надходження додаткових коштів, які дозволять покращити фінансові результати діяльності .

Оцінка зростання чистого прибутку підприємства від впровадження результатів наукової розробки. У цьому випадку збільшення чистого прибутку підприємства $\Delta П_i$ для кожного із років, протягом яких очікується отримання позитивних результатів від впровадження розробки, розраховується за формулою:

$$\Delta П_i = \sum_1^n (\Delta П_я \cdot N + П_я \Delta N)_i \quad (5.9)$$

де $\Delta П_я$ – покращення основного якісного показника від впровадження результатів розробки у даному році;

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

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

$П_я$ – основний якісний показник, який визначає діяльність підприємства у даному році після впровадження результатів наукової розробки;

n – кількість років, протягом яких очікується отримання позитивних результатів від впровадження розробки.

В результаті впровадження результатів наукової розробки витрати на виготовлення інформаційної технології зменшаться на 20 грн (що автоматично спричинить збільшення чистого прибутку підприємства на 20 грн), а кількість користувачів, які будуть користуватись збільшиться: протягом першого року – на 200 користувачів, протягом другого року – на 175 користувачів, протягом третього року – 150 користувачів. Реалізація інформаційної технології до впровадження результатів наукової розробки складала 600 користувачів, а прибуток, що отримував розробник до впровадження результатів наукової розробки – 200 грн.

Спрогнозуємо збільшення чистого прибутку від впровадження результатів наукової розробки у кожному році відносно базового.

Отже, збільшення чистого продукту $\Delta П_1$ протягом першого року складатиме:

$$\Delta П_1 = 20 \cdot 600 + (200 + 20) \cdot 200 = 56000 \text{ грн.}$$

Протягом другого року:

$$\Delta П_2 = 20 \cdot 600 + (200 + 20) \cdot (200 + 175) = 94500 \text{ грн.}$$

Протягом третього року:

$$\Delta П_З = 20 \cdot 600 + (200 + 20) \cdot (200 + 175 + 150) = 127500 \text{ грн.}$$

5.4 Розрахунок ефективності вкладених інвестицій та період їх окупності

Визначимо абсолютну і відносну ефективність вкладених інвестором інвестицій та розрахуємо термін окупності.

Абсолютна ефективність $Е_{абс}$вкладених інвестицій розраховується за формулою:

$$Е_{абс} = (ПП - PV), \qquad (5.10)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному із років, протягом яких виявляються результати виконаної та впровадженої НДДКР, грн;

т – період часу, протягом якого виявляються результати впровадженої НДДКР, 3 роки;

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

t – період часу (в роках) від моменту отримання чистого прибутку до точки 2, 3,4.

Рисунок, що характеризує рух платежів (інвестицій та додаткових прибутків) буде мати вигляд, рисунок 5.1.

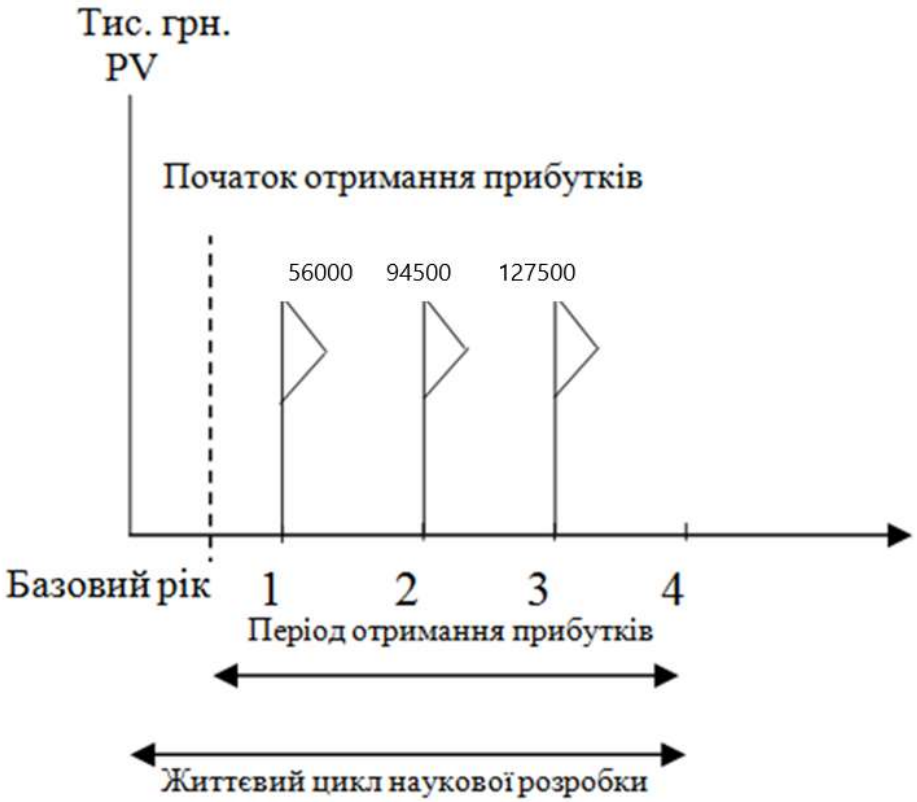

Рисунок 5.1 – Вісь часу з фіксацією платежів, що мають місце під час розробки та впровадження результатів НДДКР

Розрахуємо вартість чистих прибутків за формулою:

$$\mathbf{ПП} = \sum_1^m \frac{\Delta \mathbf{П}_i}{(1+\tau)^t} \qquad (5.11)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному із років, протягом яких виявляються результати виконаної та впровадженої НДДКР, грн;

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

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

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

Отже, розрахуємо вартість чистого прибутку:

$$ПП = \frac{27486,15}{(1+0,1)^0} + \frac{56000}{(1+0,1)^2} + \frac{94500}{(1+0,1)^3} + \frac{127500}{(1+0,1)^4} = 231850,59(грн.)$$

Тоді розрахуємо $E_{абс}$:

$$Е_{абс} = 231850,59 - 27486,15 = 204364,44 \text{ грн.}$$

Оскільки $E_{абс} > 0$, то вкладання коштів на виконання та впровадження результатів НДДКР буде доцільним.

Розрахуємо відносну (щорічну) ефективність вкладених в наукову розробку інвестицій $Е_в$ за формулою:

$$Е_в = \sqrt[Т]{1 + \frac{Е_{абс}}{PV}} - 1 \qquad (5.12)$$

де $Е_{абс}$ – абсолютна ефективність вкладених інвестицій, грн;

PV – теперішня вартість інвестицій PV = ЗВ, грн;

$Т_ж$ – життєвий цикл наукової розробки, роки.

Тоді будемо мати:

$$Е_в = \sqrt[3]{1 + \frac{204364,44}{27486,15}} - 1 = 1,03 \text{ або } 103\ \%$$

Далі, розраховану величина $Е_в$ порівнюємо з мінімальною (бар'єрною) ставкою дисконтування $\tau_{мін}$, яка визначає ту мінімальну дохідність, нижче за яку інвестиції вкладатися не будуть. У загальному вигляді мінімальна (бар'єрна) ставка дисконтування $\tau_{мін}$ визначається за формулою:

$$\tau = d + f,$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; в 2019 році в Україні d = 0,2;

f – показник, що характеризує ризикованість вкладень, величина f = 0,1.

$$\tau = 0,2 + 0,1 = 0,3$$

Оскільки $E_в = 103\% > \tau_{мін} = 0,3 = 30\%$, то у інвестор буде зацікавлений вкладати гроші в дану наукову розробку.

Термін окупності вкладених у реалізацію наукового проекту інвестицій. Термін окупності вкладених у реалізацію наукового проекту інвестицій $T_{ок}$ розраховується за формулою:

$$T_{ок} = \frac{1}{E_в}$$

$$T_{ок} = \frac{1}{1,03} = 0,97 \text{ року}$$

Обрахувавши термін окупності даної наукової розробки, можна зробити висновок, що фінансування даної наукової розробки буде доцільним.

5.6 Висновок

Отже, інформаційна технологія захисту абонента мобільного зв’язку має економічне підгрунття і доцільність розробки.

ВИСНОВКИ

У результаті проведених досліджень за визначеною тематикою було створено інформаційну технологію захисту абонента мобільного зв’язку, яка дозволяє захищати факт передачі персональних даних абонента мобільної мережі і контролювати доступ до конфіденційних даних. Проведено аналіз моделей і методів захисту абонента мобільного зв’язку. Таким чином доведено доцільність розробки інформаційної технології.

Для реалізації було обрано мову програмування C# частини і бібліотеку React для реалізації інтерфейсу користувача.

Створено інформаційну технологію захисту абонента мобільнго зв’язку, яка підвищує рівень захиста даних абонента мобільного зв’язку надаючи ролі та повноваження кожному абоненту. Удосконалено модель захисту абонента мобільного зв’язку, яка використовує QR-кодування для пришвидшення аналізу доступу до даних абонента. Удосконалено метод захисту абонента мобільного зв’язку, який записує кожнового абонента мобільної мережі до структури даних і присвоює унікальний ідентифікатор кожному абоненту, це дозволить підвищити рівень захисту даних абонента мобільного звязку. При цьому, при тестуванні запропонованої інформаційної технології, було спроектовано інформаційну систему, для якої характерним є те, що кількість абонентів, які мають доступ до персональних даних рольового абонента необмежене, є можливість коригувати доступ до персональних даних, кількість рівнів QRn доступу до персональних даних не обмежено. Результати тестування показали підвищення рівня захисту абонента мобільного звязку на 15,7%. Розроблено графічні схеми інтерфейсів головного вікна та основних компонентів.

За результатами досліджень подано заявку на реєстрацію авторського права на твір (комп'ютерну програму) “Інформаційна технологія моніторингу виконання завдань” (номер реєстрації заявки АПС/10094-18), а також опубліковано 2 тез доповіді з науково-технічних конференцій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Савчук Т.О. Використання QR-кодування під час захисту абонентів мобільного зв'язку/ Савчук Т., Верхсоь Д.О. /Всеукраїнська науково-практична Інтернет-конференція «Молодь в науці: дослідження, проблеми, перспективи - 2019»,URL:https://conferences.vntu.edu.ua/index.php/mn/mn2019/paper/view/8188/6821 Збірник праць. – Вінниця : ВНТУ, 2019.

2. Савчук Т.О. захисту абонентів мобільного зв'язку з використанням QR-коду/ Савчук Т., Верхсоь Д.О. /« Науково-технічна конференція підрозділів Вінницького національного технічного університету - 2019», URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2019/paper/view/7183/6255 Збірник праць. – Вінниця : ВНТУ, 2019.

3. Костюк, Ю. Л. Основи розробки алгоритмів [Електронний ресурс]: навчальний посібник / Ю. Л. Костюк, І. Л. Фукс. - М.: БИНОМ. Лабораторія знань, 2010. - 286 с. : Ил. ; 60x90 / 16. - (Елективний курс. Інформатика). - Режим доступу: http: // www. znanium.com

4. Soumya Krishnan M. Software Development Risk Aspects and Success Frequency on Spiral and Agile Model. / M. Soumya Krishnan // International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 1, January 2015 pp.301-310

5. Sherman M. Building Secure Software for Mission Critical Systems [Электронный ресурс] – Режим доступа: http://resources.sei.cmu.edu/asset_files/Presentation/ 2017_017_001_495865.pdf

6. Полицын С. А. Подходы к вычислению временных затрат на проекты в сфере разработки программного обеспечения на основе использования прецедентов / С.А. Полицын // Программная инженерия №7 2011 С.9-14

7. Економічна теорія – [Електронний ресурс] – Режим доступу: http://osvita.ua/vnz/reports/econom_theory/22280/

8. Тернопільський національний педагогічний університет дисципліна «Управління інтелектуальною власністю» [Електронний конспект лекцій]– Режим доступу:https://studfiles.net/preview/5252516/page:2/

9. Тернопільський національний педагогічний університет дисципліна «Етапи процему управління» [Електронний конспект лекцій]– Режим доступу:https://studfiles.net/preview/5252516/page:3/

10. Кравченко В.О. Jснови менеджменту Навчальний посібник/ Т.І. Лепейко, докт. екон. наук, професорОдеса: Атлант, 2012 р. – 211 с.

11. Dirk Kreuter «Entscheidung: Erfolg» /Armin Dittrich – Deutschland, 2017. – 367s.

12. Habgood J. The Game Maker's Apprentice. /J. Habgood. – USA, 2006. – 334 pages.

13. Степанченко И.В. Методы тестирования программного обеспечения: Учеб. пособие / И.В. Степанчеко. – ВолгГТУ. – Волгоград, 2006. – 74 с.

14. Рихтер Д. CLR via C#. Программирование на платформе Microsoft .NET Framework 4.5 на языке C#. / Д. Рихтер. – 4–е изд. – Москва, 2017. – 896 с.

15. Bura J. Construct 2 Game Development by Example/ John Bura. – England, UK, 2014. – 230 pages.

16. Єлісеєнко О. Є. Порівняльний аналіз сучасних гральних рушіїв / О.Є. Єлісеєнко – Вінниця: ВНТУ, 2016. – 55 с.

17. Кроністер Дж. Blender – Базовий матеріал. 4–те видання : пер. з англ. / Дж. Кроністер. – Київ, 2015. – 588 с.

18. Habgood J. The Game Maker's Apprentice. /J. Habgood. – USA, 2006. – 334 pages.

19. Романюк О. В., Єлісеєнко О. Є. Гральний рушій Unity як універсальний інструмент розробки roguelike–ігор / О. В. Романюк, О. Є. Єлісеєнко – Вінниця: ВНТУ, 2016. – 80 с.

20. Goldstone W. Unity Game Development Essentials. / W. Goldstone. – Birmingham, UK, 2009. – 894 pages.

21. Степанченко И.В. Методы тестирования программного обеспечения: Учеб. пособие / И.В. Степанчеко. – ВолгГТУ. – Волгоград, 2006. – 74 с.

22. Бейзер Б. Тестирование чёрного ящика. Технологии функционального тестирования программного обеспечения и систем. / Б. Бейзер – СПб.: Питер, 2004. – 320 с

23. Sherman M. Building Secure Software for Mission Critical Systems [Электронный ресурс] – Режим доступа: http://resources.sei.cmu.edu/asset_files/Presentation/ 2017_017_001_495865.pdf

24. Полицын С. А. Подходы к вычислению временных затрат на проекты в сфере разработки программного обеспечения на основе использования прецедентов / С.А. Полицын // Программная инженерия №7 2011 С.9-14