**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ, КОМП’ЮТЕРНОЇ ТА ПРОГРАМНОЇ ІНЖЕНЕРІЇ  
КАФЕДРА КОМП’ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ**

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.В. Казмірчук

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р.

На правах рукопису

УДК

**МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА**

**ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ**

**«МАГІСТР»**

**Тема**:Методи захисту повідомлень

|  |  |
| --- | --- |
| **Автор:** | Б.О. Вінявський |
| **Науковий керівник:** к.т.н., доц. | А.Б. Петренко |
| **Нормоконтролер:** |  |

**Київ 2020**

**РЕФЕРАТ**

Магістерська атестаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків і має \_\_\_ сторінки основного тексту, \_\_ рисунка, \_\_ таблиць, \_\_ сторінок додатків. Список використаних джерел містить \_\_ найменування і займає \_\_ сторінок. Загальний обсяг роботи \_\_\_ сторінок.

Метою магістерської є досягнути підвищеного рівня захисту повідомлень при передачі повідомлень за допомогою технології Bluetooth 4.0.

В роботі вирішено наступні задачі: розкрито сутність захисту персональних даних та сучасний стан впровадження мобільних додатків захисту персональних даних та повідомлень, обґрунтовано доцільність створення програмного модуля захисту повідомлень, здійснено аналіз технологій розробки мобільних додатків, створено прототип мобільного додатку, проведено аналіз алгоритмів захисту, проведено аудит безпеки обміну інформацією.

В роботі розроблено модуль програмного забезпечення для передачі повідомлень по захищеному каналу технології Bluetooth.

Розроблений модуль програмного забезпечення відноситься до галузі інформаційної безпеки і може бути використаний для підвищення якості обслуговування підчас передачі даних.

Можливі напрямки розвитку цієї роботи пов’язані із застосуванням розробленого модуля в програмному забезпеченні націленому на організацію mesh мережі.

Ключові слова: .

**ЗМІСТ**

ВCТУП………………………………………………………………………..4

Розділ 1. ТЕXНOЛOГIЇ ЗАXИCТУ ДАНИХ, ТЕOPЕТИЧНИЙ АСПЕКТ, ТЕOPЕТИЧНI ПIДXOДИ ДO ВИВЧЕННЯ………………………………………..8

1.1 Сутність захисту даних, методи впровадження мобільних додатків з захистом даних………………………….………..……………………….…….…8

1.2 Доцільність розробки програмного модуля по обміну захищеними повідомленнями………………………………..………………………………….16

1.3. Аналіз ризиків в середовищах обміну інформацією…………….…18

1.3.1 Вразливості…………………………………………………………….18

1.3.2 Загрози…………………………………………………………………21

1.3.3 Модель порушника……………………………………………………21

1.3.4 Правова система………………………………………………………22

Висновки до розділу 1………………………………………………………23

Розділ 2. АНАЛIЗ МЕТOДIВ POЗPOБКИ МOБIЛЬНИX ДOДАТКIВ.….25

2.1 Мобільні додатки та засоби їх розробки…………………………….…25

2.2 Аналiз технологій розробки мобільних додатків. Вибір технології для розробки додатку захисту повідомлень…………………………………….…..29

2.3 Аpxiтектуpа вирішення задачі та функціональна структура додатку захисту повідомлень………………………………………………….……………33

2.4 Функціональна структура додатку захисту повідомлень……………36

2.4.1 Уведення та оброблення ключових даних…………………………..36

2.4.2 Оброблення вхідної та вихідної інформації…………………………37

2.4.3 Формування/перевіряння електронного цифрового підпису………38

2.4.4 Генератори випадкових (псевдовипадкових) послідовностей, які використовуються для формування ключів, векторів ініціалізації тощо………38

2.4.5 Самотестування………………………………………………………..38

2.5 Вибір засобів захисту даних………………………….……………….40

2.5.1 Метод експертної оцінки…………………………………..………….43

2.5.2 Метод віднесеної оцінки……………………………………………..46

Висновок до розділу 2………………………………………………………54

Розділ 3. МАТЕМАТИЧНИЙ АНАЛІЗ ОБМІНУ ПОВІДОМЛЕННЯМИ.55

3.1 Вибір алгоритму шифрування………………………………………….55

3.3 Вибір алгоритмів стиснення…………………………………………….57

Висновок до розділу 3………………………………………………………58

ВИCНOВКИ………………………………………………………….……...60

CПИCOК ВИКOPИCТАНИX ДЖЕPЕЛ……………………………………61

ДOДАТКИ……………………………………………………………………70

Додаток В. Фрагменти вихідного коду мобільного додатку

Додаток Г. Журнали сеансів безпровідного обміну

Додаток Д. Слайди

**ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ**

|  |  |  |
| --- | --- | --- |
|  |  |  |
| ПЗ | − | програмне забезпечення; |
| ISO | − | International Organization for Standardization. |
| MITM | − | Man In The Middle |
| SSP | − | Secure Simple Pairing |

**ВCТУП**

***Актуальнicть роботи.*** Кожен день людина користується електронними пристроями, завдяки їм спілкується з друзями, заводить нових знайомих, замовляє необхідні товари. Таким чином виникає необхідність для створення нових програм та додатків для роботи з цими пристроями, як розважального характеру, так i для роботи, освіти та іншого. Отже мобільна розробка це стрімко розвиваюча галузь, яка охоплює всі сфери життя людини i надає широкий вибір послуг, розрахованих на потреби різного типу. Мобільні додатки допомагають користувачам економити власний час, виконують багато важливих функцій та роблять життя простішим.

Значний прогрес у розвитку інформаційних технологій, а саме – запровадження інформаційно-телекомунікаційних технологій та пов’язане з ним збільшення обсягів i напрямів використання інформації у різних сферах суспільного життя, її передача новітніми комунікаційними засобами істотно розширили можливості щодо збирання, зберігання i обробки інформації відносно окремих громадян. Активнicть у формуванні автoматизoваниx баз даних, обробка та поширення відомостей про осіб без їхнього відома призвели до виникнення глобальної за своїми масштабами у часі та просторі проблеми інформаційної безпеки людини, суспільства i держави щодо захисту персональних даних. Тобто проблема захисту інтересів особи в інформаційній сфері – це i проблема захисту персональних даних, що стосується будь-якої сфери діяльності людини, суспільства i держави. Від розуміння важливості й необхідності створення державного механізму захисту персональних даних залежить добробут як окремої людини, так i держави.

Метою даної магістерської роботи є досягнути підвищеного рівня захисту повідомлень при передачі повідомлень за допомогою технології Bluetooth 4.0.

Для отримання необхідних результатів були сформульовані наступні задачі:

- розкрити сутність захисту персональних даних та сучасний стан впровадження мобільних додатків захисту персональних даних та повідомлень;

- обґрунтувати доцільність створення програмного засобу захисту повідомлень в умовах сьогодення;

- здійснити аналіз технологій розробки мобільних додатків;

- створити прототип мобільного додатку;

- провести аналіз алгоритмів захисту;

- провести аудит безпеки обміну інформацією.

Об’єкт досліджень – програмний модуль мобільного додатку обміну повідомленнями в безпровідному середовищі.

Предмет дослідження – технологія передачі інформації Bluetooth.

Методи дослідження. При вирішенні поставленого завдання використовувалися наукові досягнення в областях розробки інформаційних систем i програмного забезпечення, математичні методи аналізу захищеності повідомлень, методи захисту даних в мережах інформаційної безпеки.

Наукова новизна полягає в удосконаленні системи захисту безпеки безпровідного обміну повідомленнями на основі застосування методів захисту з використанням засобів шифрування та стиснення.

Практична цінність отриманих результатів полягає в використанні програмного модуля та ініційовані ним елементи захисту даних для використання в mesh мережах обміну даними.

Структура i обсяг роботи. Робота складається з вступу, трьох розділів, висновків та додатків. Містить \_\_\_\_ сторінок друкованого тексту, в тому числі \_\_ сторінки тексту основної частини з \_\_\_ рисунками, списку використаних джерел з \_\_\_ найменуваннями на \_\_\_ сторінках, \_\_\_ додатка на \_\_\_ сторінках.

**POЗДIЛ 1. ТЕXНOЛOГIЇ ЗАXИCТУ ДАНИХ, ТЕOPЕТИЧНИЙ АCПЕКТ, ТЕOPЕТИЧНI ПIДXOДИ ДO ВИВЧЕННЯ**

* 1. **Сутність захисту даних. Впровадження мобільних додатків захисту даних**

Розвиток міжнародно-економічної, фінансової, банківської, культурної, правоохоронної, правової та інших форм співробітництва, що передбачає вільний рух інформаційних ресурсів щодо товарів, капіталів і послуг за умов використання інформаційно-телекомунікаційних технологій, збільшення потоків персональних даних і підтримання суверенітету держави визначають об’єктивну необхідність захисту персональних даних. Без дослідження всесвітніх міжнародних та європейських стандартів, вивчення особливостей національних регулятивних підходів окремих країн Європи, Сполучених Штатів Америки (США) та інших демократичних держав, що мають теоретичні напрацювання, розвинуте законодавство і багаторічний досвід з питань захисту прав і свобод людини, у тому числі права на захист персональних даних, украй ускладнюється розуміння сучасних проблем забезпечення відносин із захисту відомостей про особу взагалі та персональних даних громадянина зокрема [5–8, 13, 14].

Головною передумовою появи законодавства про захист персональних даних у європейських країнах на початку 1970-x роках було виникнення автоматизованих баз даних, розвиток телекомунікації та потреба у забезпеченні приватного життя людини відповідно до принципів Європейської Конвенції “Про захист прав людини та основоположних свобод” (Рим, 04. 11. 1950 p.) [29, 45]. Більшість закордонних законів у сфері захисту персональних даних мають типову назву – “Закон про захист даних”.

При виникненні нових загроз та видів порушень прав особи на її персональні дані система захисту залишається незмінною, а до галузевої нормативно-правової бази вносяться необхідні доповнення та зміни. При цьому створення зазначених національних базових законів обов'язково ґрунтується на принципах захисту персональних даних, що були розроблені різними міжнародними організаціями, що представляють політико-економічні союзи та співтовариства держав, зокрема Організацію з економічного співробітництва і розвитку, Раду Європи, Євросоюз, Організацію американських держав, країни Шенгенської угоди, Міжнародну торговельну палату [27, 30–35, 45, 46, 49, 50]. Слід додати, що розвиток технічних засобів масових комунікацій обумовило лавино утворене зростання обсягів переданих персональних даних. Це призвело до необхідності оцінки різних характеристик інформації, зокрема її обсягу та захисту.

З точки зору соціально-філософської концепції, поняття інформація нерозривно пов'язана з категорією відображення інформаційного простору в інформаційному суспільстві. Інформація, будучи віддзеркаленням матеріальної суті, служить способом опису взаємодії між джерелом інформації та одержувачем. Оскільки інформацію можна зберігати, перетворювати й передавати, мають бути її носії, передавачі, канали зв’язку, приймачі та середовище передачі інформації.

Слід згадати, що термін “інформація” увійшов у науковий обіг задовго до того, як стрімкий розвиток засобів комунікації, комп'ютерної техніки й заснованих на ній технологій перетворення й передачі даних, поява безпосередньо пов'язаних з ними галузей науки й техніки перетворили його в знаковий символ сучасної епохи. Відома безліч визначень інформації як результат наукової дискусії і різних підходів до трактування даного поняття. Первісне поняття “інформація” пов’язувалося винятково з комунікативною діяльністю в суспільстві (Н. Вінер, P.Хартлі, К. Шенон, Ю. Шрейдер) [55, 79–84]. Було з’ясовано, що інформація – це найвищий, найскладніший результат упорядкованого відображення у вигляді повідомлень, знань, відомостей про природу, суспільство, у цілому про об’єктивну реальність, що охоплюють всі сфери людської діяльності, використовуються в процесі спілкування, управління, виробництва, пізнання, творчості, виховання, освіти тощо. Це дозволяє звернути увагу на управлінську природу інформації. Інформація розглядається як єдність поновлення різноманітності і як її обмеження. Основна функція інформації - давати уявлення (інформувати) про об’єкт, відображаючи його властивості [3, 26, 40, 59, 79, 80].

Різновидом інформації є персональна інформація, що відображає як індивідуальність окремої особи, так i її загальнолюдські бioлoгiчнi й соціальні властивості. Персональна інформація відображає людську різноманітність, індивідуальність кожної людини як носія унікальних елементів фізичної, фізіологічної, психічної, економічної, культурної або соціальної тотожності. Визначальною ознакою персональної інформації є її індивідуалізований характер, здатність ідентифікувати конкретну особу за допомогою тих чи інших критеріїв. Під час такої ідентифікації відбувається процес персоніфікації тих чи інших відомостей, тобто прив’язування їх до конкретної людини. Інформація, що ідентифікує (ототожнює), дозволяє безпосередньо або за допомогою інших чинників ідентифікувати особу, є персональною інформацією. Відомості (як документовані, так i в усному вигляді) є формою відображення бioлoгiчнoї й соціальної тотожності, а також індивідуальності кожної людини [73, 81, 85, 86].

Для позначення відомостей про особу, які вже зазнали певної обробки людиною, зафіксовані на певному носії, упорядковані i придатні для автoматизoванoї обробки, уживається термін “персональні дані” (лат. personalitas – особистість) [4, 6, 13, 64, 76].

Неправомірне збирання, використання й поширення персональної інформації завдає шкоду уявленню про індивіда. Це не тільки бioгpафiчнi дані, як-от: прізвище, ім’я, по батькові, дата i місце народження особи, національність, релігійні, політичні чи філософські переконання, освіта, місця навчання i роботи, відомості про сімейний стан, наявність дітей, ставлення до військової служби [4, 8, 13, 68]. До персональної інформації також належать відомості про матеріально-фінансовий стан (банківські рахунки, платежі по них, нерухоме та рухоме майно, майнові права), стан здоров’я, особисті стосунки приватного характеру та багато інших відомостей у матеріальній формі в різних сферах суспільного життя, що створюються, збираються, зберігаються, поширюються та використовуються в інший спосіб як з відома особи – суб’єкта даних, так i без її відома. Ця інформація дозволяє суспільству оцінювати людину як індивідуальність, формувати її репутацію (лат. reputatio – оцінка) [8, 13, 64– 66, 77, 81].

Захист персональної інформації став актуальним під час виникнення та широкого розповсюдження ризиків життю, здоров’ю, репутації, добробуту людини внаслідок неправомірного збирання й використання персональної інформації, тобто від небажаного вторгнення у внутрішню сферу життя людини, що охороняється правом на повагу до приватного життя [2, 7, 10, 45, 57, 67, 80].

Якщо півстоліття тому для здобуття інформації про людину необхідно було витратити значні зусилля, сучасний рівень розвитку інформаційних технологій дозволяє здійснити обробку даних про тисячі людей за лічені секунди i без надмірних витрат. Поєднання неточних чи застарілих персональних даних створюватиме спотворену уявлення про особу та наносити відповідні збитки.

Практика створення цифрового образу особи набула поширення за допомогою, так званих, процедур “співставлення даних” (data matching), під час яких здійснюється збирання, співставлення й об’єднання персональних даних, що знаходяться в різних базах даних; а також “профілювання” (profiling) – створення профілю людини, сукупності характеристик особи за певними критеріями на підставі аналізу відомостей про особу з різних баз даних. Ці види таємного збору відомостей про особу отримали складноскорочену назву “датавейленс” (dataveillance), що перекладається як “стеження за даними” [8, 12, 13, 18, 19–23, 26, 27, 46, 49].

Можливості технічних засобів, що дозволяють збирати й обробляти персональну інформацію, постійно й стрімко розширюються; технології вдосконалюються, а ціна на них зменшується. Навіть за звичайними технологіями збору інформації значна кількість персональної інформації постійно збирається. Будь-яка платіжна операція, будь-то покупка, продаж чи інвестування, створює сукупність персональних даних. Ця інформація використовується як із комерційною метою, так i для звітування перед фіскальними органами держави.

Певні соціальні ризики виникають у зв’язку з використанням багатофункціональних кредитних карток із мікропроцесором (multi-function smart card), так званих, “смарт-карток”,що використовуються для ідентифікації особи в різних сферах суспільних відносин. Серед найбільш важливих – ризики, що пов’язані з ідентифікацією особи й можливістю неправомірного використання персональної інформації. Питання захисту від “крадіжок ідентичності” є серед іншого одним із завдань Міжнародної організації поліції – Інтерполу [45–47].

Слід відзначити, що з точки зору безпеки особи та чи інша персональна інформація має різний ступінь важливості для індивіда, що зумовлюється рівнем ризику заподіяння шкоди. Загроза неадекватного сприйняття оточуючими, дискримінації за певною ознакою, іншого протиправного використання персональної інформації вимагає передбачення її потенційної “вразливості” для людини. Урахування інтересів особи i її суб’єктивного ставлення до тієї чи іншої інформації, що неможливо повною мірою охопити в узагальнених нормативних приписах, вимагає законодавчого віднесення об’ємного переліку даних до категорії “вразливих даних” (про расове або етнічне походження чи національність, політичні погляди, релігійні або філософські переконання, членство у профспілках чи громадських організаціях, дані, що стосуються стану здоров’я чи надання медико-санітарної допомоги, сімейних i особистих стосунків приватного характеру чи статевого життя, відомості про кримінальні вчинки чи протиправну поведінку), а також надання особі права самостійно визначати межі циркуляції персональної інформації в суспільстві. Цим створюється територіальний простір, у якому особа може контролювати межі своєї індивідуальності. Для ефективного захисту цього простору особа повинна мати право сама окреслювати ці межі, тобто встановлювати, яка персональна інформація, для яких цілей, у якому обсязі i яким одержувачам може передаватися [7, 11, 18–27, 29–38].

Такий підхід зумовлений тим, що тільки особа, якої стосується персональна інформація, може оцінити ймовірний ризик неправомірного використання такої інформації та шкоду, яку може задіяти особі розкриття такої інформації. Це становить основу природи права на приватність персональної інформації та усвідомлення такого феномену, як “приватна сфера” життя людини. У західній правовій доктрині для позначення цього правового інституту використовується термін “прайвесі” (privacy). Найбільш удалим його перекладом українською мовою є “приватність”, що походить від слова “приватний”. Воно характеризує якісний стан об’єкта, що випливає з його належності до “приватної сфери” життя людини. До того ж цей термін одразу асоціюється з тим, що належить безпосередньо приватній особі i є недоступним для людського загалу, є “приватною справою” i протиставляється публічному. Його антонім англійською мовою “пабліситі” (publicity) також близький за звучанням до українського еквівалента “публічність”, що означає відкритість для публіки, гласність [8, 11, 29, 56, 57, 64, 66].

Право на приватність оформилось в окреме правове поняття не так давно, наприкінці XIX століття, хоча його коріння можна знайти у ранніх джерелах права. Для виокремлення права на приватність у самостійне поняття людству потрібно було дійти до такого рівня розвитку цивілізації, при якому автономність життя стала вкрай необхідною для збереження й реалізації людиною себе як особистості [1, 3, 7, 8, 10, 11, 13, 28, 48–50, 58, 63, 78–82].

Перша концепція права на приватність пройшла судову апробацію у CША. У практиці амеpиканcькиx судів нерідко розглядалися випадки комерційного використання персональних характеристик індивідів, таких як зовнішній вигляд, ім’я та голос. Нерідко такі випадки порушення прав людини супроводжувалися порушеннями права власності. Американські суди вбачали в цих індивідуальних рисах особистості, на які посягли інші особи, певний об’єкт захисту майнового інтересу. Традиційне західне уявлення про право на приватність бере свій витік з права на недоторканність домоволодіння, а західна доктрина приватності має територіальний характер, оскільки захищає персональний життєвий простір особи [14, 33].

Американський юрист Вільям Л. Проссер після вивчення прецедентів, створених американським судами під час розгляду справ щодо втручання у приватне життя людини, запропонував таку класифікацію: розкриття фактів, що стосуються приватного життя; повідомлення неправдивої інформації про людину; неправомірне використання зображень зовнішності, голосу людини i, нарешті, останнє – фізичне домагання.

Питання правового регулювання збору й передачі інформації є ключовими для захисту приватності інформації про особистість. При цьому комунікації й бази даних виступають як носії персональної інформації.

Стрімке поширення електронних комунікацій, у яких повідомлення передаються у цифровому вигляді, не дозволяє технічно й нормативно розмежувати, де закінчується комунікаційна приватність i починається приватність персональних даних [8, 11, 18, 27, 30, 41, 46, 49].

Проблема забезпечення права на приватність користувачів Інтернетом ускладнюється екстериторіальним характером інформаційного обміну. Інтернет дозволяє встановлювати безпосередній контакт між людиною-суб’єктом даних, який перебуває під юрисдикцією однієї держави, та іншими суб’єктами інформаційного обміну, які можуть перебувати на території інших держав. Забезпечити дію національних положень, а значить гарантувати належний рівень захисту приватності для своїх громадян у цьому середовищі, для держави стає проблематичним. У той же час створення національними урядами штучних перешкод для вільного транскордонного обігу персональної інформації негативно відбиватиметься на міжнародному співробітництві у багатьох сферах.

Розуміння цієї проблеми спонукало міжнародне співтовариство до розвитку співробітництва з метою забезпечення безперешкодного інформаційного обміну, яке призвело до створення сукупності міжнародних норм i принципів, що охоплюються міжнародно-правовим інститутом захисту приватності персональної інформації [19–23, 30–35, 49, 50, 57].

Таким чином, особливістю захисту права на приватність персональної інформації є спрямованість на забезпечення свободи особи у визначенні просторових i часових рамок інформаційного контакту з іншими суб’єктами, підконтрольності циркуляції персональної інформації в суспільстві, що є важливим для підтримання автономії особи, захисту приватної сфери її життя.

Слід відзначити, що міжнародно-правовий інститут захисту приватності персональної інформації містить відповідні норми й принципи, спрямовані на забезпечення безперешкодності передачі інформації через кордони. Ця мета нерозривно пов’язана з міжнародним захистом права людини на приватність персональної інформації, що становить головний елемент усього міжнародного правового механізму регулювання транскордонної передачі персональної інформації [19–21].

Отже, стрімкий розвиток сучасних цифрових технологій значно спростив доступ до питомої інформації. Дані, на пошук яких раніше витрачалися місяці, тепер можна отримати, увімкнувши комп’ютер та задавши запит на пошуковому сайті в Інтернеті. Цей, здавалося б, позитивний прогрес у справі пошуку інформації має також i вкрай негативну сторону. Саме спрощення процедури отримання інформації призвело до розвитку кіберзлочинності. У наш час кожний користувач Інтернету, телефонного зв’язку та інших комунікацій є потенційною жертвою кібершахраїв та кіберзлочинців [30, 47, 49, 51].

Питанням захисту персональних даних присвячено багато різнопланових праць як зарубіжних, так i вітчизняних дослідників. Роботи, що проаналізовані нами в дослідженні, як i роботи багатьох інших авторів, безумовно, мають наукове i практичне значення, але вони не дають цілісного уявлення про єдину систему захисту персональних даних, сучасного стану впорядкування суспільних інформаційних відносин та перспективи його комплексного розвитку в Україні. Сучасне законодавство у сфері захисту персональних даних, хоч i постійно змінюється та вдосконалюється, усе ще не може врегулювати більшість питань щодо захисту від згаданих загроз. Але, перш за все, обґрунтування нормативно-правових та організаційних аспектів механізму забезпечення захисту персональних даних повинно базуватися на розвинутому понятійно**-**категорійному апараті у сфері захисту персональних даних.

* 1. **Доцільність розробки програмного модуля по обміну захищеними повідомленнями**

Рядовий користувач привик до зручності користування програмами в його власному телефоні. Звиклість до однотипного виконання програми формується на основі її кореня – потреби в користуванні, і стовбура вивчення функціоналу прикладної програми. Про службове програмне забезпечення користувач переважно не знає, а якщо і знає, то лише відомості скільки відсотків заряду акумуляторної батареї споживає наприклад Android OS. Для забезпечення цілісності операційної системи і одноманітності системного середовища, розробники все більше стараються обмежити поле діяльності користувача. Це також призводить до покращення прогнозування реакції користувача на роботу програми. Проте в цьому випадку закривається від вільного перегляду, в тому числі зміни, інформація про фактичні дії програми, створення та обмін інформацією. З огляду на це, а також популярність телефонів з операційною системою Android, можна взяти до розгляду екземпляри деяких з таких пристроїв. Розробником операційної системи Android є компанія Google LLC, на даний момент заявляє більше 70 офісів в 50 країнах світу. Отже можна говорити про вплив політки 50 країн на написання операційної системи Android, програмного забезпечення, яке в ній виконується. Як би це не звучало, але програми писалися різними розробниками з використанням різних інструкцій і в умовах різних законодавчих правил. Отже можна підсумувати, що досліджуваний екземпляр не може бути настільки різноманітним, та повинен вміщати сталі, які виконуватимуться на кожній платформі в межах лінійки операційної системи однаково. Також для дослідження важливо, що об’єкт дослідження не повинен діяти як виокремлений продукт, але повинен виконуватися як будь-який схожий по класу та функціональності.

Оскільки досліджуваний екземпляр програмного забезпечення виконуватиме функції обміну інформацією, як і інше схоже програмне забезпечення, то важливо підібрати методи виявлення аномалій і реєстрації поведінки середовища обміну. Потрібно брати до уваги, що публіковане та розповсюджуване програмне забезпечення для ОС Android підписане цифровим ключем розробника ПЗ та накладені ліцензійні умови на розповсюдження, використання і виконання. Однією з умов публікації програми в магазині ПЗ, а також виконання на ліцензійних копіях ОС Android є накладення цифрового ключа, наданого розробнику від компанії Google LLC. Накладення ключа відбувається в інтегрованому середовищі розробки Android Studio. Безумовно є і інші методи підписання програми, але вони не засвідчують протокол накладення ключа що обумовлює відмови в роботі програми.

Отже можна дійти висновку, що компанія Google LLC монополізувала ринок платформи Android, займає головне місце в розробці, та вимагає співпраці розробників для підтримки їхнього програмного забезпечення.

Тому важливим є використання засобів розробки мобільних додатків, для уникнення конфронтації в правових відносинах, та вільної оболонки операційної системи. Виконання підвищених вимог до безпеки обміну за допомогою безпровідної технології диктує забезпечення цього за допомогою додаткових засобів та конфігурації існуючих.

Застосування методів захисту даних до мобільного додатку є найкращим доступним рішенням. Використання інших методів і засобів диктує економічні затрати і пониження комфортності використання мобільного додатку.

* 1. **Аналіз ризиків в середовищах обміну інформацією**

**1.3.1 Вразливості**

Оскільки Bluetooth технологія передачі інформації є стандартизованою NIST, то про знайдені вразливості технології потрібно звертатися до них. На сьогоднішній день відомі і задокументовані[91]. Що стосується Bluetooth v4.0 подано в таблиці 1.1.

Таблиця 1.1

|  |  |
| --- | --- |
| Вразливість безпеки | Роз’яснення |
| МІТМ під час сполучення | Для найвищої безпеки пристрої BR / EDR повинні вимагати захисту MITM під час SSP і відмовлятися приймати неаутентифіковані ключі посилань, створені за допомогою спарювання. |
| Пари ключів SSP ECDH можуть бути статичними або іншим чином слабо генеруватися | Слабкі пари ключів ECDH мінімізують захист від прослуховування SSP, що може дозволити зловмисникам визначати секретні ключі посилань. Усі пристрої повинні мати унікальні, сильно сформовані пари ключів ECDH, які регулярно змінюються. |
| Статичні ключі SSP полегшують атаки MITM. | Пакети доступу забезпечують захист MITM під час SSP. Пристрої повинні використовувати випадкові унікальні ключі для кожної спроби створення пари. |
| Пристроям режиму безпеки 4 (тобто 2.1 або пізнішої версії) дозволяється повернутися до будь-якого іншого режиму безпеки при підключенні до пристроїв, які не підтримують режим безпеки 4 (тобто 2.0 і раніше). | Найгіршим сценарієм буде пристрій, який повернеться до режиму безпеки 1, який не забезпечує ніякого захисту. NIST настійно рекомендує пристрою режиму безпеки 4 повернутися до режиму безпеки 3 у цьому випадку. |
| Спроби автентифікації повторювані. | Потрібно включити механізм у пристрої Bluetooth, щоб запобігти необмеженим запитам автентифікації. Специфікація Bluetooth вимагає експоненційно збільшення інтервалу очікування між послідовними спробами автентифікації. Однак він не вимагає такого інтервалу очікування для запитів виклику автентифікації, тому зловмисник може зібрати велику кількість відповідей на виклик (які зашифровані секретним ключем посилання), які можуть просочувати інформацію про секретний ключ посилання. |
| Алгоритм потокового шифрування E0, що використовується для шифрування Bluetooth BR / EDR, є відносно слабким | Шифрування, схвалене FIPS, може бути досягнуто шляхом розшарування рівня шифрування, затвердженого FIPS, над шифруванням Bluetooth BR / EDR. Зауважте, що Bluetooth із низьким енергоспоживанням використовує AES-CCM. |
| Конфіденційність з низьким енергоспоживанням може бути порушена, якщо адреса Bluetooth зафіксована та пов’язана з певним користувачем. | Для зменшення енергоспоживання можна застосувати конфіденційність адрес, щоб зменшити цей ризик. |
| Устаріле сполучення з низьким енергоспоживанням не забезпечує пасивного захисту від прослуховування. | У разі успіху підслуховувачі можуть захоплювати секретні ключі (тобто LTK, CSRK, IRK), розподілені під час сполучення з низьким енергоспоживанням |
| Режим захисту від низького енергоспоживання 1 Рівень 1 не вимагає жодних механізмів безпеки (тобто, відсутність автентифікації або шифрування). | Подібно до режиму безпеки BR / EDR 1, це по своїй суті небезпечно. Натомість настійно рекомендується режим енергобезпеки з низьким рівнем енергії 1 рівень 4 (автентифіковане з'єднання та шифрування). |
| Ключі посилань можуть зберігатися неправильно. | Ключі посилання можуть бути прочитані або змінені зловмисником, якщо вони не надійно зберігаються та захищаються за допомогою елементів керування доступом. |
| Сильні сторони генераторів псевдовипадкових чисел (PRNG) невідомі. | Генератор випадкових чисел (RNG) може створювати статичні або періодичні числа, які можуть знизити ефективність механізмів безпеки. Впровадження Bluetooth повинно використовувати сильні PRNG на основі стандартів NIST. Див. NIST SP 800-90A, SP 800-90B, SP 800-90C. |
| Не існує автентифікації користувача. | Специфікація передбачає лише автентифікацію пристрою. Захист на рівні програми, включаючи автентифікацію користувача, може бути доданий розробником програми за допомогою накладання. |
| Наскрізна безпека не виконується. | Зашифровані та автентифіковані лише окремі посилання. Дані розшифровуються в проміжних точках. Наскрізна безпека поверх стеку Bluetooth може бути забезпечена за допомогою додаткових засобів контролю. |
| Послуги охорони обмежені | Аудит, відмова та інші послуги не є частиною стандарту. За потреби розробник програми може накласти ці служби накладеним способом. |
| Виявні та / або підключені пристрої схильні до атак. | Будь-який BR / EDR / HS пристрій, який повинен перейти в режим пошуку або підключення для створення пари або підключення, повинен робити це лише протягом мінімальної кількості часу. Пристрій не повинен постійно знаходитись у режимі пошуку або підключення. |

Операційна система Android 7.1.2 використовує власний стек інструкцій для управління процесом з’єднання. Проте з’єднання створює драйвер від Oracle, та стандартизований NIST і який на даний момент немає відкритих інструкцій. Отже до вразливості також можна віднести підміну DalvikVM в AOSP на будь-яку сторонню в тому числі комерційну без зміни функціональних інструкцій. Знайдені офіційні вразливості розміщені [99], проте нові вразливості не розміщаються за рішенням автора гілки ресурсу.

Програмний екземпляр не використовує додаткові сторонні бібліотеки та не відкриває каналів передачі даних без згоди на це користувача. Отже вразливістю можна визначити умисне інфікування чи об’єднання досліджуваного програмного екземпляру з іншим ПЗ, яке при запуску буде мати привілегії батьківського.

**1.3.2 Загрози**

З сторони користувача, загрозами розкриття обміну даних є:

* розголошення часу, режиму обміну інформацією;
* розголошення частини повідомлення або всього повідомлення.

З сторони програмного забезпечення загрозу відкриття передаваних даних становить запуск досліджуваного ПЗ поза технічними умовами.

З сторони радіоканалу передачі даних:

* наведений шум і блокування радіоканалу;
* моніторинг радіоканалу;
* повторення сигналу радіоканалу;
* розкриття технології каналу і передача сигналів по іншим каналам;

**1.3.3 Модель порушника**

Модель порушника служить макетом сприйняття користувача для втілення загроз. Тому потрібно розглянути порушника як комплекс правил які впливають на здійснення ним впливу загрозливого характеру.

Мета порушника:

* отримання повідомлення та інформації, що становить інтерес;
* отримання можливості виконання сторонніх інструкцій в радіоканалі;
* контроль апаратного забезпечення користувача;
* розкриття зашифрованої інформації в зручний для причитування вигляд, компрометація повідомлень;
* нанесення збитків для користувача та третім особам.

Засоби впливу:

* програмно-апаратний комплекс захоплення і моніторингу каналу зв’язку;
* апаратний комплекс постановки завад;
* пристрій користувача або схожий за характеристиками;
* утиліти віддаленого контролю обладнання користувача;
* утиліти виконання експлоітів;
* фізичний вплив на користувача.

Для того щоб модель розглядуваного порушника не перетворилася в еталонну модель робота, тобто не стала відірваною від реальності, потрібно вжити правила використання досліджуваного середовища.

Дії порушника носять умисний характер, оскільки випадкове отримання доступу до ідентифікаторів безпровідної передачі даних захищено, як вказано в специфікації NIST [91]

Також потрібно попередити користувача про застосування засобів розвідки до ОС Android, оскільки відповідні дозволи від компанії Google LLC не отримані.

**1.3.4 Правова система**

Операційна система Android ліцензована компанією Google LLC, та надається у використання як OEM інстальована при купівлі підтримуваного тачфона. У випадку не погодженням з їхніми ліцензійними умовами та згодами про використання даних, компанія Google просить повернути пристрій та отримати компенсацію витрат. В результаті дослідження ринку тачфонів, взято до уваги сектор малосерійних приладів, які встигли змінити власників чи змінити юридичні умови надання цих приладів виробниками. Тому увага автора впала на вибір пристроїв компанії Motorola. Лінійка пристроїв Droid 4 випускалася для Американського ринку з розблокованим модулем звязку CDMA, але заблокованим GSM модулем. Оскільки в Україні кількість CDMA провайдерів перебуває в меншості і такий стандарт зв’язку є не затребуваним, то в переважній кількості пристрої Droid 4 продавалися заробітчанами, які повернулися з заробітків. В даний момент не маючи жодної гарантійної підтримки чи підтримки з сторони виробника, немає потреби запрошувати у виробника згоду на використання його пристроїв в лабораторних цілях. Проте програмне забезпечення обмежене підтримкою ОС Android 4.0.1. В програмний інтерфейс користувача інтегровано патентовані технології енергозбереження, що безпосередньо впливає на можливість відлагодження і тестування програмних модулів. Також спроби зворотної розробки обмежують патенти конструкторів пристрою.

**Висновки до розділу 1**

Стрімкий розвиток сучасних цифрових технологій значно спростив доступ до питомої інформації. Дані, на пошук яких раніше витрачалися місяці, тепер можна отримати, увімкнувши комп’ютер та задавши запит на пошуковому сайті в Інтернеті. Цей, здавалося б, позитивний прогрес у справі пошуку інформації має також i вкрай негативну сторону. Саме спрощення процедури отримання інформації призвело до розвитку кіберзлочинності. У наш час кожний користувач Інтернету, телефонного зв’язку та інших комунікацій є потенційною жертвою кібершахраїв та кіберзлочинців.

Питанням захисту персональних даних присвячено багато різнопланових праць як зарубіжних, так i вітчизняних дослідників. Роботи, що проаналізовані в дослідженні, як i роботи багатьох інших авторів, безумовно, мають наукове i практичне значення, але вони не дають цілісного уявлення про єдину систему захисту персональних даних, сучасного стану впорядкування суспільних інформаційних відносин та перспективи його комплексного розвитку в Україні.

Мобільні інформаційні технології сприяють поліпшенню сервісного обслуговування споживчої аудиторії, а також розвитку торгових i виробничих відносин.

Динаміка розвитку ринку мобільних додатків підтверджує прогнози про високе зростання доходів в короткостроковій перспективі.

Бiльшicть сучасних методів виявлення атак використовують деяку форму аналізу контрольованого простору на основі правил або статистичного підходу.

**РOЗДIЛ 2. АНАЛIЗ МЕТOДIВ POЗPOБКИ МOБIЛЬНИX ДOДАТКIВ**

**2.1 Мобільні додатки та засоби їх розробки**

Смартфони стають незамінними гаджетами для кожної людини. Зараз набагато частіше зустрічаються люди без персонального комп'ютера, але з декількома телефонами. За даними Gartner, в 2017 році по всьому світу було продано майже 1,5 млрд смартфонів проти 1,4 млрд штук роком раніше [1], в зв'язку з цим і число мобільних додатків з кожним днем ​​стрімко зростає.

Станом на третій квартал 2017 року, більш ніж один мільйон додатків були розроблені для Android, з більш ніж 25 млрд завантажень додатків [8]. Аналіз, який проводився протягом 2015 року, показав, що більше 67% мобільних розробників використовували платформу Android для розробки і публікації додатків [20; 30]. У 1 кварталі 2016 року Android домінував на ринку мобільних телефонів з часткою в 84,1% [41].

Розробка додатків під ОС Android є найбільш актуальним процесом в розробці мобільних додатків. Виходячи з цього, актуальним є і тема роботи, пов'язана з реалізацією програмного продукту захисту персональних даних з використанням нейронних мереж.

Android - це повноцінна операційна система, в основі якої покладено ядро Linux V3.6. Найперші версії Android знайшли своє застосування в сегменті мобільних телефонів, включаючи смартфони і дешевші розкладні пристрої. Однак повний спектр обчислювальних сервісів і багаті функціональні можливості Android дозволяють створювати додатки, які далеко виходять за рамки тільки сегмента мобільних телефонів. Операційна система Android стає все більш популярною і в інших платформах і програмах.

У сучасних умовах розробка ПЗ в більшості випадків ведеться з використанням інтегрованих середовищ розробки (IDE). IDE мають безсумнівні гідності: процес компіляції, збирання і запуску програми зазвичай автоматизовані. Сучасна IDE «Anroid-розробника» повинна підтримувати Java 8, Scala, Groovy, а також іншими мовами віртуальної машини Java, які регулярно використовуються. IDE повинна бути сумісна з будь-якими складками систем контролю версій, наприклад, Ant, Maven або Gradle. Розглянемо IDE, придатні для розробки під ОС Android.

Одним з найбільш популярних IDE для розробки під ОС Android є IntelliJ IDEA. З точки зору можливостей і ціни IDEA поставляється в двох варіантах: безкоштовна Community edition, і платна Ultimate edition з розширеною функціональністю. Community edition призначена для JVM і Android-розробки. Безкоштовна версія підтримує Java, Kotlin, Groovy і Scala; Android; Maven, Gradle і SBT; працює з системами контролю версій Git, SVN, Mercurial і CVS. Ultimate edition пристосована для веб і enterprise-розробки. Ця версія IDE працює не тільки з Git, SVN, Mercurial і CVS, але також з Perforce, ClearCase і TFS; в ній можна писати на JavaScript і TypeScript. І, звичайно, не обійшлося без SQL і інструментів для роботи з базами даних. IntelliJ IDEA виділяється своїм глибоким розумінням коду, розумною ергономікою, вбудованими функціями для розробки і підтримкою багатьох мов. Підсвічування синтаксису і просте автодоповнення коду - звичайна справа для будь-яких сучасних Java-редакторів. IntelliJ IDEA аналізує код при завантаженні і безпосередньо при введенні. Вона вказує на передбачувані проблеми і, по бажанням, пропонує список ймовірних швидких правок до виявлених проблемам. На всі дії, які потрібні під час написання коду, є комбінації клавіш для швидкого доступу до них, в тому числі – визначення символів у спливаючих вікнах. Також IDEA оснащена інструментами для збірки, середовищем виконання тестів, інструментами покриття і вбудованим термінальним вікном. IntelliJ IDEA підтримує всі основні сервери додатків JVM, і дозволяє розгортати і проводити налагодження на цих серверах, що нівелює добре знайомі всім програмістам Java Enterprise труднощі. IDEA безпосередньо з коробки «розуміє» та іншими мовами - Groovy, Kotlin, Scala, JavaScript, TypeScript і SQL. На даний момент є 19 мовних плагінів IntelliJ [6].

Наступна розглядаються IDE для розробки під ОС Android середу Eclipse. Довгі роки це середовище впевнено лідирувала за популярністю серед розробників під ОС Android. Вона повністю безкоштовна, з відкритим вихідним кодом, написаним переважно на Java. Проте, її модульна архітектура дозволяє використовувати Eclipse і з іншими мовами. Проект Eclipse, ініційований IBM, з'явився в 2001 році. Портативність Java допомагає Eclipse бути кроссплатформенним середовищем: ця IDE працює на Linux, Mac OS X, Solaris і Windows. Своєю продуктивністю Eclipse зобов'язана JVM. Eclipse працює досить повільно, оскільки впирається корінням в досить старе «залізо» і древні версії JVM. Екосистема плагінів Eclipse - це одночасно сильна сторона цієї IDE і одна з головних її проблем. Саме через несумісність плагінів часом падають цілі підбірки, і програмістам доводиться починати роботу спочатку. В даний час для Eclipse написано понад 1700 плагінів, офіційних і неофіційних. Модулі Eclipse, підтримують понад 100 мов програмування і майже 200 фреймворків для розробки додатків. Eclipse, підтримує налагодження як локально, так і віддалено, за умови, що використовується JVM, яка підтримує віддалену налагодження. У Eclipse - широка база документації самого різного віку, цінності і корисності. На відміну від розглянутих вище середовищ розробок NetBeans з'явилася як студентський університетський проект в Празі в 1996 році. У 1997 році IDE стала комерційним продуктом, а в 1999 році її викупила компанія Sun Microsystems і вже на наступний рік представила open source-реліз. Актуальна версія працює на машинах під керуванням ОС Windows, Mac OS X, Linux і Solaris. Ну а пакет portable можна запустити на будь-яких системах, для яких існує Java-машина.

Редактор NetBeans підтримує мови, виявляє помилки під час друку, і допомагає за допомогою спливаючих підказок і «розумним» автодоповненням коду. Крім того, NetBeans володіє повним спектром інструментів, які дозволяють програмісту реструктуризувати код, не ламаючи його, виконувати аналіз початкових кодів, а також пропонує широкий набір підказок для швидких виправлень або розширення коду. До складу NetBeans входить інструмент проектування для графічного інтерфейсу користувача Swing, раніше відомий як «Project Matisse». У NetBeans є відмінна вбудована підтримка Maven і Ant, а також плагіна для Gradle. Це означає, що їх можна просто відкривати, а не імпортувати. NetBeans також містить графічне відображення для залежностей Maven. Окремий візуальний відладчик дозволяє програмісту робити знімки екрану графічного інтерфейсу і вивчати інтерфейси додатків, виконаних за допомогою JavaFX і Swing. Профайлер NetBeans робить більш очевидним те, яким чином використовується процесор і пам'ять, і володіє відмінними інструментами для пошуку витоків пам'яті [7].

Слід згадати середовище розробки Android Studio, орієнтоване на розробку додатків під ОС Android. IDE Android Studio - результат співпраці JetBrains і Google, вона була анонсована 16 травня 2013 року на конференції Google I / O. За великим рахунком, це та ж сама IDEA, за винятком того, що в якості збирача використовується Gradle, а не Ant. Всі зміни, що вносяться в Android Studio, через деякий час з'являються в IDEA і навпаки. Google рекомендує саме Android Studio для розробки додатків під ОС Android [5].

У даному підрозділі проведено аналіз та огляд існуючих інструментальних засобів для розробки програмного забезпечення для платформи Android.

Проведений аналіз показав, що платформа Android з кожним днем стає все більш популярною як серед розробників, так і серед користувачів.

Нами виконано огляд офіційних засобів розробки і засобів розробки, представлених сторонніми розробниками. Проведений аналіз показав, що розробка додатків для платформи Android може проводиться різними засобами з використанням мови програмування Java. Більшість розглянутих засобів програмування є або вільно поширюваними, або умовно безплатними, що теж підвищує популярність платформи Android.

Таким чином, можна зробити висновок, що платформа Android і інструменти розробки під цю ОС будуть користуватися великою популярністю в найближчий час.

**2.2 Аналіз технологій розробки мобільних додатків. Вибір технології для розробки додатка захисту повідомлень**

Нині існує хороший вибір мов програмування для розробки мобільних додатків. Це пов'язано з тим, що для різних мобільних пристроїв доводиться використовувати різні мови програмування. Зазвичай це пов'язано з тим, що мобільні пристрої мають різні ОС.

Нижче будуть розглянуті такі технології як Java, Qt (заснований на бібліотеках C ++), Windows Phone SDK (написання на мові XAML), iPhone SDK (основна мова - Objective-C), Android SDK (основна мова - Java) і Symdian (основна мова - C ++).

1. Java 2 Micro Edition (J2ME). В першу чергу J2ME це набір специфікацій і технологій, призначених для різних типів портативних пристроїв. Існують два основних напрямки: Connected Device Configuration (CDC) і Connected Limited Device Configuration (CLDC). Напрямок визначає тип конфігурації центральних бібліотек Java, а так же параметрів віртуальної машини Java (в якій будуть виконуватися додатки). Логічно припустити, що пристрої CDC будуть більш «розвиненими», як приклад можна привести комунікатори. До пристроїв CLDC відносяться звичайні мобільні телефони, апаратно володіють більш скромними можливостями (ресурсами). Спеціальні режими дозволяють визначати функціональність конфігурацій для різних типів пристроїв. Режим Mobile Information Device Profile (MIDP) призначений для CLDC портативних пристроїв з можливістю комунікувати. Режим MIDP визначає функціональність - роботу призначеного для користувача інтерфейсу, збереження налаштувань, роботу в мережі і модель програми. CLDC і MIDP закладають основу реалізації J2ME [1].

Java-код інтерпретується безпосередньо самим пристроєм за допомогою так званої Java Virtual Machine. Цей механізм робить можливим вільне поширення Java-додатків, так як вони працюють на всіх пристроях з аналогічною Java-платформою [2].

Програмування Java-додатків і на сьогоднішній день займає більшу частину, так як більшість мобільних пристроїв (в основному мобільні телефони) в світі мають вже встановлену Java-машину.

2. Qt. Середовище розробки Qt була придбана Nokia в 2008 р у норвезької Trolltech за 150 мільйонів доларів. Qt в основному використовується в якості крос-платформного середовища, яке дозволяє використовувати написані з її допомогою додатки на різних пристроях і операційних системах, в тому числі Windows, Mac OS X, Linux, Symbian, Android та інших [3]. Починаючи з версії Qt 4.0 з'явилася можливість програмувати для мобільних пристроїв. З зростаючою користувальницькою базою Qt, росте потреба у вбудованих, мобільних додатках і UI-розробниках.

Qt є однією з найбільш вдалих бібліотек для С ++. Налагодження додатків, розроблених для мобільних пристроїв, відбувається за допомогою емулятора, який міститься в середовищі розробки. Таким чином, ми можемо писати складні програми для мобільних пристроїв з використанням бібліотек C ++ і підтримкою платформ.

Для роботи Qt на мобільних пристроях необхідна установка відповідного фреймворка.

Платформа Windows Phone не просто чергова платформа для мобільних пристроїв. Вона містить в собі не тільки технологічну складову, але і повністю опрацьовану концепцію дизайну інтерфейсу і взаємодії з користувачем під назвою Metro-дизайн або стиль Metro [4].

Вся розробка під Windows Phone ведеться в середовищі Visual Studio. Середовище є дуже зручною для розробки і налагодження додатків. Для мобільних додатків під Windows Phone налагодження відбувається за допомогою емулятора Windows Phone за допомогою середовища розробки Windows Phone.

3. iPhone SDK. Розробка під iPhone під операційну систему iOS можлива тільки під Mac OS X. Але в Інтернеті можна знайти статті, як можна програмувати і на Macintosh і навіть на VM. Варто зауважити, що Apple надає інструменти безкоштовно, платити доведеться за підписку розробника [5].

Для написання програм під iPhone пропонується використовувати Objective-C. При цьому є можливість писати так само і на C і на C ++ (для цього необхідно змінювати розширення файлів з .m на .mm). Правда при цьому повністю піти від Obj-C не вдасться, майже весь API розрахований саме на Obj-C, виключення складають наприклад OpenGL (хоча для його ініціалізації доведеться використовувати кілька рядків коду на Obj-C), так само повністю доступні стандартні бібліотеки C / C ++ (так, наприклад, з файлової системою можна працювати як засобами SDK на Obj-C, так і використовуючи стандартну бібліотеку С для введення / виведення (fopen (), fgetc (), etc)) [5].

Налагодження програми відбувається за допомогою середовища XCode і емулятора iPhone встановленого в ній.

4. Android SDK. Для розробки під Android можна використовувати середу Eclipse з встановленим плагіном ADT. Розробка ведеться на мові програмування Java. Є можливість налагодження з використанням емулятора вбудованого в ADT або безпосередньо на мобільному пристрої з ОС Android.

Існує різні версії SDK, які використовуються для написання коду для різних версій Android. В даний час велика поширення отримали версії 2.2 і 2.3. Підтримується майже повна зворотна сумісність версій.

Крім розробки на мові Java підтримується можливість більш низкоуровневая розробка з використанням Android NDK (Native Development Kit) на мові C / C ++.

6. Symbian і C ++. Для створення програмного забезпечення під Symbian можна використовувати мову програмування C ++. В основному даний підхід використовується для Symbian OS v6.1, 7.0, 7.0s і 8.0 [61].

Розробка для Symbian OS (якщо говорити про C ++) зазвичай ведеться на ПК. Середовище розробки - звична багатьом програмістам Visual Studio, це також можуть бути IDE Metrowerks CodeWarrior Development Studio, Borland C ++ BuilderX Mobile Edition, Carbide.C ++ (відносно нова IDE, створена компанією Nokia на базі Eclipse), забезпечена додатковими інструментальними пакетами (SDK). Розробнику доступні практично всі звичні можливості щодо як створення ПО, так і налагодження (трасування, перегляд змінних, стека викликів, структур класів і ін.).

Налагоджений скрипт буде працювати в емуляторі Symbian OS. Відзначимо, що цю підсистему правильніше було б назвати симулятором, оскільки імітуються НЕ апаратні засоби, а лише програмне оточення (відповідні API операційної системи, реалізовані поверх API Win32). При цьому програмні модулі, які завантажуються в емулятор, являють собою виконані файли для архітектури x86 (НЕ ARM, на базі якої побудовані смартфони), відповідне ПО для цільової платформи формується після підсумкової компіляції. Це передбачає певну специфіку (скажімо, раніше була досить поширена ситуація, коли програма, нормально функціонувала в середовищі емулятора, відмовлялася працювати на реальному пристрої), але сьогодні емулятор забезпечує досить високу ступінь подібності та проблеми виникають лише при створенні програм, нестандартно використовуючих API [74].

З появою нових технологій, раніше використовувані йдуть в історію. Зараз розробників, які використовують такі технології як Symbian з використанням C ++ і / або J2ME, стає все менше і лідируючу позицію займають технології, що використовують різні SDK (Windows Phone SDK, iPhone SDK, Android SDK). Але недолік всіх існуючих SDK в тому, що розробляються нативні додатки, тобто додатки, що функціонують під управлінням тільки однієї ОС.

На сьогоднішній день розробка програм для ОС Android верифікується магазином Google Play. Протокол накладеня ключа підпису відбуваться при застосуванні команди Release в підтримуваній IDE Android Studio.

Процес розробки відбувається шаблонним методом, та передбачає використання наперед визначених типових застосувань інструкцій. Інструкції середовища розробки Android Studio розміщені у вільному доступі [94]. Мови програмування, використовувані в графічному редакторі – Java та мова розмітки XML. Для автора Java є вільною для програмування, з XML може не виникнути проблем, оскільки середовище розробки передбачає графічний, текстовий та змішаний режими конструктора візуального інтерфейсу розроблюваної програми.

**2.3 Аpxiтектуpа вирішення задачі та функціональна структура додатку захисту повідомлень**

Архітектура ПЗ – це артефакт, що представляє собою результат процесу розробки програмного забезпечення. Елементи архітектури ПЗ і моделі їх з'єднання призначені для задоволення вимог до проектованих системам. У проекті архітектури ПЗ повинні бути враховані функціональні та не функціональні вимоги до ефективності, витривалості, розширюваності, відмовостійкості, продуктивності, можливості повторного використання, а також адаптування розробляється ПО. Архітектурний проект ПЗ, дозволяє оперативно визначити, наскільки даний програмний продукт відповідає пропонованим до нього вимогам. [92] Базуючись на цьому визначенні розгляд досліджуваного програмної оболонки потрібно розпочати з операційної системи. Оскільки в попередніх розділах вже визначилися з апаратним середовищем, та зважаючи на правові висновки, потрібно зазначити що використання операційної системи у вигляді в якому надає розробник мобільного телефону компанія Motorola є неможливим. В зв’язку з цим проведено заміну програмної оболонки операційної системи Android на аналогічну за функціональністю Android Open Source Project, Lineage OS на основі Android 7, розповсюдження на вимогах Apache License v2.0. [96] Тим не менше середовище Android Studio вільно працює з мобільним телефоном, підготовленим на основі вказаного відкритого проекту.

Алгоритм виконання екземпляру програмного забезпечення без впливу моделі порушника в досліджуваних умовах наступний:

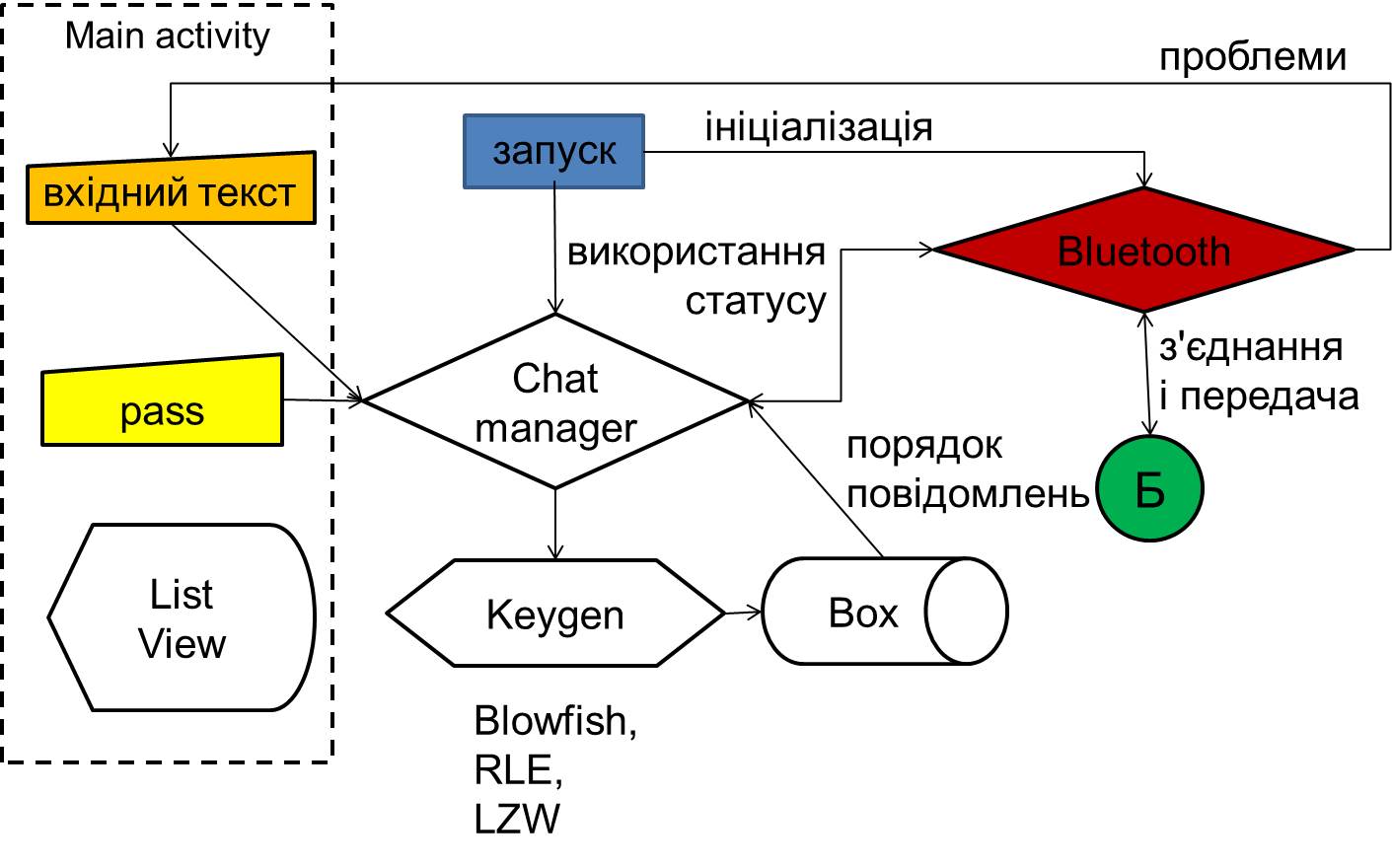
1. Мобільні пристрої запущені, жодних програм в головній черзі;

2. Користувач А, Б запускають Silent Messenger;

3. Користувач А вибирає назву потрібного пристрою з випадаючого списку та вводить повідомлення;

4. Вкінці набору повідомлення користувач А натискає кнопку Send в інтерфейсі програми;

5. Користувач А вголос передає користувачу Б парольну строку.

6. Користувач Б отримує повідомлення в зашифрованому вигляді. 

7. Користувач Б вводить парольну строку та розшифровує повідомлення.

8. Користувачі закінчують роботу з технічним засобом.

Блок-схему роботи модуля мобільного додатку наведемо на рисунку 2.1.

Рисунок 2.1 Блок-схема роботи модуля мобільного додатку

Повне безпровідне середовище передачі даних становить ту ж вказану послідовність, проте на будь-якій стадії присутній порушник, який не виключено може бути одним з користувачів або третьою особою.

Отже концептуальними є модулі шифрування повідомлення, збереження інформації, відправки, доставки.

Модуль шифрування забезпечується алгоритмом Blowfish в його експортному вигляді, з наперед генерованим S-блоком, змінним 18hex значним ключем ініціалізації P-блоку. Стійкість переданих даних становить 0, тому що порушнику відомі ресурси програми з розміщеного коду[93]. Оскільки програмне забезпечення розробляється з урахуванням масовості, то для даного модуля передбачається інші функції, не розглядувані в межах роботи.

Модуль збереження інформації представлений масивом з маркованими індексами якому пристрою і які дані відправити. У випадку збоїв в роботі програми чи збоїв операційної системи інформація повідомлення буде втрачена. Також у випадку перезапуску програми інформація та дані повідомлення будуть затерті влаштованими в ОС засобами. Цим досягається стерильність програми як засобу передачі інформації.

Модуль відправки повідомлення організований внутрішніми класами програми для перевизначення управління апаратним Bluetooth передавачем. Цим прийомом гарантується виконання Bluetooth з’єднання та передача анонімної строки по радіоканалу. У випадку постановки радіошумів, програмне забезпечення конфігурує з'єднання з іншими параметрами, перебираючи всі доступні для з’єднуваного пристрою комбінацій. Передача повідомлення відбувається тільки за умови створення радіоканалу (сокета).

Модуль отримання інформації організований в якості серверної частини. Підбір конфігурації сокета також відбувається з урахуванням зайнятих чи ушкоджених комбінацій.

У випадку потреби порушника видати себе за користувача А та відправити повідомлення з свого пристрою від імені користувача А – це працює за наявності в порушника відповідних технічних засобів та навиків керування ними. Оскільки спосіб порушення включає нанесення шкоди об’єктам власності потенційного користувача А і Б в обміну інформацією, це одночасно створює порушення в юридичній сфері. Доказами порушення є логи мережевого обміну, зібрані у випадку конфігурації відповідної опції в параметрах розробника. Детальніше описано в додатку А. В даній роботі не розглянуто фізичні аспекти передачі повідомлень та виклики порушення середовища.

**2.4 Функціональна структура додатку захисту повідомлень**

**2.4.1 Уведення та оброблення ключових даних.**

Основним призначенням засобу досліджуваного екземпляру є обмін текстовими повідомленнями. Тому потрібно користувачу А потрібно ввести довільне повідомлення, а користувачу Б прочитати його.

Отже необхідно використати модулі введення тексту з клавіатури пристрою Motorola Droid 4 або екранної клавіатури наданої віртуальною машиною Dalvik у випадку потрапляння курсора в текстове поле. Оскільки текстове поле в операційній системі забирає місце в пам’яті відповідне до розміру введених символів представлених в машинному коді, то будь-який елемент з наявних в інтерфейсі або інтерфейсів прослуховування завдань може отримати дані текстового поля, що є неприпустимим. Тому найкраще забрати дані текстового поля функцією, яка б передала дані в обробку або зберегти в пам’яті в якості набору зашифрованих символів, призначених до відправки користувачу Б.

Для передачі даних необхідно виявити та авторизувати канали передачі повідомлень. Згідно обраних методів визначено канали передачі RFCOMM технології Bluetooth. Для утворення каналу передачі необхідно розпізнати ідентифікатори пристроїв, які знаходяться поряд та визначити чи є серед них потрібний, утворити канал передачі даних повідомлення. Отже необхідно зберегти або відтворити з наявних записів стан попередньо утворених каналів зв’язку (спарованих пристроїв). Цим займається віртуальний адаптер реального пристрою Bluetooth. Зчитування попередньої інформації відбувається з конфігураційних записів в операційній системі Android через відповідні методи доступу до захищених від зміни даних про спаровані пристрої

**2.4.2 Оброблення вхідної та вихідної інформації.**

Для ізолювання оточення інтерфейсу від оточення шифрування і засобів передачі інформації в операційній системі Android застосовуються інструменти створення та управління потоками. Це дає можливість уникнути впливу на елементи даних, підготовлених до обробки, в процесі та після обробки в криптографічному алгоритмі та впродовж сеансів отримання і відправлення шифротексту. Доступ до елементів віртуального масиву можна отримати по факту завершення потоку, або спеціальним інструментом отримання системних повідомлень з потку Handler. Цей інструмент дозволяє витягувати або вставляти необхідні дані в робочому потоці, що в свою чергу дозволяє створювати обмін інформацією між робочим каналом звязку і методами запису і зчитування в віртуальний сокет — віртуальний сеансовий зв'язок. Перед відправленням відкритого тексту від користувачів відбувається шифрування або дешифрування такого масиву символів та попрерднє перетворення в шіснадцятковий вигляд. Фізично ніякі дані не використовуються, а лише тимчасове віртуальне перетворення фізисно введених символів в шифрований вид алгоритмом Blowfish з гененрацією сенансового P-блоку. Зтиснений вигляд P-блоку виводиться у текстову строку інтерфейсу для зчитування користувачом А та передачі користувачу Б. Користувач Б вказаними перетвореннями отримає зашифроване повідомлення, але без введеної текстової строки P-блоку не отримає розшифрованого повідомлення користувача А. У випадку неналежного введення відповідної текстової строки згенрованої з P-блока, в користувача Б повідомлення видалиться засобами «Збірника сміття» віртуальної машини Dalvik. Програмний екземпляр не пропонує, а також не передбачено передачу текстової строки P-блока будь-яким іншим методом крім зчитування і введення в текстову строку.

**2.4.3 Формування/перевіряння електронного цифрового підпису.**

В пропонованому екземплярі програмного забезпечення не використовується електронний цифровий підпис. Натомість використовується ідентифікатори обладнання в якості таких, що дозволяють відкрити канал зв’язку та достатні для незахищеного обміну шифрованим текстом.

**2.4.4 Генератори випадкових (псевдовипадкових) послідовностей, які використовуються для формування ключів, векторів ініціалізації тощо**.

Вибірка значень P-блоку відбувається з перетворених до шіснадцяткового виду 8ми значних символьних змінних. Такі змінні генеровані за допомогою функції Rundom, доступ до якої імпортовано з загальної бібліотеки Java. Дана функція повертає псевдовипадкове значення допустиме для цілочисленної змінної int. За допомогою розробленої функції відбувається вибірка значень змінної int , перетворення її до виду 16 значного символу текстової строки та формування строки з 8 таких елементів. P-блок включає 16 таких строк, тому генерація відбувається індивідуально для кожної строки. Для недопущення генерації схожих строк з заданих в S-блоці відбувається перевірка згенрованої строки P-блоку в циклі перед присвоєнням в масив P-блоку.

**2.4.5 Самотестування.**

Перевірка поточного стану обігу повідомлень відбувається передачею і обробкою службових повідомлень всередині програми та інтерфейсом користувача.   
Під час запуску програмний екземпляр проводить ініціалізацію користувацького середовища, ініціалізує віртуальне середовище для роботи з обладнанням. При відсутності працюючого передавача Bluetooth або якщо він вимкнений,то користувацький інтерфейс покаже повідомлення типу Toast про виключений інтерфейс. Також про відсутність з’єднання, проблеми з під’єднанням, проблеми з передачею, користувач також буде повідомлений про такі проблеми за допомогою Toast повідомлень. Також при першому запуску програмного екземпляра на мобільному пристрої буде організовано перевірку наданих дозволів користувача на експлуатацію та встановлення параметрів згідно правил безпеки операційної системи Android.

До технічних характеристик, які характеризують програмно-апаратне середовище належать технічні характеристики обладнання, найменування встановленого операційного забезпечення, характеристики віртуального середовища та встановлені на ньому версії користувацького інтерфейсу, технічні характеристики інтерфейсів, які задіяні в передачі та обслуговуванні послуг надаваних ТЗ. Дані наведено в таблиці 2.1 взяті з [97] та доповнено.

Таблиця 2.1 Специфікація ТЗ «Silent Messenger»

|  |  |
| --- | --- |
| Назва характеристики | Значення |
| 1 | 2 |
| Клас обладнання | Мобільний телефон |
| Марка виробника | Motorola |
| Модель | Droid 4 |
| Характеристики апаратної частини | |
| Процесор | Cortex-A9 |
| Чіпсет | TI OMAP 4430 |
| Оперативна пам’ять | 1Gb |
| Відеокарта | PoweVR SGX540 |
| Технічні характеристики інтерфейсу Bluetooth | |
| Версія технології інтерфейсу | 4.0 |
| Частота передачі сигналу | 2,4-2,4835 ГГц |
| Швидкість передачі в каналі | в асинхронному режимі 723,2 Кбіт/с |
| в синхронному режимі 433,9 Кбит/с |
| Кількість застосованих каналів | 32 |
| Фізичний режим передачі | частотно-стрибковий спектр поширення |
| Профіль роботи | Serial Port Profile (SPP) на специфікації ETSI TS07.10 |
| Протокол програмної обробки | RFCOMM |
| Кількість одночасних з’єднань за допомогою протоколу між парою | 79 |
| Характеристики програмного середовища | |
| Операційна система | Lineage OS |
| Тип операційної системи | відкрита на основі AOSP |
| Версія операційної системи | CM14 (Android 7) |
| Активна резервована оперативна пам’ять | 1Gb |

Вказані параметри зібрані з умовами мінімального і достатнього переліку умов за якими ТЗ зможе повністю надавати послуги.

**2.5 Вибір засобів захисту даних**

Засоби захисту кінцевої інформації – даних, переданих за допомогою безпровідного каналу слід аналізувати починаючи з найвищого рівня за моделлю OSI – фізичним. На цьому рівні відбувається фізична передача бітів даних в безпровідному повітряному середовищі за допомогою технології Bluetooth. Оскільки типове обладнання обмежене наведеним, то фізичне обладнання також буде згідно технічної характеристики, а відповідно – схожим.

В даній роботі не розглядається розробка додаткового апаратного впливу, тому вважаємо що пристрої передачі даних справні та відповідні апаратні перетворення виконуються згідно заявленої NIST специфікації.

Технологія передачі Bluetooth побудована на використанні псевдовипадкового перелаштування робочої частоти в межах робочого діапазону. Зміна частоти відбувається з кроком 1 МГц кожну секунду 1600 разів. В обладнання влаштовано пристрій передачі 2 класу з споживанням 2.5 mW, та відстанню передачі до 10м. Частота контролюється гауссівською частотною модуляцією.

На вищому рівні – канальному відбувається отримання фізичних адресів обладнання користувачів А та Б. На цьому рівні обладнання позначене унікальною MAC адресою. За цією адресою пристрій визначається як віддалений та на основі цього створюється сокет. Використовується P-192 Elliptic Curve, E1/SAFER алгоритм аутентифікація пристроїв. Надалі обіг даних шифрується за допомогою E0/SAFER+.

На мережевому рівні відбувається робота сокета, покривається перетворення режиму передачі в RFCOMM.

5 основних послуг безпеки надає стандарт Bluetooth:

Аутентифікація: перевірка і ідентифікація комунікації пристроїв на сонові їхніх адрес;

Конфіденційність: тільки авторизовані пристрої можуть мати доступ і запрошувати передачу даних;

Авторизація: контроль підтвердження авторизації пристрою перед використанням сервісів;

Інтеграція повідомлень: перевірка надісланого повідомлення, що воно отримане;

Парування: створення хоча б одного таємного ключа для під’єднання до інших пристроїв на цій технології, зберігання цього ключа.

Режими безпеки пристроїв технології Bluetooth надаються на основі організації 4 режимів роботи і вказані в таблиці 2.2.

Таблиця 2.2 BR/EDR/HS режими безпеки

|  |  |
| --- | --- |
| Режим | Процедури безпеки відбуваються під час встановлення |
| 4 | Сервісу |
| 3 | З'єднання |
| 2 | Сервісу |
| 1 | Ніколи |

Аутентифікація і шифрування використовуються на режимі безпеки 2 і влаштовуються засобами контролера. Всі пристрої технології 2.0 і раніші, підтримують режим безпеки 2, але виконані за технологією 2.1 і новіше підтримують це в фоні на основі сумісності з раднішими пристроями.

Режим безпеки 3 є режимом з'єднання, в якому пристрої Bluetooth оперують процедурами безпеки на вже встановленому з’єднанні. Bluetooth пристрої оперують мандатною аутетифікацією і шифруванням для всіх з’єднань пристрою на цій технології.

Режим безпеки 4, як і 2 оперує SSP, ключом парування. Починаючи з Bluetooth версії 4.0 використовується P-192 Elliptic Curve для генерації ключів, а процедури аутентифікація і шифрування ідентичні тим які використовуються в Bluetooth версії 2.0 [91].

Починаючи з версії Bluetooth 4.1 надається послуги аутентифікація на основі алгоритму HMAC-SHA-256. А нові пристрої на основі технології Bluetooth 5.0 використовують приховування адресного ідентифікатора на режимі низького споживання енергії, а аутентифікація відбувається за умови наявності попередньої пари і порівнянням ключів.

На основі сказаного способи передачі ключів за технологією Bluetooth 4.0 не використовують достатньої безпечної передачі цих ключів підчас парування, чим активно користуються порушники. Щоб уникнути такого, потрібно створити такий обмін на вищих рівнях моделі OSI. Програмні засоби Android дозволяють використовувати процедури додаткової аутентифікація на сеансовому рівні.

Щоб уникнути передачі додаткового ключа аутентифікації через технологію Bluetooth, та в межах розробки програмного модуля, запропонуємо користувачу самостійно передавати такий ключ в кодованому вигляді.

**2.5.1 Метод експертної оцінки**

Оскільки цей метод об’єднує різні засоби впливу, то в свою чергу їх можна поділити за організацією впливу у відповідності до вчиненого впливу на життєвий цикл ТЗ. Потрібно пояснити, що життєвий цикл технічного засобу вживається в розумінні ступенів розвитку ТЗ. Це дослідження проблеми створення ТЗ, стратегічного планування життєвого циклу ТЗ, розробки специфікацій, розробки самого ТЗ, тестування, проведення сертифікації якості ТЗ, впровадження, підтримки підчас експлуатації, впровадження змін, яке також повторює попередні етапи, виведення ТЗ з експлуатації, завершення стратегії життєвого циклу ТЗ, проведення заключень по результатам звітів. Потрібно нагадати, що всі етапи життєвого циклу ТЗ тісно зв’язані між собою і включають нищі ступені опрацювання ТЗ з використанням наявного матеріально-технічного забезпечення та потенціалу розвитку. Оскільки значення безпеки є плаваючим значенням і постійно корегується відносними впливами різних чинників: політичним, економічним, культурним і соціальними рівнями життя, то процес розробки можна окреслити процес без кінцевої точки. На даних твердженнях покладено циклічну основу стадіям тестування, сертифікації і впровадження.

До індивідуального методу експертної оцінки програмного екземпляру дослідного середовища належать інструменти захисту інформації: специфікація, самотестування, політика і правила застосування засобів розробки, сертифікація, впровадження, експлуатаційна підтримка КЗІ, закінчення роботи з КЗІ, висновки щодо подальшої роботи.

Політика розробки програмного забезпечення для дослідного середовища та підбір апаратних засобів в повній мірі розглядається в попередніх розділах та формувалося під впливом чинного законодавчого стану та діючих положень. Зокрема основу Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації Державної служби спеціального зв'язку та захисту інформації від 20.04.2007 (надалі Положення). Проте згідно Положення пункту 7 абзацу 2, автор роботи не може провести сертифікацію програмного середовища. Згідно пункту 6 цього Положення, допускається розроблення такого ТЗ.  
Згідно пункту 8 Положення з чотирьох рівнів можливостей порушника визначено перший рівень — порушник має обмежені кошти та самостійно створює засоби, розробляє методи атак на засоби КЗІ, а також інформаційно-телекомунікаційні системи із застосуванням поширених програмних засобів те електронно-обчислювальної техніки. Згідно пункту 9 Положення програмний екземпляр належить до класу В1 - відповідає вимогам забезпечення стійкості криптоперетворення в умовах несанкціонованих дій з боку легального користувача системи (захист від порушника першого рівня);

Засіб КЗІ належить до підвиду Б2 - апаратні, апаратно-програмні або програмні вироби, які підключаються до інших засобів та виконують функції криптографічних перетворень у взаємодії з ними або під їх управлінням. Та за призначенням відноситься до категорії Ш — засоби шифрування інформації.

Розроблений зразок екземпляру програмного забезпечення є зразком для проведення дослідження та підпадає під вплив пункту 22 Положення.

Критерії оцінювання здатності системи організовувати необхідні рівні безпеки поділяються на 2 види: вимоги до захисту функцій, вимоги до гарантій. Далі наводиться оцінювання ТЗ до вимог НД-ТЗІ-2.5-004-99.

КД-1 Мінімальна довірча конфіденційність надається на основі засобів операційної системи Android на основі дозволів наданих від користувача для запущеного процесу мобільного додатка та роботі з оперативною пам’яттю.

Права на виконання процесу в середовищі операційної системи надає користувач і тільки він здатен змінювати права доступу мобільного додатку.

КО-1 Повторне використання об’єктів надається у вигляді захищеного цілісного і ізольованого середовища віртуальної машини Dalvik в якому виконується запущений процес. Процеси між собою взаємодіють через внутрішні віртуальні інтерфейси. Експорт чи імпорт інформації користувача відбувається засобами повторної ініціалізації об’єктів. Збирач сміття постійно вивільнює не використовувані об’єкти і ресурси.

КВ-1 Мінімальна конфіденційність при обміні надається дозволами користувача на обмін даними. Перед обміном інформація захищається.

ДР-1 Політика квот надається засобами операційної системи і керується програмно. Запити на зміну статусу ресурсів обробляються головним потоком процесів і розділяються від запущеного.

Тестування на стійкість до відмов не проводилось.

НР-1 Зовнішній аналіз надається інструментами самотестування операційної системи на основі політики заповнення звітів. Користувач не має доступу до звітів. Розробник має доступ до звітів і журналів мережевої трансляції.

НИ-1 Зовнішня ідентифікація і автентифікація. Розпізнання користувача вказують засоби запуску мобільного додатку. ТЗ використовує зовнішні ідентифікатори для ідентифікації мобільного додатку на наявному і віддаленому обладнанні.

НК-1 Однонаправлений достовірний канал організовується користувацьким інтерфейсом. Обмін інформацією спадкується від указівок користувача на інтерфейсі.

НО-3 Розподіл обов’язків на основі привілеїв організовується операційною системою методом окремого віртуального середовища, створення окремого користувача з його відповідними потоками середовища і потоком ТЗ. Користувач може підвищити права до адміністратора за умови втручання в налаштування середовища.

НТ-3 Самотестування в реальному часі працює на основі покрокового ініціювання віртуальних об’єктів у відповідності їхнім інтерфейсам. Результати тестування, якщо їх рівень належний, виводяться користувачу у вигляді виринаючи повідомлень. У випадку тестування в процесі розробки – це повні дані про етапи роботи мобільного додатку.

НВ-2 Автентифікація джерела даних відбувається при запиті на з’єднання з віддаленим пристроєм. Ідентифікація стану і відклику віддаленого ТЗ організовують відповідь на запит.

Вимоги до архітектури Г-4 доведено до вимог відділити критичні компоненти відділені від некритичних за рахунок організації програмно-апаратного середовища мобільного обладнання.

Детальний проект ТЗ не має відношення до розглядуваної роботи, тому принципи і політика розробки не вноситься.

Середовище функціонування відноситься до Г-3, оскільки точні початкові коди надано у вільний доступ, а програмно-апаратний комплекс обслуговується користувачем та гарантується відповідність вимогам специфікації.

Випробування та тестування в якості розглядуваного модуля не проводилися.

**2.2 Метод віднесеної оцінки**

Метод віднесеної оцінки в цій роботі використано з наслідуваним засобом впливу методу — сертифікації. Вживане тут значення сертифікації належить до загально прийнятих процедур сертифікації. При застосуванні до досліджуваного середовища сертифікація проводиться для ТЗ як об’єкту програмного забезпечення в поєднанні з апаратним комплексом та засобами комунікації, політики управління безпекою введення, виведення, трансформації і передачі інформації, правилами використання КЗІ.

Результатом експертизи є встановлення належності або не належності досліджуваного середовища до відкритого міжнародного стандарту ДСТУ ISO/IEC 27001:2015.

В розділі 1 цієї роботи розглянуто необхідність і особливості виконання середовища дослідження, що може послужити виконанням умов пунктів 4.1 -4.2 ДСТУ ISO/IEC 27001:2015. Сфера застосування системи управління інформаційною безпекою згідно пункту 4.3 згаданого стандарту є:

а) зовнішня та внутрішні обставини:

Автор бере на себе відповідальність за проектування, розробку та тестування TЗ “Silent Messenger”. Зовнішній вплив на ці етапи здійснюють вплив закони і положення, розглянуті в пункті 1.3.4 цієї роботи. Внутрішніми обставинами в межах цієї роботи є розгляд модуля ТЗ в межах екземпляра програмного забезпечення в межах розгляду досліджуваного середовища.

б) Зацікавленою стороною є розробник ТЗ з метою розгляду проблеми цієї роботи та встановлення висновків. Інші сторони допускаються до консультації щодо розгляду проблеми роботи, але повний вплив на здійснення ТЗ виконує розробник.

с) Вплив на організацію роботи виконує Міністерство освіти і науки України через Національний авіаційний університет в особі керівника дипломного проектування цієї роботи як сторона, яка здійснює нагляд за дотриманням вимог до оформлення робіт.

Автор, як розробник ТЗ в межах цієї роботи не зобов’язується розробляти і впроваджувати систему управління безпекою згідно пункту 4.4 вказаного стандарту.

Згідно розділу 5 ДСТУ ISO/IEC 27001:2015 керівником роботи є встановлений і діючий керівник дипломного проектування і здійснює безпосередній вплив на розробника ТЗ. Надалі наведено цілі заходів безпеки та заходи безпеки в трактуванню відповідного до додатку А ДСТУ ISO/IEC 27001:2015

А.5 Політики безпеки

А.5.1 Принципи управління інформаційною безпекою

Ціль: Забезпечити принципи управління та підтримку інформаційної безпеки згідно з вимогами завдання на дипломне проектування та відповідними законами й нормативами.

А.5.1.1 Політики інформаційної безпеки

Заходи безпеки організовуються на основі рекомендацій до виконання та оформлення дипломної роботи Національного авіаційного університету.

А.6 Організація інформаційної безпеки

А.6.1 Внутрішня організація

Ціль: Визначити структуру управління для започаткування та контрою впровадження та функціонування інформаційної безпеки під час проектування дипломної роботи.

А.6.1.1 Ролі та обов’язки щодо інформаційної безпеки

Автор дипломного проекту несе відповідальність за своєчасне виконання ТЗ в межах розгляду дипломного проекту.

Керівник згідно розкладу виконання дипломного проекту здійснює контроль за виконанням роботи.

А.6.1.2 Розподіл обов’язків

На автора дипломного проекту накладаються обов’язки інформувати керівника дипломного проекту у відведений час про стан виконання цієї роботи, уточнювати наявність внутрішніх положень, які можуть здійснювати вплив на розгляд і проектування ТЗ.

А.6.1.3 Контакти з повноважними органами не обмежуються керівником дипломного проектування та може бути залучена будь-яка особа в якості такої, що надає консультації, що не передумовлює матеріальним затратам чи нанесенню матеріальної шкоди яка прямо впливає на TЗ “Silent Messenger”.

А.6.1.4 Контакти з групами фахівців з певної проблематики.

TЗ “Silent Messenger” розробляється як вільний програмний засіб, на основі ліцензії GPLv3 і тому до консультації щодо проблемних питань залучаються спеціалісти з форуму stackoverflow.com, github.com.

А.6.1.5 Інформаційна безпека в управлінні проектами

В даній роботі застосовується єдиний проект, та на час проекту автор не працює над жодними іншими проектами, які б вимагали підтримання інформаційної безпеки.

А.6.2 Мобільне обладнання та віддалена робота

Ціль: Гарантувати безпеку віддаленої роботи та використання мобільного обладнання.

А.6.2.1 Політика щодо мобільного обладнання

В даній роботі використовується засоби зв’язку користувача в вигляді обладнання, яке повністю відповідає специфікації. TЗ “Silent Messenger” розповсюджується на вільній основі, проте без умов комерційного використання. Забезпечення умов використання ТЗ в складі обладнання користувача організовує користувач, та несе безпосередню відповідальність за захист або порушення своїх обов’язків. Перед використанням, користувач зобов’язаний ознайомитися та виконувати інструкцію щодо експлуатації TЗ “Silent Messenger”.

А.6.2.2 Віддалена робота

Віддалена робота над проектом надається у вигляді віддаленої роботи. Кожен вільний від інших обов’язків розробник або компетентна особа можуть надавати безоплатні консультації щодо проекту. Будь-яка шкода, нанесена у процесі виконання консультацій лягає на сторони автор і віддалений консультант, та стосується лише TЗ “Silent Messenger”. Віддалена співпраця відбувається на добровільній основі та не передбачає відшкодування шкоди, нанесеній в час виконання такої роботи, або в зв’язку з подальшим таким впливом. Автор не несе відповідальності за використання ТЗ іншими користувачами.

А.7 Безпека людських ресурсів

Розробка, експлуатація і провадження обслуговування TЗ “Silent Messenger” відбувається на вільних засадах і не передбачає найму в трактуванні національної примітки до цього розділу ДСТУ ISO/IEC 27001:2015.

А.8 Управління ресурсами СУІБ

А.8.1 Відповідальність за ресурси СУІБ

Ціль Ідентифікувати СУІБ організації і визначити відповідні обв’язки щодо їх захисту

А.8.1.1 Інвентаризація ресурсів СУІБ

Засоби захисту інформації не інвентаризуються.

А.8.1.2 Володіння ресурсами СУІБ

Визнається право власності на ТЗ “Silent Messenger” за автором роботи.

А.8.1.3 Припустиме використання ресурсів СУІБ

ТЗ “Silent Messenger” надається у вільному доступі і може бути використаний будь-якими сторонами.

А.8.1.4 Повернення ресурсів СУІБ

Повернення ТЗ “Silent Messenger” у вигляді інсталятора не проводяться. Натомість користувачем проводиться виведення з експлуатації та знищення ТЗ.

А.8.2 Класифікація інформації

Ціль: Забезпечити належний рівень захисту інформації відповідно до її важливості для організації

А.8.2.1 Класифікація інформації

Класифікація відбулася згідно НД-ТЗІ-2.5-004-99 в пункті 4.1 цієї роботи.

А.8.2.2 Маркування інформації не проводиться

А.8.2.3 Поводження з ресурсами СУІБ не впроваджується

А.8.3 Поводження з носіями – розділ не доцільно розглядати в межах ТЗ

А.9 Контроль доступу

Ціль: Забезпечити санкціонований доступ користувача і запобігти несанкціонованому доступу до системи та послуг

А.9.1 – А.9.3 Користувач авторизується в операційній системі, надалі параметри користувача наслідуються. Користувач обмежений в перегляді, виправленні, вилученні прав доступу до віртуального середовища.

А.9.4 Контроль доступу до системи та прикладних програм відбувається інструментами захисту наданої операційної системи.

А.10 Криптографія

А.10.1 Криптографічні засоби захисту

Ціль: Гарантувати відповідне та ефективне використання криптографії для захисту конфіденційності, автентичності та/або цілісності.

А.10.1.1 Політика використання криптографічних засобів не впроваджувалася

А.10.1.2 Управління ключами передбачено програмним кодом, але не введено в дію.

А.11 Фізична безпека та безпека інфраструктури в межах роботи не впроваджуються.

А.12 Безпека експлуатації встановлена на правилах експлуатації, інше не впроваджується в межах роботи.

А.13 Безпека комунікацій заснована на політиці застосування документованих засобів комунікації та їх характеристик.

А.14-А.17 Розробка, підтримка, збір доказів, тестування, поставка, безперервність продукту належать до бізнес процесів, які в роботі не визначені.

А.18 Відповідність правовим нормам розглянуто в якості приведених класифікацій та сертифікації цього розділу.

На сонові вказаної політики безпеки потрібно розробити відповідну інструкцію для користувача по експлуатації технічного засобу. Умовами для створення такої інструкції є вище згадуване Положення.

* 1. Загальні положення

Інструкція визначає організаційно-технічні заходи щодо захисту інформації при організації і експлуатації захищених сесій передачі інформації з використанням TЗ “Silent Messenger”. Порушення положень інструкції може привети до втрати та поушення конфіденційності інформації.

* 1. Вимоги до організаційного забезпечення безпеки експлуатації TЗ “Silent Messenger”

Згідно відкритої ліцензії GPLv3 заборонено використання програмного забезпечення в комерційних цілях та забезпечення передачі інформації яка буд-яким шляхм впливає на бізнес процеси. Організацією безпеки займається безпосередньо користувач TЗ “Silent Messenger” з моменту встановлення даного засобу на власне обладнання. З цього моменту TЗ “Silent Messenger” підпадає під формат КЗІ, в якому використовується до закінчення етапу виведення з експлуатації.

* 1. Вимоги до умов і правил експлуатації ТЗ “Silent Messenger”

З моменту запуску ТЗ “Silent Messenger” починається процес експлуатації даного ТЗ в складі умов КЗІ, які діють на даний момент. Користувач погоджується перевсти режими обладнання в пропоновані інтерфейсом програми. У випадку не прийняття цих правил, користувач зобовязується припинити експлуатацію даного програмного забезпечення та перейти до пункту виведення з експлуатації.

* 1. Порядок забезпечення безпеки TЗ “Silent Messenger” під час його встановлення, тестування, виведення з експлуатації, ремонту апаратної частини

Для гарантування безпеки особистої інформації користувача під час встановлення та експлуатації ТЗ організовано таким що не збирає, не зберігає та не здійсню обмін такою інформацією.

Перед використанням ТЗ користувач зобов’язується ознайомитися з специфікацією на TЗ “Silent Messenger” та привести апаратне і програмне середовище до такого, яке вказано в специфікації.

Встановлення відбувається виконанням інсталятора TЗ “Silent Messenger” у вигляді виконуваного файлу apk на апаратно-програмному пристрої користувача. Поточну і оновлену версію ТЗ можна знайти за адресою <https://github.com/D0kLabs/Silentmessenger/releases>.

Встановлення ТЗ проводиться на основі вказівок програмного середовища користувача. Перед початком експлуатації потрібно провести пошук та створення пар пристроїв з яким в подальшому буде здійснюватися обмін інформацією.

Тестування ТЗ відбувається засобами самотестування. Інформування користувача відбувається через користувацький інтерфейс короткочасними повідомленнями.

Порядок виведення з експлуатації встановлюються програмною оболонкою користувача.

У випадку ремонту апаратної чи програмної чистини а також обслуговування обладнання користувача, користувач зобов’язується привести програмно-апаратні характеристики свого обладнання до тих, які вказані в специфікації до TЗ “Silent Messenger”.

* 1. Порядок забезпечення безпеки КЗІ “Silent Messenger” під час експлуатації

З моменту успішного встановлення TЗ “Silent Messenger” користувач несе повну і безпосередню відповідальність за обмін інформацією, її суть і втрати, які можуть понести будь-які сторони в результаті неналежного виконання цієї інструкції.

Користувачу заборонено перешкоджати та вносити будь-які зміни в програмно-апаратну частину обладнання в час використання TЗ “Silent Messenger” оскільки це може нанести користувачу або іншим сторонами шкоду у вигляді втрати інформації та сукупної до неї шкоди.

* 1. Заходи у випадку підозри компрометації інформації передаваної за допомогою TЗ “Silent Messenger”, закінчення сеансу обміну інформацією.

Будь-який користувач може розірвати обмін інформацією. Рекомендується попередити про такі наміри інші сторони обміну інформацією.

Завершення роботи з ТЗ, що і є закінченням сеансу обміну інформацією є завершення роботи користувацького інтерфейсу та видалення програми з головного потоку черги програм.

Висновки до розділу 2

В даному випадку технічний засіб не відповідає вимогам ДСТУ ISO/IEC 27001:2015 в поаному обсязі та потребує доопрацювання в розділах, які не опрацьовані. Також в даному випадку наведено неправильну класифікацію по відношенню до ДСТУ ISO/IEC 27001:2015, оскільки одиночний програмний засіб, який не є виконаним повністю, та має не покриті загрози, вразливості та ризики, порівнюється з стандартом, який за вимогами стосується рівня організації. Також з цього випливає, що потрібний в даному випадку ДСТУ ISO/IEC 27013 повинен бути наведеним замість розглянутого, про що на даний час законодавство України не передбачено, та ДСТУ ISO/IEC 27013 у вільний доступ не надано, проте прийнято як діючий.

**РОЗДІЛ 3 МАТЕМАТИЧНИЙ АНАЛІЗ ОБМІНУ ПОВІДОМЛЕННЯМИ**

**3.1 Вибір алгоритму шифрування**

Безпровідне середовище в якому передається інформація сертифікованими пристроями здійснюється за вказівкою програмного забезпечення операційної системи проекту АОSP. Так, як специфіка захисту в каналі передачі диктується апаратними рішеннями гарантованими виробниками елементів мобільних телефонів, а також технологією Bluetooth, то єдиним незахищеним залишається власне дані, які передаються.

Отже користувач набирає текст в кодуванні ASCII довільної довжини.

Брюс Шнаєр[98] розглядає, що способами захисту даних повідомлення є перетворення, зміщення, кодування. Працівники безпеки інформації об’єднують такі способи як основні для методів шифрування: асиметричний і симетричний.

Асиметричний метод полягає у використанні над відкритим текстом деякої функції, яка породжена закритим ключем, у випадку дешифрування, і відритим ключем у випадку шифруванням. В силу організації обох пристроїв з однаковою конфігурацією обладнання, можна припустити, що підготовлений ключ на одній стороні буде розшифрований на іншій за умови синхронізації обладнання. Реальність же диктує, що в безпровідне середовище передачі потрібно буде відправити хоча б один ключ, відокремлений від інформації, і запропонований приймаючій стороні як ключ дешифрування.

Передача ключів є неприйнятною, оскільки маємо загрозу витоку каналу передачі сторонніми особами.

Симетричний метод полягає в розрахунку деякої пари ключів на основі розрахунків з великими числами, та накладання такого ключа як відкритого для шифрування чи закритого для розшифровування. Тобто дані передаються також з як мінімум одним ключем.

Пропонований спосіб передбачає шифрування способом переміщення і перетворення без передачі ключів в безпровідний канал зв’язку. Строкові послідовності для ініціалізації розшифрування надаються програмному забезпеченню від користувача. В такий спосіб можна повністю покласти відповідальність на користувача за управління безпекою повідомлення. Щоправда такий спосіб обумовлює цифрові послідовності Rі в рамки Ri=ASCII \* mEditText, де ASCII – таблиця міжнародного кодування символів, mEditText – строка введених символів.

Тобто для створення випадкової послідовності ключа розшифрування, користувачу потрібно самому придумати таку символьну послідовність. Потрібно звернути увагу, на те, що не всі алгоритми шифрів пропонують безпосереднє введення строки символів в якості ключа шифрування чи дешифрування. З розглядуваних відкритих алгоритмів симетричного шифрування[95]: Twofish, Serpent, AES, Blowfish, TDES (3DES). Кожен з цих шифрів можна використовувати в різних режимах роботи. З відкритих ресурсів автор дослідження зміг отримати Blowfish в вигляді імплементації на Java.

Алгоритм Blowfish використовує для внутрішніх перетворень S-блоки і P-блоки. S-блоки використовуються мають константний характер і використовуються для генерації зсуву байтів в межах блоку. Р-блок є результатом генерації числа з будь-якого значення. Отриманий алгоритм працює з 255\*8 масивами шіснадцяткових значень, які утворюють S-блок і 18\*8 масивами шіснадцяткових значень для Р-масиву. На вході відкритий текст в вигляді вибірки 18 шіснадцяткових значень тексту, на виході відповідно 32 шіснадцяткових значення шифротексту. На розкриття одної комбінації P – блоку необхідно 28\*16+1 підібраних відкритих текстів. Проте дана атака не відкриє ні готового S-блоку, ні P-блоку. Тому є пропозиція залишити S-блок статичним, а P-блок генерувати. В якості P-послідовності можна взяти строку, введену користувачем, і відповідно перетворену.

Отже отримаємо:

Pвх =144256 (hexascii);

Один символ це два значення шіснадцяткових. Для підвищення зручності передачі символів, оскільки засіб передачі – голос користувача А, потрібно стиснути строку. Допустимим і зручним вважається строка 4-12 символів. Стиснення можна запропонувати за допомогою алгоритмів безвтратного стиснення та кодування символів в інших даних. Для початку розглянемо кодування строки з довільної строки в 144 символи формату hex. В подальшому в проекті будуть використовуватися ідентифікатори пристрою, які також потрібно буде передати користувачу Б для організації обміну повідомлення, але в межах роботи приділимо увагу лише передачі за допомогою Bluetooth. Дане повідомлення відноситься до службових і також несе інформацію, яка характеризує обладнання на стороні користувача, який її згенерував і відправляє. Розкриття сторонній особі ідентифікаторів пристрою не несе жодного раціонального значення. Також ці значення можна отримати і іншими методами, наприклад стороннім програмним забезпеченням, про встановлення якого користувача згідно умов експлуатації повідомлено.

**3.3 Вибір алгоритмів стиснення**

При виконанні простої операції xor побайтово відбувається порівняння двох вхідних даних згідно таблиці xor. Так можна гарантувати прогнозований результат виконання операції. Ідентифікатори програмного середовища, модулів разом мають різну кількість символів, що повністю підходить як ресурс для кодування. Кожне встановлення операційної системи встановлює нові ідентифікатори. Для розглядуваної строки в 18\*8 символьних значень та змінної строки більше одного символа пропонований спосіб приховування P-масиву носить випадковий характер для кожного окремого екземпляру обладнання.

I = Idboard mod10 + Idbrand mod10 + Idcpu\_abi mod10 + Idmanufacturer mod10 + Idboard mod10 + Idmodel mod10 + Idproductmod10

Таким переліком ідентифікаторів гарантується, що порушник не запустив копію технічного засобу на окремому віртуальному середовищі з метою підстановки повідомлення, оскільки при запуску на розповсюджених продуктах віртуалізації дані параметри заповнюються нулями, про що проведено перевірку в алгоритмі виконання збору ідентифікаторів.

Розібємо масив по 8 hex значень c та проведемо почерговий xor:

Pi = ci(bin) + ci+1(bin) + … ci+8(bin);

Ki= I(bin) XOR Pi

Таких ітерацій буде 18 для кожного нового масиву, тому К буде довжиною в 18 символів.

Алгоритми безвтратного стиснення найкраще підходять для деформації передаваної строки. Алгоритм LZW зменшує строку з 18 символів до \_\_. Проте в такому випадку постає проблема читання такої строки перетворених символів. Для полегшення зчитування застосовується алгоритм RLE, що встановлює довжину строки приблизно рівній \_\_ символів. Алгоритм RLE об’єднує комбінації повторюваних символів у пару значень: цифрове значення кількості повторень та символ, який повторяється.

**Висновки до розділу 3**

В даному розділі розглянуто алгоритми кодування та стискання інформації для підвищення зручності передачі. Запропоновано використану модель шифрування і дешифрування в якості набору засобів впливу на інформацію – інструментів впливу. Проведено аналіз впливу цих інструментів та структуру на прикладі стиснення. Отримано кінцеві результати такого шифрування у вигляді довжини строки символів, які читаються і передаються користувачами.

#### ВИСНОВКИ

Результатом виконаної роботи є розроблений модуль мобільного додатку з впровадженим посиленим захистом обміну повідомленнями.

У процесі виконання роботи отримані наступні результати:

Розглянуто сутність захисту персональних даних, сучасний стан впровадження мобільних додатків захисту персональних даних та повідомлень;

Обґрунтовано доцільність створення програмного засобу захисту повідомлень в умовах сьогодення;

Проведено аналіз технологій розробки та функціональні можливості засобів розробки;

Створено прототип модуля мобільного додатку;

Проведено аналіз алгоритмів зазисту;

**Список використаної літератури**

1. Аналіз Закону України про захист персональних даних: DGI/DP/expertiseUKR(2012) / М. Жорж, Г. Саттон. – Страсбург: Рада Європи, 2012. – 63 с.

2. Бобрик В. І. Право власності на персональні дані [Електронний ресурс] / В. І. Бобрик // Вісник Хмельницького інституту регіонального управління та права. – 2002. – № 2. – С. 114–117.

3. Городиський І. М. Виконання Україною міжнародних зобов’язань із захисту персональних даних / І. М. Городиський // Інтеграція України в Європейське інформаційне суспільство: виклики та завдання / Упор. Пазюк А. В.; Рец. Гріненко О. О., Олійник О. В. – К.: ФОП Клименко, 2014. – С. 89–97.

4. Дмитренко О. А. Право фізичної особи на власні персональні дані в цивільному праві України [Текст]: автореф. дис. ... канд. юрид. наук: 12.00.03 / О. А. Дмитренко; НДІ приват. права і п-ва Акад. прав. наук України. – К., 2010. – 19 с.

5. Інтеграція України в Європейське інформаційне суспільство: виклики та завдання / Упор. Пазюк А. В. ; Рец. Гріненко О. О., Олійник О. В. – К.: ФОП Клименко, 2014. – 221 c.

6. Каретник О. С. Поняття інформації про фізичну особу (персональні дані) в цивільному праві України [Електронний ресурс] / О. С. Каретник // Часопис Київського університету права. – 2013. – № 2. – С. 228–231.

7. Косіцин М. Проблемні питання правового регулювання повноважень Держспецзв’язку України із захисту інформації про персональні дані / М. Косіцин, Е. Плешко // Прав., нормат. Та метрол. забезп. системи захисту інформації в Україні. – 2010. – Вип. 2. – С. 10–13.

8. Макушев П. В. Персональні дані як елемент системи інформаційного забезпечення державної виконавчої служби України / П. В. Макушев // Форум права. – 2013. – № 2. – С. 333–339.

9. Макушев П. В. Системи інформаційного забезпечення державної виконавчої служби України та персональні дані як їх складові / П. В. Макушев // Право і суспільство. – 2013. – № 4. – С. 70–76.

10. Оніщенко О. В. Персональні дані працівників: деякі особливості використання / О. В. Оніщенко // Вісник Академії адвокатури України. – 2012. – Число 3. – С. 173–175.

11. Пазюк А. В. Захист прав громадян у зв’язку з обробкою персональних даних у правоохоронній діяльності: європейські стандарти і Україна / А. В. Пазюк. – К.: МГО «Прайвесі Юкрейн», 2001. – 260 c.

12. Пазюк А. В. Міжнародно-правовий захист права людини на приватність персоніфікованої інформації: Автореф. дис... канд. юрид. наук: 12.00.11 / А. В. Пазюк; Київ. нац. ун-т ім. Т. Шевченка. – К., 2004. – 19 c.

13. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних / В. М.Брижко, А. І.Радянська, М. Я.Швець. – К.: Тріумф, 2006. – 256 с.

14. Посібник з європейського права у сфері захисту персональних даних. – К.: К.І.С., 2015. – 216 с.

15. Погребна А. Коментар до Закону України «Про захист персональних даних» / А. Погребна // Юридичний журнал. – 2010. – №7. – [Електронний ресурс]. Цит. 02.09.2010 р. Доступно з – <http://www.justinian.com.ua/article.php?id=3579>.

16. Романюк І. Особливості змісту та реалізації права на персональні дані в Україні та зарубіжних країнах / І. Романюк // Список рекомендованої літератури: Юридичні науки. – 2013. – Вип. 2. – С. 102–106.

17. Романюк І. І. Персональні дані особи як об’єкт цивільного обороту / І. І. Романюк // Право і суспільство. – 2014. – № 6.1(2). – С. 58–65.

18. Сопілко І. М. Генезис змісту категорії «персональні дані» / І. М. Сопілко // Юридичний вісник. Повітряне і космічне право. – 2013. – № 4. – С. 62–66.

19. Чанишев Р. І. Інформація про персональні дані працівника та її захист / Р. І. Чанишев // Актуальні проблеми держави і права. – 2010. – Вип. 52. – С. 94–99.

20. Чанишева Г. І. Право на інформацію за трудовим законодавством України: монографія / Г. І. Чанишева, Р. І. Чанишев. – О.: Фенікс, 2012. – 193 c.

21. Щербіна А. О. Персональні дані в системі інформаційного забезпечення органів місцевого самоврядування / А. О. Щербіна, П. В. Макушев // Публічне право. – 2013. – № 3. – С. 39–46.

22. Герберт Шилдт. Java. Полное руководство. –М.:Вильямс, 2012. – 1104 с.

23. Рето Майер. Android 4. Программирование приложений для планшетных компьютеров и смартфонов. – М.: ЄКСМО, 2013. – 816 с.

24. Документація Realm (Електрон. ресурс) / Спосіб доступу: URL: https://realm.io/ – Загол. з екрана.

25. Документація Git (Eлектрон. ресурс) / Спосіб доступу: URL: https://gitscm.com/. – Загол. з екрана.

26. Матеріал з Вікіпедії - вільної енциклопедії (Електрон. ресурс) / Спосіб доступу: URL:https://ru.wikipedia.org/wiki/Android\_Studio.

27. Документація Dagger (Eлектрон. ресурс) / Спосіб доступу: URL: https://google.github.io/dagger/. – Загол. з екрана.

28. Дэвид Гриффитс. Head First. Программирование для Android. – М.:Питер, 2016. – 704 с.

29. Пол Дейтел. Android для разработчиков. –М.:Питер, 2016. – 512 с.

30. Матеріал з Вікіпедії - вільної енциклопедії (Електрон. ресурс) / Спосіб доступу: <https://ru.wikipedia.org/wiki/Android>.

31. Матеріал з Вікіпедії - вільної енциклопедії (Електрон. ресурс) / Спосіб доступу: URL: <https://ru.wikipedia.org/wiki/Git>.

32. Habrahabr – «Структура приложения для Android» (Електрон. ресурс) / Спосіб доступу: URL: habrahabr.ru/company/ncloudtech/blog/274025/

33. Habrahabr – «Dagger 2. Часть первая» (Електрон. ресурс) / Спосіб доступу: URL: https://habrahabr.ru/post/279125/ 13 Habrahabr – «Dagger 2. Часть вторая» (Електрон. ресурс) / Спосіб доступу: https://habrahabr.ru/post/279641/

34. Скотт Чакон. Git для профессионального программиста. –М.:Питер, 2016. – 496 с.

35. Чад Фаулер. Программист-фанатик. –М.:Питер, 2016. – 208 с.

36. Стив Макконнелл. Совершенный код. Мастер-класс. – М.:Питер, 2016. – 896 с. 96

37. Эрих Гамма. Приемы объектно-ориентированного проектирования. Паттерны проектирования. – М.:Microsoft, 2016. – 366 с.

39. Роберт К. Мартин. Чистый код: создание, анализ и рефакторинг.. – М.:Питер, 2016. – 464 с.

40. Документація Java (Eлектрон. ресурс) / Спосіб доступу: URL: https://docs.oracle.com/javase/7/docs/api/. – Загол. з екрана.

41. Документація Android (Eлектрон. ресурс) / Спосіб доступу: URL: https://developer.android.com. – Загол. з екрана.

42. Шилдт, Г. Java. Полное руководство, 8-е изд. [Текст] / Г. Шилдт; пер. с англ. – М. : ООО “И.Д. Вильямс”, 2012. – 1104 с. : ил. – Парал. тит. англ. ISBN 978-5-8459-1759-1 (рус).

43. Etheridge David. Java, Graphical User Interfaces. David Etheridge & Ventus Publishing ApS, 2009. – 101 p.

44. Evans В.J., Verburg M. The Well-Grounded Java Developer: Vital techniques of Java 7 and polyglot programming. Manning Publications, 2012. - 496 P.

45. Goncalves A. Beginning Java EE 7. Apress, 2013. – 608 p.

46. Higuera-Toledano M.T., Wellings A.J. (eds.) Distributed, Embedded and Real-time Java Systems. Springer, 2012, -389 p.

47. Jendrock E. The Java EE 6 Tutorial: Basic Concepts. Prentice Hall, 2010. – 600 p.

48. Coward D. Java EE 7: The Big Picture: Master the Code, Applications, and Frameworks of Java Platform, Enterprise Edition 7. McGraw-Hill, 2015. – 512 p.

49. Gupta A. Java EE 7 Essentials. O'Reilly Media, 2013.– 362 p.

50. Pilgrim P.A. Java EE 7 Developer Handbook: Develop professional applications in Java EE 7 with this essential reference guide. Packt Publishing, 2013. – 634 p.

51. Эванс Б., Вербург М. Java. Новое поколение разработки. СПб.: Питер, 2014. – 560 с. 97

52. Сети М. Программирование игр. – М.: Вильямс, 100 книг, 2007. – 384 с.

53. Шилдт Г. Полный справочник по Java. – М.: Вильямс, 2009. - 1040 с. 33

54. Блинов И.Н. Java 2: практическое руководство / И.Н. Блинов, В.С. Романчик. – Мн.: УниверсалПресс, 2005. – 400 с.

55. Грофф Дж. Энциклопедия SQL. 3-е издание / Дж. Грофф, П. Вайнберг – М.: Вильямс, 2003. - 896 с.

56. Гарсиа-Молина Г. Системы баз данных. Полный курс / Г. ГарсиаМолина Дж. Ульман, Дж. Уидом – М.: Вильямс, 2003. – 1088 с.

57. Дашко Ю.В. Основы разработки компьютерных игр / Ю.В. Дашко, А.А. Заика. – М.: Форум, 2009. - 350с.

58. Роллингз Э. Проектирование и архитектура игр: пер. с англ. / Э. Роллингз, Д. Моррис. – М.: Вильямс, 2006.- 1040с.

59. Adamatzky A. (Ed.) Advances in Unconventional Computing. Volume 2. Prototypes, Models and Algorithms. – Springer International Publishing, 2017. – 812 p.

60. Albers V., Still B. (Eds.) Usability of Complex Information Systems: Evaluation of User Interaction. – CRC Press, 2011. – 392 p.

61. Arlow Jim, Neustadt Ila. Enterprise Patterns and MDA: Building Better Software with Archetype Patterns and UML. – Addison–Wesley Professional, 2004. 528 p.

62. Aslaksen E.W. Designing Complex Systems: Foundations of Design in the Functional Domain. – Auerbach Publications; 1 edition (October 27, 2008). – 176 p.

63. Baskerville R., De Marco M., Spagnoletti P. (Eds.) Designing Organizational Systems: An Interdisciplinary Discourse. – Springer, 2013 – 342 p.

64. Braun A.W. Enterprise Software Delivery. – Addison–Wesley, 2012. – 291 p.

65. Camp O., Filipe J.B.L., Hammoudi S., Piattini M. Enterprise Information Systems V. – Kluwer, 2005. –339 p.

66. Cheng B.H.C., de Lemos R., Paola H.G., Magee I.J. (eds.) Software Engineering for Self–Adaptive Systems. – Springer, 2009. –270 p.

67. Cruz–Cunha M.M. Social, Managerial, and Organizational Dimensions of Enterprise Information Systems. – IGI Global, 2010. –604 p.

68. Cruz–Cunha M.M., Varajago J. (Eds.) Enterprise Information Systems Design, Implementation and Management: Organizational Applications. – Information Science Reference, 2010. – 622 p.

69. Эккель Б. Философия Java. Библиотека программиста. 4-е изд.; пер. с англ. – СПб.: Питер, 2009. – 640 с.: ил.

70. Duggan D. Enterprise Software Architecture and Design: Entities, Services, and Resources. – Wiley, 2012. – 512 p

71. Evans Eric. Domain–Driven Design: Tackling Complexity in the Heart of Software. – Addison Wesley, 2003. – 560 р.

72. Архипин В.Я. Bluetooth. Технические требования. Практическая реализация 2. BLE – настольная книга разработчика, 1-е издание 3. http://developer.android.com/about/versions/android-4.0.html

73. Доля Android на рынке смартфонов [Електронний ресурс]: Ferra.ru – Режимдоступу:http://www.ferra.ru/ru/techlife/news/2014/01/30/strategyanalytics-2013-smartphone/#.U6DXXyjiLt0

74. Операційна система Google Android [Електронний ресурс]: ALLS.IN.UA – Режим доступу: http://alls.in.ua/13729-operacijjna-sistema-googleandroid.html

75. Языки программирования для Androidhttp [Електронний ресурс]: kakprosto.ru – Режим доступу://www.kakprosto.ru/kak-861348-yazykiprogrammirovaniya-dlya-android

76. Родной язык Андроида [Електронний ресурс]: toster.ru – Режим доступу: https://toster.ru/q/8860

77. Васильев А.Н. Java. Объектно-ориентированное программирование.Учебное пособие. – СПб.: Питер, 2011. – 400 с.: ил. 9. Новая среда разработки Android Studio [Електронний ресурс]: cnews.ru – Режим доступу: http://www.cnews.ru/top/2013/05/20/novaya\_sreda\_ razrabotki\_android\_studio\_sozdana\_na\_osnove\_rossiyskogo\_proekta529258

78. Android Studio – среда мобильной разработки на базе технологий JetBrains [Електронний ресурс]: soft.mail.ru – Режим доступу: http://soft.mail.ru/pressrl\_page.php?id=51774

79. Genymotion — лучший эмулятор Андроид на ПК [Електронний ресурс]: 4idroid.com – Режим доступу: http://4idroid.com/genymotion-luchshijemulyator-android-na-pk/

80. Genymotion — функциональный эмулятор Android для PC и Mac [Електронний ресурс]: androidinsider.ru – Режим доступу: http://androidinsider.ru/video/genymotion-funktsionalnyiy-emulyatorandroid-dlya-pc-i-mac.html

81. Этапы разработки [Електронний ресурс]: itech-mobile.ru – Режим доступу: http://itech-mobile.ru/stages.html 14.UX – это не UI [Електронний ресурс]: cmsmagazine.ru – Режим доступу: http://www.cmsmagazine.ru/library/items/usability/ux-is-not-ui/ 15.Ївженко C.М.,

82. Гафіатуліна І.В. Перша медична допомога. Методичні матеріали для викладачів БЖ ВНЗ [Текст] / Гафіатуліна І.В. – Полтава, 2004.

83. Роджерс Р., Ломбардо Д. Android. Разработка приложений [Текст] / Роджерс Р., Ломбардо Д. – М.: ЭКОМ Паблишерз, 2010. — 400 с.

84. ДБН В.2.5-28-2006. Природне і штучне освітлення.

85. ДСанПіН 3.3.2.007-98. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ЕОМ.

86. ДНАОП 0.00-1.31-99. Правила охорони праці під час експлуатації електронно-обчислювальних машин.

87. ДСН 3.3.6.037-99. Санітарні норми виробничого шуму, ультразвуку та інфразвуку.

88. ДСанПіН 3.3.6.096-2002. Державні санітарні норми і правила при роботі з джерелами електромагнітних полів

89. СНиП 2.09.02-85. Cтроительные нормы и правила производственные здания

* + 1. ДНАОП 0.00-1.21. Правила безпечної експлуатації електроустановок споживачів
    2. J Padgette, K Scarfone, L Chen - NIST Special Publication [Електронний ресурс]: https://nist.gov – Режим доступу: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf>
    3. Освітній сайт КНУБА. Архітектура та проектування програмного забезпечення [Електронний ресурс]: knuba.edu.ua – Режим доступу: [http://org2.knuba.edu.ua/pluginfile.php/28591/mod\_resource/content/1/ЛЕКЦІЯ\_1\_\_АП ПЗ\_Архітектура\_ПЗ.pdf](http://org2.knuba.edu.ua/pluginfile.php/28591/mod_resource/content/1/ЛЕКЦІЯ_1__АП%20ПЗ_Архітектура_ПЗ.pdf)
    4. Репозиторій Github [Електронний ресурс]: github.com – Режим доступу: <https://github.com/D0kLabs/Silentmessenger>
    5. Documentation for app developers [Електронний ресурс]: developer.android.com – Режим доступу: <https://developer.android.com/docs>
    6. Електронна енциклопедія Wikipedia [Електронний ресурс]: wikipedia.org – Режим доступу: <https://uk.wikipedia.org/> wiki/Шифрування\_з\_симетричними\_ключами
    7. Електронна енциклопедія Wikipedia [Електронний ресурс]: wikipedia.org – Режим доступу: <https://uk.wikipedia.org/wiki/LineageOS>
    8. Motorola DROID 4 XT894 [Електронний ресурс]: www.niora.net – Режим доступу: <https://www.niora.net/en/p/motorola_droid_4_xt894>
    9. Б. Шнайер Прикладная криптографія: протоколы, алгоритмы, и исходный код на С, 2е-юбил. издание.: Пер.с англ. – СПб.:ООО «Диалектика», 2019-1040с.
    10. [Lineageos](https://www.cvedetails.com/vendor/16630/Lineageos.html) : Security Vulnerabilities [Електронний ресурс]: www.cvedetails.com – Режим доступу: https://www.cvedetails.com/vulnerability-list/vendor\_id-16630/Lineageos.html
    11. Електронна енциклопедія Wikipedia [Електронний ресурс]: wikipedia.org – Режим доступу: <https://uk.wikipedia.org/wiki/Віртуалізація_на_рівні_операційної_системи>
    12. Форум Хабр [Електронний ресурс]: habr.com – Режим доступу: https://habr.com/ru/company/drweb/blog/484664/