ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УНІВЕРСИТЕТ ЕКОНОМІКИ ТА ПРАВА «КРОК»

КВАЛІФІКАЦІЙНА РОБОТА

Тема: «Гнучке управління розробкою мобільного застосунку Blur»

Ступінь вищої освіти – магістр

Спеціальність – 073 «Менеджмент»

Освітня програма «Agile-технології розробки програмного забезпечення»

ПОЯСНЮВАЛЬНА ЗАПИСКА

Керівник: зав. кафедрою, к.е.н., доцент
Денис БАЛДИК

Керівник: доцент, к.ф-м.н.
Іван КРИКУН

Виконав: здобувач
групи МЕН/Agile-23м
Андрій ГЛИБЧЕНКО

Київ, 2024 р.

ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УНІВЕРСИТЕТ ЕКОНОМІКИ ТА ПРАВА «КРОК»

ЗАТВЕРДЖУЮ:
завідувач кафедри інформаційного менеджменту, математики та статистики
_____ Денис БАЛДИК
«___»_____20__ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
ГЛИБЧЕНКА АНДРІЯ ОЛЕКСІЙОВИЧА

Тема роботи	ГНУЧКЕ УПРАВЛІННЯ РОЗРОБКОЮ МОБІЛЬНОГО ЗАСТОСУНКУ BLUR
Номер та дата наказу про затвердження теми	№56-6 від 27.06.2024
Коротка постановка завдання	Впровадження та розробка гнучкого підходу до управління розробкою захищеного мобільного застосунку
Посилання на джерела інформації (не більше п’яти найменувань, які рекомендує науковий керівник)	Системи та методи прийняття рішень: методичні вказівки / С. М. Мічківський, Р. Ю. Подольський, Т.К. Талапов. - Старобільськ: ЛНАУ, 2020.- 80 с Розробка програмного забезпечення з використанням баз даних: навчальний посібник / Ю. В. Шамарін, С. М. Мічківський, К. В. Смоктій, Д. В. Шевцов. – Донецьк: ДонНУ, 2013. – 201 с.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має містити теоретичне та/або практичне дослідження за темою роботи, яку слід розглядати як складне спеціалізоване завдання або практичну проблематику в галузі управління та адміністрування, яка характеризується комплексністю та невизначеністю умов і потребує застосування теорій і методів Agile технологій.

Дата видачі завдання « 14 » липня 2024 р.

Керівник Денис БАЛДИК

Керівник Крикун Іван

Здобувач Андрій ГЛИБЧЕНКО

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання	Примітка
Підготовчий етап			
1	Вибір напряму дослідження та керівника	01.07.2024 р.	виконано
2	Формування теми та призначення керівника	08.07.2024 р.	виконано
3	Затвердження теми кваліфікаційної роботи	09.07.2024 р.	виконано
4	Затвердження завдання на кваліфікаційну роботу	15.07.2024 р.	виконано
Основний етап			
5	Розробка концепції кваліфікаційної роботи	22.07.2024 р.	виконано
6	Підбір та вивчення джерел інформації з напряму дослідження. Огляд існуючих аналогів.	29.07.2024 р.	виконано
7	Затвердження розширеної постановки завдання. Підготовка та подання керівнику розділу 1 кваліфікаційної роботи	18.09.2024 р.	виконано
8	Проєктування інформаційної системи. Підготовка та подання керівнику розділу 2 кваліфікаційноїроботи	18.09.2024 р.	виконано
9	Реалізація інформаційної системи. Підготовка та поданнякерівнику розділу 3 кваліфікаційної роботи	25.09.2024 р.	виконано
10	Підготовка та подання керівнику першого варіанту всієїкваліфікаційної роботи	01.10.2024 р.	виконано
11	Доопрацювання кваліфікаційної роботи з урахуванням зауважень керівника та представлення керівнику доопрацьованого варіанту кваліфікаційної роботи	04.10.2024 р.	виконано
Завершальний етап			
12	Представлення рукопису для перевірки на плагіат	07.10.2024 р.	виконано
13	Підготовка презентації та доповіді на передзахист	07.10.2024 р.	виконано
14	Передзахист кваліфікаційної роботи	08-11.10.2024 р.	виконано
15	Технічна самоекспертиза роботи на відповідність вимогам до оформлення та виправлення недоліків	08-11.10.2024 р.	виконано
16	Експертиза роботи керівником та зовнішнім експертом	14.10.2024 р.	виконано
17	Доопрацювання доповіді та презентації для захисту	18.10.2024 р.	виконано
18	Захист кваліфікаційної роботи	21-25.10.2024 р.	виконано

Керівник Денис БАЛДИК

Керівник Крикун Іван

Здобувач Андрій ГЛИБЧЕНКО

Глибченко А.О. Гнучке управління розробкою захищеного мобільного застосунку для військових комунікацій в рамках проєкту Blur.

Кваліфікаційна випускна робота на здобуття ступеня вищої освіти магістра за спеціальністю 073 – Менеджмент. – ВНЗ «Університет економіки та права «КРОК», Навчально-науковий інститут інформаційних та комунікаційних технологій, кафедра математичних методів та статистики, Київ, 2024.

В ході виконання роботи було проаналізовано ключові аспекти планування та управління розробкою мобільного застосунку для захищеної комунікації. Було обрано методологію Agile з фреймворком Scrum, що дозволило гнучко адаптувати процес розробки до змінних вимог. Окрему увагу приділено питанням захисту інформації, що є критично важливим для військових підрозділів. Використано діаграму Ганта для планування етапів розробки та контролю строків виконання завдань. У результаті роботи створено прототип мобільного застосунку, що забезпечує високий рівень захисту даних.

Ключові слова: менеджмент, комунікації, застосунок, інформаційна безпека, Agile, Scrum, діаграма Ганта, шифрування.

Табл. 2. Рис. 5. Бібліограф.: 18 найм.

Hlybchenko A.O. Agile management of the development of a secure mobile application for military communications within the “Blur” project.

Qualifying final work for obtaining a master’s degree in higher education by specialty 073 – Management. – “KROK” University, Educational and Scientific Institute of Information and Communication Technologies, Department of Mathematical Methods and Statistics, Kyiv, 2024.

In the course of this work, key aspects of planning and managing the development of a secure communication mobile application were analysed. The Agile methodology with the Scrum framework was chosen, allowing for a flexible adaptation of the development process to changing requirements. Special attention

was paid to information security, which is critically important for military units. The Gantt chart was used to plan development stages and control task deadlines. As a result, a prototype of a mobile application was created, ensuring a high level of data protection.

Keywords: management, communications, application, information security, Agile, Scrum, Gantt chart, encryption.

Tables: 2. Figures: 5. References: 18 items.

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

PM – Project Manager

QA – Quality Assurance

UI – User Interface

UX – User Experience

API – Application Programming Interface

iOS – операційна система від Apple для мобільних пристроїв

Android – операційна система для мобільних пристроїв

MVC – Model-View-Controller

SQL – Structured Query Language

Agile – гнучка методологія розробки програмного забезпечення

Scrum – фреймворк для управління проєктами в рамках Agile

VPN – Virtual Private Network

AES – Advanced Encryption Standard

E2EE – End-to-End Encryption

ВСТУП

Актуальність теми. Проблема захисту інформації в сучасному світі надзвичайно загострена, оскільки в міжнародному полі можливі витоки інформації є прямою загрозою національній безпеці та суттєво впливають на різні сфери діяльності держав. Особливо актуально це питання постає у військовій сфері, де захист даних і конфіденційність інформації є одним з головних пріоритетів. Комунікація між військовими підрозділами повинна залишатися захищеною від зовнішніх впливів, адже витік інформації може призвести до надзвичайно серйозних наслідків не лише для окремих осіб, а й для всієї операції загалом. Саме тому розробка сучасних технологічних рішень, які забезпечують високий рівень захисту даних, стає актуальним завданням у сфері інформаційної безпеки.

Створення безпечних каналів комунікації є важливим напрямом у розвитку інформаційних технологій для військових потреб. Традиційні методи захисту інформації часто не відповідають сучасним вимогам безпеки, особливо в умовах швидких змін у технологіях та розвитку методів кібератак. Військові потребують спеціалізованих рішень, що дозволяють зберігати інформацію виключно на пристроях користувачів та передавати її з мінімальними ризиками під час комунікації.

Мета дослідження. Метою даного дослідження є розробка та впровадження безпечного застосунку для військової комунікації з використанням гнучкої методології Agile, що забезпечить високий рівень захисту даних під час передачі інформації між користувачами в умовах військових операцій.

Завдання дослідження. З огляду на ці особливості, проєкт "Blur" вирішує поставлене перед ним завхдання, а саме забезпечення високого рівня безпеки під час комунікацій між військовими та зниження ризиків витоку надважливих даних. Основний акцент у проєкті зроблено на використанні сучасних інструментів захисту інформації та впровадженні гнучких підходів

до розробки, зокрема методології Agile [1]. Це дозволяє не лише створити продукт, що відповідає вимогам безпеки, але й забезпечити швидке реагування на зміни, які можуть виникати в процесі розробки та експлуатації застосунку.

На етапі дослідження було проведено аналіз наявних рішень у сфері інформаційної безпеки та виявлено, що більшість із них не відповідає сучасним вимогам військових операцій. Зокрема, часто використовуються загальні рішення для середньостатистичних користувачів, що не враховують специфіку роботи військових підрозділів. Саме це стало передумовою для розробки інноваційного рішення з високим рівнем захищенності, яке дозволить військовим здійснювати комунікацію.

Об’єкт дослідження. Об’єктом дослідження є процеси управління розробкою програмного забезпечення з використанням методології Agile [2], орієнтовані на створення безпечних рішень для військових структур.

Застосування методології Agile в процесі розробки застосунку "Blur" стало ще однією важливою особливістю проєкту. Agile підходи дозволяють гнучко реагувати на змінні вимоги, які часто виникають у процесі розробки складних технологічних рішень. Відповідно, це сприяє більш швидкому та якісному створенню продукту, що відповідає високим стандартам безпеки.

Особлива увага приділяється тому, щоб розроблений застосунок відповідав специфічним вимогам військових щодо захищеності інформації та зручності у використанні. Застосунок "Blur" має функціонал, що дозволяє зберігати дані виключно на пристроях користувачів, запобігаючи будь-яким витокам через мережеві підключення. Це досягається завдяки впровадженню найсучасніших методів шифрування та безпечної передачі даних.

Новизна результатів дослідження. Новизна дослідження полягає у створенні інноваційного рішення для безпечної комунікації у військових умовах, яке поєднує сучасні методи інформаційної безпеки з гнучким підходом до управління розробкою. За допомогою сучасних технології шифрування та зберігання даних на пристроях користувачів, використання

цього застосунку мінімізує ризики витоку інформації через бази даних чи інші точки централізованого доступу.

Відповідно до сучасних вимог безпеки, ефективне управління процесом розробки також є важливою складовою успішного впровадження таких продуктів, як застосунок "Blur". Саме тому було вирішено використовувати Agile як основний підхід до управління проєктом. Це дозволило не лише вчасно реагувати на зміни у вимогах, але й забезпечити максимально швидкий цикл розробки та тестування продукту.

Практичне значення результатів дослідження. Розроблений застосунок може бути використаний у різних військових операціях для забезпечення безпеки комунікацій. Він може стати основою для подальшого розвитку інформаційно-безпекових технологій, зокрема у військовій сфері.

Проведене дослідження також виявило ряд важливих аспектів, пов’язаних з використанням гнучких методологій у процесі розробки програмного забезпечення для військових потреб. Це дозволяє забезпечити ефективну співпрацю між командами розробників та користувачів продукту, що є ключовим елементом у створенні безпечних та функціональних рішень.

Таким чином, робота над проєктом "Blur" спрямована на вирішення гострих проблем інформаційної безпеки у військовій сфері, а також на впровадження сучасних підходів до розробки захищених додатків. Впровадження цього рішення дозволить не лише покращити комунікацію між військовими підрозділами, але й забезпечити збереження важливих даних, що є надважливим у сучасних умовах проведення війни.

Структура та обсяг роботи. Робота складається зі вступу, трьох розділів, висновків до розділів, загального висновку, списку посилань та додатків. Загальний обсяг роботи 58 сторінок, обсяг основного тексту 53 сторінок.

РОЗДІЛ 1. ДИЗАЙН БІЗНЕСУ ТА ПОСТАНОВКА ЦІЛЕЙ ПРОЄКТУ

1.1 Опис предметної області та аналіз проблеми комунікації

Предметна область проєкту “Blur” охоплює сферу інформаційної безпеки та комунікаційних технологій, орієнтованих на військові потреби. У сучасних умовах збройних конфліктів та підвищених вимог до захисту даних питання безпечної комунікації набуває особливої актуальності. Комунікація між військовими підрозділами вимагає не лише швидкості та надійності, але й абсолютної конфіденційності, що мінімізує ризики витоку інформації та можливих втручань.

Однією з головних проблем, яка виникає у процесі комунікації між військовими підрозділами, є недосконаліть наявних засобів зв’язку, які часто використовують загальні канали передачі даних. Ці канали можуть бути вразливими до кібератак або перехоплення, що створює додаткові загрози безпеці. Військові операції вимагають від засобів комунікації не лише високого рівня захисту, але й стійкості до зовнішніх загроз, таких як атаки на мережі чи спроби витоку інформації з пристроїв користувачів.

Зважаючи на специфіку військових операцій, існуючі рішення часто не відповідають вимогам безпеки. Використання хмарних сервісів або незашифрованих каналів зв’язку створює додаткові ризики. Крім того, велика кількість користувачів та динаміка військових операцій потребує максимальної ефективності та швидкості комунікації без жодних затримок. У випадку використання загальних сервісів або ненадійних рішень, виникає ризик втрати або викривлення секретної інформації, зокрема через витоки баз даних чи інших централізованих сервісів [3].

Проєкт “Blur” виник у відповідь на цю проблему та передбачає створення застосунку, що дозволяє здійснювати прямі комунікації з високим рівнем захисту даних. Основний акцент ставиться на використанні сучасних

технологій шифрування, а також на збереженні інформації виключно на пристроях користувачів. Це рішення дозволяє мінімізувати будь-які ризики, пов’язані з витоком інформації через мережу чи під час передачі даних.

1.2 Постановка цілей та завдань проєкту

Основною метою проєкту “Blur” є створення високонадійного застосунку для військової комунікації, що здатен забезпечити безпечний обмін даними між військовими підрозділами під час виконання оперативних завдань. Головний акцент робиться на максимальну безпеку переданих даних та захист від можливих кібератак, перехоплення інформації або несанкціонованого доступу до комунікацій. Застосунок має відповідати найвищим стандартам захисту, гнучкості в адаптації до змінних умов і простоті використання, що є критично важливим для військових користувачів у реальних польових умовах.

Однією з основних цілей проєкту є інтеграція сучасних технологій шифрування для забезпечення повної конфіденційності переданих даних. Передбачається, що застосунок використовуватиме наскрізне шифрування (end-to-end encryption) (рис. 1.1), завдяки якому інформація передаватиметься між пристроями користувачів у зашифрованому вигляді, без можливості доступу до неї ззовні.

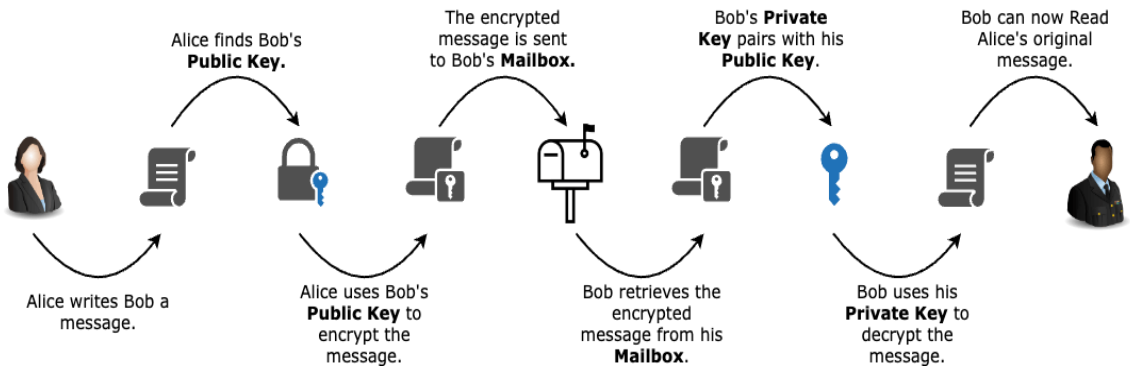


Рисунок 1.1 – Даграма наскрізного шифрування / End-to-End

Джерело: [4]

Це дозволить мінімізувати ризики втручання з боку третіх осіб, що особливо важливо в умовах активних військових операцій. Впровадження таких технологій має забезпечити захист повідомлень від перехоплення, навіть у випадках спроб атак на мережеву інфраструктуру.

Ще однією важливою метою є гарантування надійності роботи застосунку в умовах різноманітних загроз, включаючи мережеві перебої або низьку якість зв’язку. Застосунок повинен забезпечувати стабільність передачі даних навіть у ситуаціях, коли доступ до інтернету нестабільний, що часто трапляється під час активних військових дій та у місцях наближених до лінії фронту. Забезпечення безперебійної роботи застосунку в таких умовах потребує оптимізації протоколів передачі даних та використання надійних алгоритмів компресії і передачі інформації.

Проєкт також ставить перед собою завдання інтеграції застосунку з існуючими системами військових зв’язків і комунікацій. Це забезпечить ефективну взаємодію застосунку з іншими інструментами, які використовуються військовими підрозділами, та сприятиме його ширшому впровадженню в операційні процеси. Така інтеграція має на меті забезпечити зручність використання продукту без необхідності змінювати існуючі системи зв’язку.

Гнучкість застосунку також є однією з ключових цілей проєкту. Оскільки вимоги до військових операцій можуть змінюватися залежно від тактичної ситуації, застосунок повинен швидко адаптуватися до нових умов використання. Ця гнучкість досягається через впровадження Agile-методології управління розробкою, що дозволяє швидко реагувати на змінні вимоги користувачів, проводити регулярні тестування та вдосконалювати продукт на основі отриманих відгуків.

Впровадження Scrum як частина методології Agile додає гнучкості та оперативності в роботі команди при виконанні поставлених спринтів, підтримки чи оперативного зміни вектора розробки [5].

Завдання проєкту полягають у забезпеченні максимальної зручності використання застосунку для кінцевих користувачів. Інтерфейс повинен бути простим, інтуїтивно зрозумілим, щоб військові могли швидко опанувати продукт без тривалого навчання або технічної підготовки. Це особливо важливо в умовах швидкоплинних операцій, де час реакції має критичну вагу і де задтримка для розуміння складних налаштувань може призвести до втрати ініціативи або тактичної переваги.

Крім того, однією із важливих задач є забезпечення можливості швидкого видалення переданих даних з пристроїв. У випадку втрати пристрою або потрапляння його до рук противника, застосунок повинен мати функцію знищення всіх збережених даних без можливості їхнього відновлення. Це гарантує додатковий рівень безпеки, зберігаючи конфіденційність та знижуючи ризик використання важливих даних ворогом навіть у критичних ситуаціях.

Усі ці завдання мають на меті створення максимально надійного, безпечного та зручного продукту, який стане надійним інструментом для забезпечення захищеної комунікації в воєнних умовах. Проєкт “Blur” поєднує сучасні технології захисту інформації з гнучкими підходами до розробки, що дозволяє адаптувати продукт до змінних вимог і забезпечити високий рівень захищеності даних.

1.3 Визначення вимог до продукту

Проєкт “Blur” ставить перед собою мету розробити застосунок для військової комунікації, що забезпечує вищий рівень безпеки даних серед наявних та доступних на ринку та з можливістю подальшого векторного розвитку згідно потреб військових. Визначення вимог до продукту є ключовим етапом, оскільки від їх точності та повноти залежить ефективність реалізації проєкту. Вимоги до застосунку “Blur” були сформовані на основі аналізу

специфічних потреб військових підрозділів, загроз інформаційній безпеці та сучасних технологій захисту даних.

Основні вимоги до продукту можна розділити на функціональні та нефункціональні. Функціональні вимоги включають необхідний функціонал застосунку, який забезпечуватиме виконання завдань комунікації, а нефункціональні вимоги визначають критерії якості, безпеки та продуктивності.

Функціональні вимоги:

- застосунок повинен забезпечувати захищену передачу повідомлень у режимі реального часу;

- інформація, що передається, має бути шифрованою на обох кінцях комунікації (end-to-end encryption);

- застосунок повинен дозволяти голосові та текстові комунікації, а також передачу файлів (медіа та аудіо форматів) з мінімальними затримками;

- інтерфейс користувача має бути інтуїтивно зрозумілим і простим у використанні, що дозволить військовим підрозділам швидко адаптуватися до продукту;

- повідомлення та файли мають автоматично видалятися після певного періоду часу або за ініціативи користувача, забезпечуючи додатковий рівень конфіденційності;

- застосунок має бути інтегрований з існуючими протоколами військових комунікацій, а також мати імпорт даних існуючих проєктів типу “Кропива” [6], забезпечуючи безшовну роботу в польових умовах.

Нефункціональні вимоги:

- застосунок повинен забезпечувати високий рівень стійкості до кібератак, включаючи атаки на мережеву інфраструктуру та спроби перехоплення даних;

- платформа повинна працювати автономно, забезпечуючи збереження всіх даних локально на пристроях користувачів без їх передачі на сервери;

- продукт має бути легко масштабованим, для можливості застосування його у великих військових операціях з численними користувачами;

- безперебійність роботи застосунку повинна бути забезпечена навіть у складних умовах зв’язку (низька швидкість інтернету, відсутність стабільного сигналу);

- продукт повинен забезпечувати сумісність із широким спектром мобільних пристроїв, що використовуються військовими.

Формування вимог до продукту здійснюється на основі тісної співпраці з кінцевими користувачами — військовими підрозділами, що допомагає точніше визначити ключові функції, необхідні для ефективної роботи застосунку. Окрім того, вимоги постійно оновлюються під час розробки продукту в рамках гнучкої методології Agile, що дозволяє своєчасно реагувати на нові виклики та адаптувати застосунок до змін у потребах користувачів.

1.4 Визначення потреб у ресурсах та їх оптимізація

Для успішної реалізації проєкту “Blur” важливим етапом є правильне визначення потреб у ресурсах та їх оптимізація. Використання ресурсів у проєкті є критичним аспектом, оскільки від цього залежить ефективність процесу розробки, а також якість кінцевого продукту. Основними ресурсами, необхідними для реалізації проєкту, є людські ресурси, технологічні ресурси та фінансові ресурси [7].

Для успішної розробки застосунку “Blur” необхідна команда фахівців, кожен з яких виконує конкретні функції, забезпечуючи загальну ефективність процесу розробки продукту на різних етапах. Важливо також обрати висококваліфікованих спеціалістів, оскільки від їхніх знань та досвіду залежить не лише якість розробки, але й здатність швидко реагувати на складні технічні виклики, впроваджувати сучасні інноваційні рішення та дотримуватися високих стандартів інформаційної безпеки. Правильно підібрана команда фахівців забезпечить не тільки продуктивність і гнучкість

у процесі роботи, але й гарантуватиме стабільну та захищену роботу продукту, що є критично важливим для військових комунікацій.

Мінімальний очікуваний перелік людського ресурсу можна побачити на табл. 1.1, загалом можна розділити за вектором роботи на технічні та нетехнічні позиції.

Таблиця 1.1 – Очікувані людські ресурси по позиціям

Технічний персонал	Нетехнічний персонал
Технічний керівник	Менеджер проєкту
Розробники-архітектори	UI / UX дизайнери
iOS / Android / Backend розробники	Бізнес-аналітики
Тестувальники	Маркетологи
Оператори технічної підтримки	Бухгалтери
Експерти з кібербезпеки	Психолог

Згідно вищезазначеної таблиці можемо окреслити сектори впливу та обов’язки для кожної ролі:

Менеджер проєкту (Project Manager):

- розробку плану проєкту, що охоплює всі етапи робіт, строки та ресурси;

- контроль витрат та виконання бюджету проєкту;

- регулярне коригування плану-графіку проєкту відповідно до нових вимог чи змін;

- забезпечення дотримання термінів розробки та якості виконуваних робіт;

- управління комунікацією між командами та забезпечення вирішення конфліктів;

- узгодження змін з керівництвом та іншими зацікавленими сторонами.

Розробка застосунку залучає кілька галузей та напрямків в розробці ПЗ, кожен з яких займається реалізацією різних аспектів кінцевого продукту.

Командний / Технічний керівник (Team / Tech Lead):

- оцінка технічних рішень, вибір технологій / фреймворків для реалізації проєкту;
- керування процесом розробки та вирішення технічних проблем в команді;
- проведення код-рев'ю для забезпечення якості коду, дотримання загального стилю коду;
- підтримка комунікації між членами команди та сприяння обміну знаннями.

Розробник-архітектор (Software Architect):

- проектування архітектури продукту з урахуванням вимог безпеки та гнучкості;
- забезпечення масштабованості, можливості різноманітних тестувань, розширення та стійкості продукту;
- співпраця з командою для узгодження архітектурних рішень та їхнього впровадження.

iOS / Android розробник:

- розробка застосунку для iOS / Android з урахуванням особливостей мобільної платформи;
- впровадження нових функцій та підтримка існуючих компонентів застосунку;
- забезпечення регулярного та оперативного оновлення застосунку для підтримки його сумісності з новими версіями iOS / Android та безпековими оновленнями;

- взаємодія з іншими розробниками, інтеграції з бекенд API та сервісами автентифікацій / авторизації.

Backend розробник:

- проєктування і реалізація серверних API для обміну даними з додатком;

- забезпечення високого рівня безпеки серверної частини застосунку та менеджера звернень;

- управління базами даних, побудова зв’язків, нормалізація, оптимізація їх продуктивності;

- тестування, оновлення та налагодження серверної частини застосунку.

Експерти з інформаційної безпеки:

- тестування застосунку на стійкість до кібератак (пентестинг, ін’єкційні тести, UI-скрепінг, перевірки на витоки пам’яті (memory leak) та сканування вразливостей);

- впровадження та налаштування протоколів шифрування для захисту даних;

- аналіз загроз, статистичний аналіз та рекомендації щодо покращення захисту застосунку;

- забезпечення точної відповідності застосунку міжнародним стандартам інформаційної безпеки.

UI / UX дизайнери:

- розробка інтуїтивно зрозумілого дизайну інтерфейсу, що полегшує роботу військових користувачів;

- забезпечення зручності навігації та доступності ключових функцій застосунку;

- узгодження дизайну з брендовими стандартами та рекомендаціями щодо мобільних інтерфейсів;

- створення макетів та прототипів для узгодження з командою розробки.

Тестувальники (QA):

- створення сценаріїв тестування для виявлення можливих помилок та недоліків у функціонуванні застосунку;

- проведення автоматизованого та ручного тестування застосунку;

- документування знайдених помилок та їх передача розробникам для виправлення;

- перевірка безпеки застосунку, його стійкості до навантажень та швидкості роботи.

Бізнес-аналітики:

- збір і документування вимог до функціоналу продукту;

- аналіз ринку та конкурентних рішень для визначення можливих шляхів розвитку продукту;

- координація між командами технічної та бізнесової частини для ефективної реалізації вимог.

Маркетологи та бухгалтери:

- створення маркетингових матеріалів і стратегій для просування продукту;

- оцінка ринкових перспектив та аналіз потенційних користувачів;

- ведення фінансової звітності та контроль за витратами проєкту.

Оператори технічної підтримки:

- надання технічної допомоги кінцевим користувачам;

- моніторинг роботи застосунку та оперативне вирішення малих технічних проблем;

- підтримка безпеки і оновлення системи відповідно до нових вимог.

Важливу роль у розробці проєкту відіграють технологічні ресурси, необхідні для створення та підтримки продукту:

- програмне забезпечення та інструменти розробки, які забезпечують створення коду та тестування продукту;

- інструменти шифрування та захисту даних, які є основою для безпечної передачі інформації між користувачами застосунку;

- засоби для тестування безпеки, які дозволяють виявляти вразливості на різних етапах розробки;

- серверна інфраструктура для проведення проміжних тестів та оцінки продуктивності застосунку в реальних умовах.

Реалізація проєкту також потребує фінансування, яке охоплює:

- витрати на заробітну плату команди розробників та експертів;

- витрати на ліцензійні інструменти, необхідні для розробки, контролю та тестування продукту;

- витрати на тестування застосунку в реальних умовах та отримання зворотного зв’язку від кінцевих користувачів.

Оптимізація ресурсів. Оптимізація ресурсів у процесі розробки є важливим етапом для забезпечення ефективності проєкту. Використання гнучкої методології Agile дозволяє адаптувати процес розробки відповідно до змін у вимогах та викликах, що виникають у ході роботи. Це дає змогу уникнути надмірних витрат часу та ресурсів, сприяє швидкому виявленню та виправленню помилок на ранніх етапах розробки. Крім того, постійний зворотний зв’язок із кінцевими користувачами допомагає краще розуміти їхні потреби, що дозволяє уникати надмірних витрат на непотрібний функціонал.

Таким чином, правильне визначення потреб у ресурсах та їх оптимізація є критичними чинниками успішної реалізації проєкту “Blur”. Використання гнучких підходів до управління дозволяє забезпечити високу ефективність

розробки, водночас мінімізуючи витрати та підвищуючи якість кінцевого продукту.

Висновки до розділу 1

У першому розділі було розглянуто основні аспекти, пов’язані з проєктом “Blur”, що спрямований на створення застосунку для захищеної комунікації. Предметна область проєкту охоплює сферу інформаційної безпеки, де критично важливим є забезпечення надійності та конфіденційності переданих даних, особливо в умовах військових операцій. Аналіз проблеми комунікації показав, що наявні рішення не завжди відповідають сучасним вимогам захисту, що створює додаткові ризики для користувачів, особливо у військовому контексті.

Постановка цілей та завдань проєкту включає розробку застосунку, який забезпечуватиме безпечну передачу даних між військовими підрозділами, використовуючи сучасні методи шифрування та зберігання інформації на пристроях користувачів. Проєкт також спрямований на інтеграцію інструментів захисту з максимально зручним інтерфейсом, що робить застосунок ефективним і зручним у використанні.

Окрім цього, у розділі було детально визначено вимоги до продукту, що включають функціональні та нефункціональні аспекти. Ці вимоги формуються на основі аналізу специфічних потреб військових та сучасних стандартів інформаційної безпеки. Важливою частиною проєкту є також оптимізація ресурсів, де людські, технологічні та фінансові ресурси використовуються з максимальною ефективністю для досягнення поставлених цілей.

Завдяки впровадженню Agile-методології у процес розробки забезпечується гнучкість у реагуванні на нові виклики та змінні вимоги користувачів. Це дозволяє не лише своєчасно вносити корективи у продукт,

але й оптимально використовувати наявні ресурси для досягнення максимальних результатів при мінімальних витратах.

Таким чином, у першому розділі було закладено основу для подальшого детального аналізу та розробки рішення, яке відповідатиме високим вимогам військової сфери та сучасним стандартам інформаційної безпеки.

РОЗДІЛ 2. УПРАВЛІННЯ РОЗРОБКОЮ ПРОДУКТУ ДЛЯ ЗАХИЩЕНОЇ КОМУНІКАЦІЇ

2.1 Вибір фрейму гнучкого управління для розробки застосунку

Успішна розробка застосунку для захищеної комунікації в умовах військових операцій вимагає використання гнучких підходів до управління проєктом, що дозволяють швидко реагувати на зміни вимог користувачів і нові виклики. Одним із таких підходів є методологія Agile, яка вже давно зарекомендувала себе як ефективний інструмент для розробки програмного забезпечення. Загалом Agile має 12 принципів побудови процесів, що забезпечують ефективну та швидку взаємодію частин команди чи команд при створенні value продукту [8], вони відображені на рис. 2.1.

1 Найвищим пріоритетом є задоволення потреб замовника через ранню та безперервну поставку цінного програмного забезпечення.	7 Робоче програмне забезпечення є основною мірою прогресу
2 Приймайте змінні вимоги, навіть на пізніх етапах розробки. Гнучкі процеси використовують зміни для забезпечення конкурентної переваги замовника.	8 Гнучкі процеси сприяють стабільній розробці. Спонсори, розробники та користувачі повинні мати змогу підтримувати постійний темп на невизначений термін.
3 Доставляйте робоче програмне забезпечення часто, від кількох тижнів до кількох місяців, надаючи перевагу коротшому часовому циклу.	9 Постійна увага до технічної досконалості та хорошого дизайну підвищує гнучкість.
4 Бізнес-люди та розробники повинні працювати разом щодня протягом усього проєкту.	10 Простота — це мистецтво максимального зменшення обсягу невиконаної роботи — є ключовою
5 Будуйте проєкти навколо мотивованих людей. Надайте їм необхідне середовище та підтримку, і довіряйте їм виконання роботи.	11 Найкращі архітектури, вимоги та проєктні рішення виникають у самоврядних команд.
6 Найефективніший і результативний спосіб передачі інформації в команді розробки — це особиста розмова.	12 Через регулярні проміжки часу команда аналізує, як стати ефективнішою, і відповідним чином коригує свою поведінку.

Рисунок 2.1 – Принципи Agile згідно Agile Manifesto

Джерело: розроблено автором

Для проєкту “Blur” було обрано саме Agile-методологію, а зокрема фреймворк Scrum, як основний підхід до управління розробкою.

Scrum дозволяє розбити розробку на невеликі ітерації, так звані спринти, кожен з яких триває фіксований проміжок часу. Це забезпечує регулярне отримання результатів, які можна тестувати та перевіряти на відповідність вимогам. Кожен спринт має чітко визначені цілі та завдання, що дозволяє команді зосередитися на конкретних аспектах продукту і поступово вдосконалювати його функціонал.

Для розробки застосунку “Blur” було вирішено використовувати Scrum через кілька важливих причин [9]:

1. Гнучкість. Умови військових операцій можуть швидко змінюватися, і застосунок має адаптуватися до нових вимог. Scrum забезпечує можливість швидкої реакції на ці зміни шляхом регулярних ретроспектив і оцінки результатів після кожного спринту.

2. Прозорість процесу. Завдяки постійному спілкуванню між командою та зацікавленими сторонами, усі учасники проєкту завжди мають актуальну інформацію про стан розробки. Це дозволяє вчасно вносити необхідні корективи.

3. Швидке отримання зворотного зв’язку. Регулярне (цикл) тестування проміжних результатів у кожному спринті дозволяє швидко отримувати відгуки від кінцевих користувачів, виявляти можливі проблеми або нові вимоги і негайно їх вирішувати.

4. Фокус на цінність для користувача. Однією з ключових особливостей Scrum є постійна концентрація на потребах користувача, що особливо важливо для проєкту такого типу. Застосунок повинен відповідати вимогам військових підрозділів і забезпечувати найвищий рівень безпеки та зручності.

Для впровадження Scrum у проєкті “Blur” команда була розділена на кілька ключових ролей: Product Owner, Scrum Master та Scrum-команда, що є частиною базової структури (рис. 2.2).

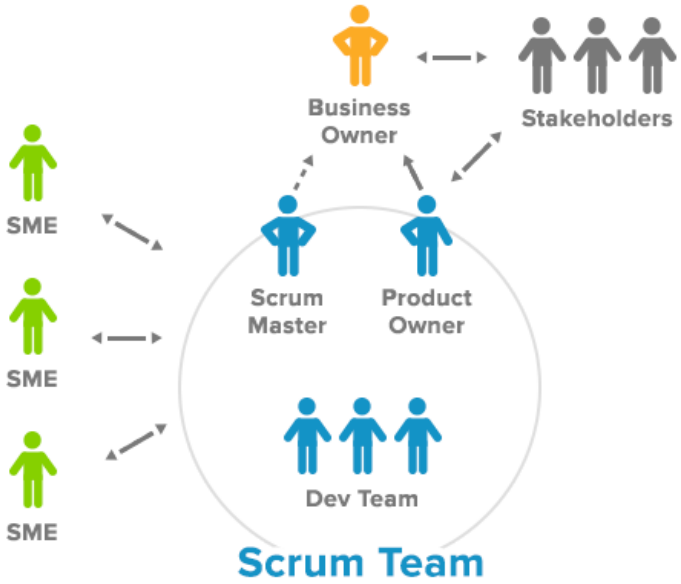


Рисунок 2.2 – Базова структура Scrum команди

Джерело: [5]

Product Owner відповідає за визначення пріоритетів у розробці, формування беклогу та забезпечення того, що кінцевий продукт відповідатиме потребам користувачів. Scrum Master координує процеси розробки, забезпечуючи дотримання правил фреймворку, і сприяє тому, щоб команда могла ефективно працювати без зайвих перешкод.

Scrum також передбачає регулярні зустрічі — щоденні стендапи, планування спринтів та ретроспективи — які дозволяють команді обговорювати поточний стан справ, визначати пріоритети на найближчий спринт та оцінювати, що можна покращити в наступних ітераціях. Цей процес надає можливість гнучко змінювати стратегію і вдосконалювати продукт без шкоди для загального терміну реалізації проєкту.

Непрямим надбанням введення Scrum є можливість парного програмування та екстремального програмування для вирішення нетипових задач, побудови складних алгоритмів чи пошуку точок відказу в модулях проєету [9].

У підсумку, вибір фрейму Scrum для проєкту “Blur” дозволив побудувати ефективну систему управління, яка забезпечує швидке реагування

на зміни, прозорість процесів і постійний зв’язок із кінцевими користувачами. Це є основою для досягнення успішних результатів у розробці застосунку, що відповідає найвищим стандартам безпеки та функціональності.

2.2 Планування проєкту з розробки застосунку - Blur

Планування проєкту включає поділ робіт на етапи з чітко визначеними завданнями та строками на їх виконання. Для наочності в проєкті використовується діаграма Ганта, що включає підготовчі та основні процедури при створенні продукта (план робіт на рис. 2.3), яка дозволяє відслідковувати хід виконання робіт і визначати залежності між етапами [9], після планування діаграми можливе планування спринтів та обосблених завдань для кожного [10].

Повна діаграма Ганта надана в Застосунку Б

Етап 0: Ініціалізація (2.1.25 — 16.1.25)

Перший етапом проєкту і включає підготовчі та аналітичні заходи, необхідні для успішного старту розробки. Тривалість етапу — 15 днів. Основні завдання включають:

1. Аналіз ринку (2.1.25 — 4.1.25). Цей етап передбачає дослідження ринку захищених комунікаційних додатків для розуміння потреб кінцевих користувачів та конкурентного середовища. Аналіз ринку дозволяє визначити тенденції та можливі ризики.

2. Аналіз конкурентів (4.1.25 — 5.1.25). Вивчаються наявні рішення, що забезпечують достатню або часткову захищенність комунікацій в потрібній мірі, або відгалужень, для визначення переваг і недоліків існуючих продуктів та адаптації найкращих з існуючих практик.

3. Пошук фінансування (5.1.25 — 12.1.25). Процес пошуку фінансування включає підготовку пропозицій для інвесторів (на умовах некомерційних

планів) або державних організацій, які можуть зацікавитися підтримкою проєкту.

4. Визначення учасників проєкту (8.1.25 — 16.1.25). На цьому етапі формується команда, що займатиметься розробкою. Включає вибір ключових фахівців, таких як розробники, дизайнери, тестувальники та експерти з безпеки.

Етап 1: Концепція та планування (16.1.25 — 20.2.25)

На цьому етапі команда зосереджена на формуванні концепції продукту та деталізації технічних вимог. Тривалість етапу — 35 днів. Основні завдання включають:

1. Аналіз вимог до застосунку (16.1.25 — 23.1.25). Визначаються ключові вимоги до базової функціональності застосунку на основі можливостей продуктів, які вже існують на ринку та адаптовано обираються актуальні до потреб військових підрозділів. При визначені вимог також проводиться аналіз актуальних загроз для інформаційної безпеки та витоку даних, консультації з агентствами по кібербезпеці та експертами.

2. Розробка технічної документації (20.1.25 — 27.1.25). Формується детальна технічна документація, що містить вимоги до архітектури, протоколів шифрування, системи управління доступом та інших важливих аспектів.

3 Розробка детального плану проєкту (27.1.25 — 3.2.25). Після аналізу вимог команда (Project Manager та Team / Tech Lead) готує деталізований план розробки, який включає розподіл задач між учасниками та планування ресурсів з закладеними очікуваними ризиками щодо технічного боргу по результатам спринтів.

4. Створення суб-прототипу застосунку (30.1.25 — 20.2.25). Створюється перший суб-прототип застосунку, який дозволить перевірити основні безпекові та користувацькі концепції на мінімальному рівні та обрати архітектурний патерн.

Етап 2: Розробка та тестування (20.2.25 — 25.5.25)

Цей етап охоплює процес розробки основних функціональних модулів застосунку, їх тестування та оптимізацію. Тривалість етапу — 90 днів. Основні завдання включають:

1. Розробка основних функціональних модулів застосунку (логіка) (20.2.25 — 20.5.25). Розробники працюють над програмною логікою застосунку, що включає реалізацію протоколів шифрування, управління повідомленнями та обробки даних.

2. Розробка основних функціональних модулів застосунку (інтерфейс) (20.2.25 — 20.5.25). Паралельно з розробкою логіки, дизайнери працюють над інтерфейсом користувача, що має бути інтуїтивно зрозумілим та зручним для військових користувачів.

3. Тестування функціональних модулів (27.2.25 — 21.5.25). Проводиться тестування функціональних можливостей застосунку для виявлення та виправлення можливих помилок у логіці та інтерфейсі.

4. Внутрішнє тестування (21.4.25 — 25.5.25). Проведення внутрішнього тестування (альфа та бета версії), під час якого визначаються стійкість застосунку до навантажень, ефективність захисту даних та зручність використання.

5. Оптимізація програмного забезпечення (8.5.25 — 25.5.25). Включає виправлення помилок, оптимізацію продуктивності та покращення загальної стійкості застосунку.

Етап 3: Впровадження та підтримка (26.5.25 — 3.7.25)

Після завершення розробки починається етап впровадження та технічної підтримки продукту. Тривалість етапу — 39 днів. Основні завдання включають:

1. Встановлення/налаштування застосунку на демонстрантах (26.5.25 — 28.5.25). Установка застосунку на реальні пристрої для демонстрації та тестування в польових умовах.

2. Навчання, демонстрації, презентації (27.5.25 — 17.6.25). Проведення навчальних сесій для кінцевих користувачів, демонстрація основних функцій застосунку.

3. Збір та аналіз відгуків користувачів (27.5.25 — 24.6.25). Після навчання збирається зворотний зв’язок від користувачів для виявлення можливих проблем або недоліків.

4. Виправлення виявлених помилок та недоліків (3.6.25 — 1.7.25). На основі отриманих відгуків вносяться корективи та виправляються знайдені помилки.

5. Надання технічної підтримки користувачам (17.6.25 — 2.7.25). Після випуску продукту команда забезпечує технічну підтримку, що включає оновлення та вирішення технічних проблем.

TASK	ASSIGNED TO	START	END	DAYS
Ініціалізація				
0,1	Аналіз ринку	2.1.25	4.1.25	3
0,2	Аналіз конкурентів	4.1.25	5.1.25	2
0,3	Пошук фінансування	5.1.25	12.1.25	8
0,4	Визначення учасників проєкту	8.1.25	16.1.25	9
Концепція та планування				
1,1	Аналіз вимог до додатку	16.1.25	23.1.25	8
1,2	Розробка технічної документації	20.1.25	27.1.25	8
1,3	Розробка детального плану проєкту	27.1.25	3.2.25	8
1,4	Створення суб-прототипу додатку	30.1.25	20.2.25	22
Розробка та тестування				
2,1	Розробка основних функціональних модулів додатку (логіка)	20.2.25	20.5.25	90
2,2	Розробка основних функціональних модулів додатку (інтерфейс)	20.2.25	20.5.25	90
2,3	Тестування функціональних модулів	27.2.25	21.5.25	84
2,4	Внутрішнє тестування (альфа-, бета-версії).	21.4.25	25.5.25	35
2,5	Оптимізація програмного забезпечення	8.5.25	25.5.25	18
Впровадження та підтримка				
3,1	Встановлення / налаштування додатку на демонстрантах	26.5.25	28.5.25	3
3,2	Навчання, демонстрації, презентації	27.5.25	17.6.25	22
3,3	Збір та аналіз відгуків користувачів	27.5.25	24.6.25	29
3,4	Виправлення виявлених помилок та недоліків	3.6.25	1.7.25	29
3,5	Надання технічної підтримки користувачам	17.6.25	2.7.25	16
	Сума днів на реалізацію		181	

Рисунок 2.3 – План робіт за діаграмою Ганта

Джерело: розроблено автором

2.3 Планування бюджету проєкту

Планування бюджету є одним з найважливіших аспектів управління проєктом, оскільки дозволяє забезпечити достатнє фінансування на всіх етапах розробки та впровадження продукту. Для проєкту “Blur” було створено наближений кошторис, який охоплює витрати на оплату праці, матеріально-технічні ресурси та інші необхідні статті витрат. Розрахунок бюджету проведено у двох валютах: доларах США та українській гривні, з використанням розрахункового курсу 40 UAH/USD.

Повний кошторис з зазначеними статтями витрат та кількості доступний у Застосунку В.

Оплата праці. Ця стаття витрат охоплює заробітну плату команди фахівців, які беруть участь у розробці та підтримці проєкту. Відповідно до плану, для роботи над проєктом залучено аналітиків, програмістів-архітекторів, інженерів-програмістів, тестувальників, менеджера проєкту, військового експерта, технічного керівника та фахівців з технічної підтримки. Загальна сума на оплату праці складає 32 460 000 UAH (811 500 USD).

Основні компоненти:

- аналітики: 1 152 000 UAH (6 міс);
- програмісти-архітектори: 1 840 000 UAH (6 міс);
- інженери-програмісти: 19 200 000 UAH (12 міс);
- тестувальники: 1 440 000 UAH (6 міс);
- менеджер проєкту: 1 200 000 UAH (6 міс);
- військовий експерт: 1 056 000 UAH (6 міс);
- технічний керівник: 1 440 000 UAH (12 міс);
- технічна підтримка: 3 840 000 UAH (12 міс).

Матеріально-технічні ресурси. Ця категорія охоплює витрати на придбання техніки та ліцензійного програмного забезпечення, необхідного

для розробки та тестування застосунку. Загальна вартість матеріально-технічних ресурсів складає 6 400 000 UAH (160 000 USD).

Основні компоненти:

- закупівля комп’ютерів: 3 120 000 UAH (26 одиниць);
- закупівля серверів: 560 000 UAH (2 одиниці);
- закупівля ліцензійного програмного забезпечення: 1 600 000 UAH (20 ліцензій).

Інші витрати. До інших витрат відносяться рекламні кампанії, оренда приміщень, комунальні послуги, канцелярія, транспортні витрати, а також послуги психолога та харчування для учасників проєкту. Загальна сума інших витрат становить 12 240 000 UAH (306 000 USD).

Зазначені витрати не є жорстко плановими, так як вимагають окремих домовленостей з постачальниками чи сторонами, що надаватимуть товари та послуги.

Основні компоненти:

- рекламні кампанії: 6 000 000 UAH;
- оренда приміщення: 480 000 UAH;
- комунальні послуги: 240 000 UAH;
- транспорт: 1 200 000 UAH;
- канцелярія: 840 000 UAH;
- психологічні послуги: 1 920 000 UAH;
- харчування: 2 880 000 UAH.

Детальний план витрат на кожному етапі розробки дозволяє оптимально розподілити ресурси і забезпечити контроль за використанням фінансових коштів. Це також допомагає своєчасно коригувати бюджет у разі зміни обставин або появи нових вимог, що особливо важливо для проєктів за мілітарними напрямками. Чітке розуміння фінансових потреб дозволяє знизити ризики перевитрат, а також забезпечити достатнє фінансування

ключових етапів, таких як розробка, тестування та впровадження продукту. Завдяки ретельному плануванню бюджету, команда зосереджується на основних завданнях, не турбуючись про фінансові обмеження, що позитивно впливає на загальну якість продукту та дотримання строків.

Таблиця 3.1 - Загальні витрати (в нульовому наближенні)

Розрахунковий курс, UAH / $	40
Загальні витрати, UAH	50 568 000
Загальні витрати, USD	1 264 200
Непередбачувані витрати	10%
Бюджет проєкту, UAH	55 624 800
Бюджет проєкту, USD	1 390 620

Висновки до розділу 2

За результатами розділу проведено роботу з аналізу ключових аспектів планування та управління розробкою мобільного застосунку для захищеної комунікації, який створюється в рамках проєкту “Blur”.

Використання сучасних підходів до управління проєктами, таких як Agile, дозволяє не тільки ефективно розподіляти ресурси та контролювати строки виконання, але й гарантувати гнучкість у разі виникнення нових вимог або непередбачуваних ситуацій.

Вибір методології Agile для управління розробкою застосунку “Blur” обумовлений необхідністю гнучкого підходу до реалізації проєкту.

Scrum дозволяє розбивати роботу на невеликі етапи, звані спринтами, що дозволяє команді концентруватися на виконанні конкретних завдань і отримувати результати вже після кожного циклу.

Діаграма Ганта стала одним з основних інструментів для планування тривалості етапів проєкту та управління часовими ресурсами.

Завдяки використанню діаграми Ганта команда отримала можливість чітко бачити критичні шляхи проєкту — етапи, затримки в яких можуть призвести до зриву загальних строків. Це дозволяє вчасно вживати заходів для усунення можливих затримок і забезпечення дотримання графіка.

Описані етапи — від ініціалізації та планування до розробки та впровадження — були чітко визначені з прив’язкою до часових рамок.

Бюджет охоплює заробітну плату ключових фахівців, таких як аналітики, програмісти, архітектори, інженери, тестувальники, менеджери проєкту та експерти з безпеки, інфраструктурні, комунальні та споживчі витрати. Окрім того, передбачено витрати на технічну підтримку продукту після його запуску, що включає як внутрішнє навчання команди, так і надання технічної підтримки кінцевим користувачам.

Для успішного планування бюджету важливо враховувати принципи мінімізації витрат та максимізації результатів [12].

Описаний план підкреслив важливість системного підходу до управління проєктом, де кожен етап — від вибору фреймворку до бюджету — відіграє критично важливу роль для успішної реалізації продукту. Використання гнучких методів управління дозволило забезпечити швидку зміну і адаптивність проєкту, а чітке планування за допомогою діаграми Ганта допомогло визначити часові рамки та забезпечити прозорість процесів.

Усі ці фактори разом гарантують успішну реалізацію застосунку “Blur”, що відповідатиме цільовим стандартам захисту даних та інформаційної безпеки.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ПРОЄКТУ ТА РЕЗУЛЬТАТИ ВПРОВАДЖЕННЯ

Розробка застосунку “Blur” є багатоступеневим процесом, що включає не лише планування та розробку, але й етапи впровадження та оцінки результатів. У поточному розділі розглянуто реалізацію функціональних можливостей застосунку, а також результати його тестування та впровадження у реальних умовах. Важливим аспектом даного розділу є також аналіз впливу проєкту на кінцевих користувачів, оцінка якості захисту даних, а також адаптивність продукту до змінних умов військових операцій. Окрім того, значна увага приділяється результатам навчання користувачів та їхньому зворотному зв’язку [13].

3.1 Реалізація функціональних можливостей застосунку

Одним із ключових завдань проєкту “Blur” було створення надійного та захищеного інструменту для військової комунікації. Реалізація функціональних можливостей застосунку передбачала поетапний процес впровадження основних модулів, таких як система шифрування повідомлень, управління доступом, обробка файлів та інтеграція з існуючими військовими протоколами зв’язку. Кожен з цих модулів був розроблений з урахуванням сучасних стандартів інформаційної безпеки та потреб кінцевих користувачів.

Реалізація системи шифрування даних. Головною особливістю застосунку є наскрізне шифрування (end-to-end encryption), що забезпечує повну конфіденційність переданої інформації. Кожне повідомлення, передане через застосунок, шифрується на пристрої відправника та дешифрується лише на пристрої одержувача. Це унеможливлює доступ до даних третіх осіб, навіть у випадку перехоплення інформації. Впровадження цього механізму стало одним із найскладніших і найважливіших етапів розробки, оскільки від цього залежить безпека всієї комунікаційної мережі.

Управління доступом та безпека користувачів. Для застосунку “Blur” було реалізовано систему багаторівневого управління доступом, яка забезпечує розмежування прав користувачів залежно від їхньої ролі. Кожен користувач має свій рівень доступу до інформації, що дозволяє уникнути витоку конфіденційних даних навіть у разі компрометації одного з користувачів. Такий підхід дозволяє мінімізувати ризики і забезпечити більш гнучке управління системою.

Окрім того, було впроваджено систему автентифікації з використанням багатофакторного захисту, що включає паролі та одноразові коди для входу в застосунок. Ця система значно підвищує рівень безпеки та знижує ймовірність несанкціонованого доступу.

Обробка файлів та повідомлень. Застосунок “Blur” дозволяє користувачам передавати не лише текстові повідомлення, але й файли різного формату. Важливим елементом реалізації цього функціоналу стало забезпечення безпеки файлів під час передачі. Кожен файл проходить шифрування за тими ж принципами, що й текстові повідомлення, забезпечуючи їхню конфіденційність і цілісність [15]. Ця функція дозволяє військовим підрозділам оперативно передавати критично важливу інформацію, не ризикуючи її витоком.

Тестування функціональних можливостей. Після впровадження основних функцій застосунку було проведено ретельне тестування, яке охоплювало перевірку на стійкість до кібератак, функціональність шифрування та надійність системи управління доступом. Тестування проводилося як внутрішньо в команді розробників, так і за участю зовнішніх експертів з інформаційної безпеки. Окрім технічних тестів, велика увага приділялася тестуванню зручності використання застосунку кінцевими користувачами для впровадження легшого переходу та покращення досвіду використання.

3.2 Тестування застосунку та оцінка результатів

Тестування є невід'ємною частиною процесу розробки програмного забезпечення, особливо коли мова йде про додатки, призначені для військових операцій і захисту конфіденційних даних. У рамках проєкту "Blur" тестування проводилося на кількох рівнях для того, щоб оцінити надійність функціональних можливостей, відповідність вимогам безпеки та зручність використання для кінцевих користувачів.

Процес тестування охоплював як внутрішні тести, зокрема тести на перевантаження шлюзу обміну даними, так і зовнішні аудити, що включали перевірку стійкості застосунку до можливих загроз та ефективності його роботи в реальних умовах [13].

Технічне тестування. На першому етапі проводилося внутрішнє системне технічне тестування, що включало функціональну перевірку базових модулів застосунку, що відповідають за безпекову складову (рис. 3.1) та має циклічний характер.

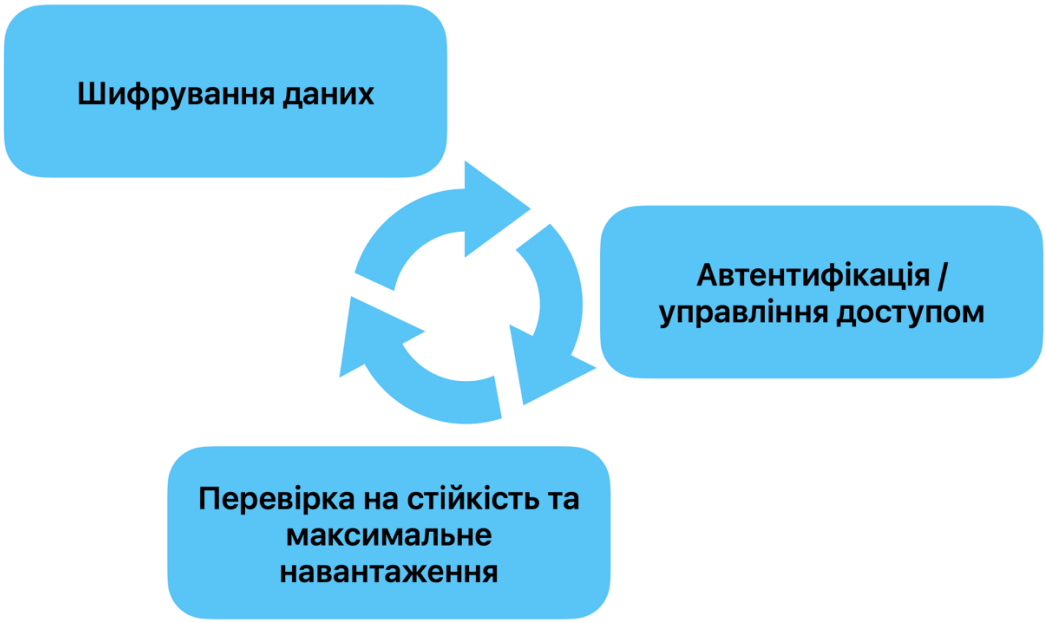


Рисунок 3.1 – Процеси внутрішнього технічного тестування

Джерело: розроблено автором

Один тестовий цикл включає наступне:

1. тестування шифрування даних. Система наскрізного шифрування повідомлень і файлів була піддана детальному аналізу на предмет її стійкості до можливих атак. Це тестування забезпечило впевненість у тому, що сторонні особи не можуть отримати доступ до переданих даних навіть у разі перехоплення трафіку. Шифрування перевірялося на швидкість обробки повідомлень, стійкість алгоритмів та можливість масштабування у випадку збільшення кількості користувачів;

2. тестування автентифікації та управління доступом. Було перевірено, наскільки надійно працює система багаторівневого доступу та багатофакторної автентифікації. Окрема увага приділялася можливості уникнення зламів або несанкціонованого доступу до конфіденційної інформації;

3. перевірка стійкості до навантажень. Було проведено тести на стабільність роботи застосунку за умов високих навантажень та великої кількості активних користувачів. Перевірялися сценарії, коли кількість одночасних підключень зростала до максимальних значень, а також відстежувалася швидкість передачі даних під час таких умов.

Тестування UI / UX. Окрім технічного тестування, велика увага приділялася зручності використання застосунку кінцевими користувачами. Оскільки продукт розробляється для військових підрозділів, важливою вимогою є простота інтерфейсу, інтуїтивність його використання та ефективність у складних умовах. Під час тестування було залучено групу кінцевих користувачів для оцінки:

1. простоти навігації. Користувачі мали змогу протестувати інтерфейс на предмет зручності виконання основних операцій: надсилання повідомлень, передачі файлів та управління доступом до даних.

2. відповідності вимогам польових умов. Інтерфейс мав бути адаптованим до використання у польових умовах, з мінімальними затримками

у виконанні операцій та безпомилковою роботою навіть за умов слабкого інтернет-з’єднання.

Отримані відгуки дозволили ввести необхідні корективи в кодову складову, вдосконалити архітектурні патерни, покращити роботу мережевого шару, відгуку на стороні клієнта та дизайн інтерфейсу, оптимізувавши його для кращої взаємодії з користувачами.

Альфа- та бета-тестування. Після завершення внутрішніх тестів було проведено альфа- та бета-тестування. На етапі альфа-тестування продукт перевірявся внутрішніми командами розробників та тестувальниками для виявлення основних технічних помилок. Цей етап дозволив провести фінальну оптимізацію коду, виправити виявлені баги та підготувати застосунок до зовнішнього тестування.

Бета-тестування було проведене із залученням зовнішніх користувачів — військових підрозділів, що взяли участь у тестуванні продукту в реальних умовах. Бета-тестування дозволило оцінити ефективність роботи застосунку в польових умовах, перевірити його стійкість до навантажень та забезпечити збір зворотного зв’язку від реальних користувачів. В результаті цього етапу було виявлено кілька невеликих недоліків у продуктивності, які були швидко виправлені командою розробників.

Результати тестування. Загалом, результати тестування підтвердили, що застосунок “Blur” відповідає вимогам інформаційної безпеки та стійкий до загроз, зокрема перехоплення даних або спроб несанкціонованого доступу. Тестування також показало, що продукт функціонує стабільно в умовах високих навантажень та може використовуватися для захищеної комунікації військовими підрозділами без ризиків втрати інформації.

Завдяки ретельному тестуванню та впровадженню необхідних коректив, застосунок готовий до повного впровадження в реальні умови та забезпечення захисту інформації на високому рівні.

3.3 Можливості масштабування та розвитку продукту

Один із ключових аспектів розробки програмного забезпечення, особливо у сфері військових комунікацій, полягає у можливості масштабування та подальшого розвитку продукту відповідно до потреб користувачів та змін у технологічних середовищах. Застосунок “Blur” був спроєктований із врахуванням необхідності його подальшого розвитку, а також здатності до масштабування як у контексті кількості користувачів та типів пристроїв, так і за рахунок інтеграції нових функціональних можливостей.

Одним із основних напрямків масштабування продукту є збільшення кількості користувачів та пристроїв, що підключені до системи одночасно та час неперервної сесії. Для того щоб забезпечити безперебійну роботу застосунку навіть при значному збільшенні навантаження, інфраструктура була побудована на основі гнучких серверних рішень за принципами буферних потужностей AWS (Amazone Web Services). Тобто, на стороні сервера наявний профіцит в +20-25% від необхідного для поточних сесій, відбувається моніторинг запитів від клієнтів, формується пакет запитів на обробку та передається в роботу; при збільшенні кількості запитів від користувачів надаються додаткові ресурси. Це дозволяє масштабувати обчислювальні потужності в залежності від потреб проєкту.

Масштабування також охоплює можливість використання застосунку у різних військових підрозділах та навіть у міждержавних військових коаліціях, де важливо забезпечити інтеграцію систем зв’язку різних країн. Для цього передбачено можливість гнучкої конфігурації застосунку, що дозволяє його налаштування відповідно до вимог конкретної системи та забезпечення сумісності з різними протоколами передачі даних.

Інтеграція нових функцій. Здатність застосунку “Blur” до розвитку передбачає можливість інтеграції нових функціональних модулів, які можуть з’являтися в процесі еволюції потреб користувачів. Оскільки вимоги до

захищених комунікацій можуть змінюватися, застосунок був розроблений з модульною архітектурою, що дозволяє додавати нові функції без суттєвих змін до основної інфраструктури.

Також у майбутньому розглядається додавання таких функцій:

- розширені можливості шифрування. З розвитком технологій та появою нових загроз, система шифрування буде оновлена для використання новітніх алгоритмів, для забезпечення більшого рівня захисту даних;

- підтримка нових форматів даних. Застосунок буде адаптований для роботи з новими типами бітних файлів або медіаформатами, що дозволить користувачам передавати більш різноманітну інформацію під час військових операцій;

Підтримка мультиплатформенності. З урахуванням постійного розвитку технологій та різноманітності платформ, на яких працюють військові підрозділи, застосунок “Blur” було спроєктовано з можливістю масштабування на різні операційні системи, зокрема клієнти для Linux дистрибутивів, які є базою для вже впроваджених продуктів (системи частотного та візуального моніторингу, відслідковування та цілей, тощо).

3.4 Впровадження продукту в організаціях та подальша підтримка

Впровадження застосунку “Blur” в штабних організаціях, частинах, бригадах, тощо є складним процесом, що включає кілька етапів — від початкової інтеграції з існуючими системами до надання технічної підтримки та оновлень у процесі експлуатації.

У даному підрозділі буде розглянуто ключові аспекти впровадження продукту в організаціях військового спрямування, особливості інтеграції, а також механізми технічної підтримки, що забезпечують його стабільну роботу після запуску.

Етапи впровадження продукту в організаціях. Процес впровадження продукту в організаціях починається з аналізу існуючих систем зв’язку та інфраструктури, що використовується кінцевими користувачами. Це дозволяє визначити можливі виклики та проблеми, які можуть виникнути при інтеграції застосунку “Blur” з існуючими системами та навчанні військових.

Етап 1: команда технічних спеціалістів проводить детальний аналіз поточних систем зв’язку організації, з якими буде інтегруватися “Blur”. Це дозволяє визначити необхідні вимоги до інтеграції, провести оцінку безпеки та сумісності з існуючими протоколами комунікації.

Етап 2: після аудиту відбувається безпосередня інтеграція з існуючою інфраструктурою на базі дублюючої системи. Це може включати налаштування серверів, синхронізацію з внутрішніми базами даних, налаштування мережевих протоколів і захисних механізмів. Особлива увага приділяється забезпеченню стабільної роботи шифрувальних механізмів під час передачі даних через різні системи.

Етап 3: після інтеграції проводиться ретельне тестування застосунку в реальних умовах експлуатації. Це включає перевірку стабільності з’єднань, відповідності вимогам безпеки, а також зручності використання кінцевими користувачами. На цьому етапі також проводиться виявлення та усунення можливих недоліків в роботі продукту.

Навчання користувачів в організаціях. Для успішного впровадження продукту необхідно провести навчання кінцевих користувачів у організаціях, де планується його використання. Це може включати як індивідуальні тренінги для ключових користувачів, так і масові навчальні сесії для великих підрозділів. Основними напрямками навчання є:

- робота з інтерфейсом застосунку. Користувачі отримують детальні інструкції щодо використання основних функцій застосунку, таких як надсилання зашифрованих повідомлень, передача файлів та управління доступом до інформації.

- забезпечення безпеки при використанні застосунку. Оскільки питання безпеки є ключовим у використанні застосунку “Blur”, значна частина навчання присвячена рекомендаціям з безпечного використання застосунку, уникнення можливих атак та забезпечення захисту конфіденційної інформації.

Навчання дозволяє користувачам не лише швидко освоїти роботу з додатком, але й впровадити в повсякденну практику стандарти безпечного використання інструментів для захищеної комунікації.

Постійна технічна підтримка та оновлення. Після впровадження застосунку “Blur” у організаціях важливо забезпечити його безперебійну роботу та оперативне вирішення технічних питань, які можуть виникнути під час експлуатації. Для цього організовується технічна підтримка, яка включає кілька ключових напрямків:

- моніторинг відказів та загальної роботи застосунку. Команди технічної підтримки постійно стежать за роботою застосунку, аналізуючи показники продуктивності, стабільності мережевих з’єднань та захищеності даних. У разі виявлення будь-яких відхилень або збоїв, фахівці швидко вирішують проблеми, забезпечуючи мінімальний час простою системи.

- оперативне виправлення помилок. Якщо у роботі застосунку виникають помилки або технічні проблеми, команда підтримки надає негайну допомогу користувачам. Це включає як дистанційну підтримку, так і можливість фізичного втручання у випадку серйозних збоїв.

- оновлення та вдосконалення застосунку. У рамках подальшого розвитку продукту команда регулярно випускає оновлення, що включають як виправлення помилок, так і впровадження нових функціональних можливостей. Користувачі отримують оновлення через захищені канали, що дозволяє зберігати безперервність використання застосунку та підвищувати його функціональність.

Окрім технічної підтримки, важливою складовою є зворотний зв’язок від кінцевих користувачів. На основі отриманих відгуків команда може

вносити корективи в інтерфейс, покращувати роботу застосунку та оптимізувати його функції відповідно до реальних потреб користувачів.

Подальше розширення використання продукту. Після впровадження у військових підрозділах застосунок “Blur” має потенціал для подальшого розширення в інших організаціях, де захищена комунікація є критично важливою. Зокрема, продукт може бути впроваджений в урядових структурах, спеціалізованих військових формуваннях та навіть у приватних компаніях, які потребують високого рівня захисту даних з можливістю персоналізації під потреби бізнесу.

Останній з зазначений варіантів також додає комерційну складову до бізнес-моделі, та потенційно є формуючим стимулом альтернативної гілки комерційних розробок на базі вже існуючого спеціалізованого застосунку.

Окрім зазначеного, застосунок може бути адаптований для використання у цивільних секторах, зокрема як суб-месенджер для розширення функціональності додатка та платформи Дія, як державна регульована альтернатива Telegram Messager [16], Viber [17], Signal [18].

Висновки до розділу 3

У ході роботи було детально розглянуто процес створення функціональних можливостей застосунку, проведення тестувань, оцінка результатів і організація подальшої технічної підтримки.

Реалізація функціональних можливостей показала, що застосунок здатен відповідати найвищим вимогам до захисту інформації. Впроваджена система наскрізного шифрування гарантує безпеку передачі даних, а багаторівнева система управління доступом забезпечує надійний захист від несанкціонованого доступу. Користувацький інтерфейс був розроблений з урахуванням польових умов, що дозволяє ефективно використовувати застосунок у складних обставинах.

Тестування застосунку на різних етапах підтвердило його стійкість до навантажень і кібератак. Проведене технічне тестування функціональних модулів, а також альфа- та бета-тестування за участі кінцевих користувачів дозволило ввести корективи і вдосконалити продукт перед його повним впровадженням.

Масштабування та розвиток застосунку є важливим етапом, що визначає його майбутнє. Продукт має потенціал для масштабування як з точки зору збільшення кількості користувачів, так і в контексті інтеграції нових функціональних можливостей. Це дозволяє застосунку залишатися актуальним та гнучким у відповідь на зміни вимог користувачів та технологічні виклики.

Впровадження продукту в організаціях вимагає належної підготовки інфраструктури, навчання кінцевих користувачів та налаштування системи для забезпечення безперебійної роботи. Забезпечення постійної технічної підтримки та можливості швидкого оновлення продукту після впровадження є критично важливими для успішної його експлуатації.

Проєкт “Blur” довів свою життєздатність як інструмент для захищеної комунікації, здатний масштабуватися та адаптуватися до різних організацій та умов використання. Завдяки впровадженню новітніх технологій безпеки, гнучкому підходу до розробки та ефективному управлінню впровадженням, продукт готовий до подальшого використання та розвитку. Його гнучка архітектура дозволяє інтегрувати нові функції та адаптуватися до вимог різних користувачів, що відкриває широкі перспективи для його подальшого впровадження у військовій та цивільній сферах.

ВИСНОВКИ

Галузь, обрана для дослідження та управління розробкою нового продукту, є вкрай актуальною і важливою, особливо в умовах сучасних реалій. Незалежно від того, чи перебуває країна в стані війни або миру, потреба в захищеній комунікації залишається постійною. Сьогодні інформаційна безпека стоїть на перших місцях не тільки для військових, але й для державних та приватних організацій. Кіберзагрози стають дедалі витонченішими, і старі системи та рішення вже не можуть забезпечити належний рівень захисту. Саме тому було обрано напрямок створення мобільного застосунку, який би вирішив проблему захищеного зв'язку. Цей застосунок здатен не лише відповідати сучасним вимогам до безпеки в умовах війни, але й бути корисним у мирні періоди, коли захист даних і комунікацій є важливим для запобігання витокам інформації та збереження конфіденційності завдяки модульній структурі та можливості кастомізації (видозміни) під бажання клієнта.

В ході дослідження та реалізації проєкту "Blur" було детально проаналізовано ключові аспекти планування, управління розробкою та впровадження мобільного застосунку для захищеної комунікації, який стане критично важливим інструментом для військових підрозділів. У першому розділі особливу увагу було приділено аналізу проблемної ситуації та комунікаційних загроз, з якими стикаються військові в умовах кіберзагроз. Було проведено огляд існуючих аналогів на ринку, серед яких Telegram, Signal, Viber, що також надають функції захисту, але не завжди відповідають специфічним вимогам до інформаційної безпеки. Важливим завданням стало створення продукту, який би забезпечив не тільки високий рівень захисту даних, але й адаптацію під постійно змінні вимоги користувачів та нові технічні виклики.

У другому розділі роботи було зосереджено увагу на плануванні процесу розробки. Для досягнення гнучкості та високої ефективності управління проєктом було обрано методологію Agile з використанням фреймворку Scrum

командою розробки. Важливими факторами успіху стали: правильне планування етапів проєкту та грамотний підбір команди фахівців. Кожен учасник команди — від менеджера проєкту до розробників, тестувальників і фахівців з інформаційної безпеки — відігравав ключову роль у процесі реалізації проєкту. Справжній успіх проєкту залежить від злагодженої роботи цих спеціалістів, їхнього професіоналізму та спільного бачення кінцевої цілі — створення надійного, безпечного продукту.

Діаграма Ганта дозволила чітко структурувати етапи розробки та впровадження продукту, контролюючи строки виконання завдань і використання ресурсів. Однак, варто відзначити, що навіть найкращий план не може передбачити всіх можливих змін і непередбачуваних ситуацій, тому обрана методологія Scrum завжди працюватиме тим ліпше, як її буде дотримуватись кожен член команди. Підбір висококваліфікованих фахівців дозволив ефективно вирішувати всі виклики, зокрема завдяки їхньому досвіду та здатності працювати в умовах змін.

Третій розділ роботи зосереджувався на реалізації технічних аспектів продукту, особливо у сфері інформаційної безпеки. Було важливо не тільки створити функціональний застосунок, але й забезпечити його стійкість до кіберзагроз та можливих атак. Використання сучасних методів шифрування, таких як наскрізне шифрування (E2EE), дозволило гарантувати високий рівень безпеки даних, що є критичним для військових комунікацій. Тестування застосунку на всіх етапах розробки дозволило виявити можливі вразливості та усунути їх до моменту впровадження.

Також особливу увагу було приділено питанням подальшого розвитку продукту. Масштабованість застосунку та його впровадження в різних організаціях вимагають ретельного планування та підтримки. Наявність надійної технічної підтримки після запуску продукту стане важливим елементом для забезпечення його ефективної роботи в умовах активного використання. Команда передбачила можливість швидкого оновлення та

розширення функціоналу застосунку в залежності від нових вимог, що є важливим для довготривалої експлуатації продукту.

Таким чином, цей проєкт підкреслив важливість не тільки технічної реалізації, але й стратегічного планування, гнучкого управління процесами та підбору правильної команди для досягнення кінцевої мети — створення якісного, безпечного мобільного застосунку для військових комунікацій. Проєкт “Blur” демонструє, як поєднання сучасних технологій і правильного управління дозволяє вирішувати складні завдання в умовах постійних викликів та змін.

СПИСОК ПОСИЛАНЬ

1. Системи та методи прийняття рішень: методичні вказівки / С. М. Мічківський, Р. Ю. Подольський, Т.К. Талапов. -Старобільськ: ЛНАУ, 2020.- 80 с. – http://dspace.lgnau.edu.ua/xmlui/handle/123456789/1456

2. Jim Highsmith, Agile Project Management: Creating Innovative Products: локальне електронне видання, 2004, 192 с.

3. Розробка програмного забезпечення з використанням баз даних: навчальний посібник / Ю. В. Шамарін, С. М. Мічківський, К. В. Смоктій, Д. В. Шевцов. – Донецьк: ДонНУ, 2013. – 201 с.

4. Aubrey Swanepoel, End-to-End Ecryption Explained: How it Keeps Your Communications Private [електроний ресурс] – URL: https://arc.net/l/quote/oxxwndpu

5. Jeff Sutherland , Scrum: The Art of Doing Twice the Work in Half the Time, електронне видання, URL: https://www.agileleanhouse.com/lib/lib/News/More_Praise_for_Scrum_The_Art_of_Doing_T.pdf

6. ПЗ Кропива, офіційний сайт [електроний ресурс] – URL: https://armysos.com.ua/uk/kropyva/

7. Швабер К. Повний навчальний посібник зі Скраму: правила гри [Електронний ресурс] / К. Швабер, Д. Сазерлеед. – 2020. – URL: https://scrumguides.org/docs/scrumguide/v2020/2020-Scrum-Guide-Ukrainian.pdf.

8. Agile Manifesto: The 12 Principles behind the Agile Manifesto [електроний ресурс] – URL: https://www.agilealliance.org/

9. Екстремальне програмування (XP) не для людей зі слабкими нервами [Електронний ресурс]. – 2017. – URL: https://worksection.com/ua/blog/extreme-programming.html.

2.

10. Mike Cohn , Agile Estimating and Planning, електронне видання, URL: https://www.academia.edu/41614300/Agile_Estimating_and_Planning_by_Mike_Cohn

11. Програмне забезпечення для відстеження завдань – Jira [Електронний ресурс]. URL: https://www.atlassian.com/ru/software/jira

12. Eric Ries , The Lean Startup, електронне видання, URL: https://ia800509.us.archive.org/7/items/TheLeanStartupErickRies/The%20Lean%20Startup%20-%20Erick%20Ries.pdf

13. Project Management Institute (PMI), URL: https://www.pmi.org/learning/thought-leadership/navigating-the-future-of-work-with-an-agile-mindset

14. David Alexander , Information Security Management Principles , електронне видання, URL: https://search.worldcat.org/title/Information-security-management-principles/oclc/1058804893

15. ISO/IEC 27001, URL: https://uk.wikipedia.org/wiki/ISO/IEC_27001

16. Telegram Messager [URL]: https://telegram.org/

17. Viber Messager [URL]: https://www.viber.com/ua/features/

18. Signal Messager [URL]: https://signal.org/uk/

ДОДАТОК А

Термінологічний словник дослідження

Предметна область менеджменту:

1. Менеджер проєкту (Project Manager) особа, відповідальна за планування, управління ресурсами, контроль бюджету та строків виконання проєкту, забезпечення комунікацій у команді

2. Тім лід (Team Lead) технічний керівник команди розробників, що відповідає за вибір технологій, контроль якості коду та підтримку процесів

3. Беклог (Backlog) перелік функцій, задач та вимог, які необхідно реалізувати в рамках проєкту

4. Скрам (Scrum) гнучка методологія управління проєктами, що базується на коротких ітераціях (спринтах) та активній комунікації між учасниками команди

5. Спринт (Sprint) короткий цикл розробки в рамках Scrum, протягом якого команда виконує визначений обсяг задач

6. Ретроспектива (Retrospective) зустріч команди наприкінці спринту для аналізу досягнень та обговорення шляхів покращення процесів

7. Беклог спринта (Sprint Backlog) перелік завдань, які команда бере на себе для виконання протягом одного спринту

8. Product owner особа, що відповідає за формування вимог до продукту, управління беклогом та забезпечення того, що продукт відповідає потребам користувачів

9. Scrum master фахівець, який сприяє впровадженню Scrum у команді, підтримує процеси та допомагає вирішувати перешкоди

Предметна область розробки програмного забезпечення:

1. API (Application Programming Interface) набір інструментів та функцій, що дозволяють програмам взаємодіяти одна з одною

2. Шифрування (Encryption) процес перетворення інформації в зашифрований формат для захисту даних від несанкціонованого доступу

3. E2EE (End-to-End Encryption) наскрізне шифрування, яке забезпечує захист інформації від моменту відправки до моменту отримання

4. Інтерфейс користувача (UI – User Interface) елементи на екрані, з якими взаємодіє користувач для роботи з додатком

5. Користувацький досвід (UX – User Experience) досвід і відчуття користувача під час взаємодії з продуктом

6. Система управління доступом (Access Control) механізми, які забезпечують надання доступу до інформації на основі ролей та прав користувачів

Предметна область інформаційної безпеки:

1. AES (Advanced Encryption Standard) передовий стандарт шифрування даних, який використовується для захисту інформації

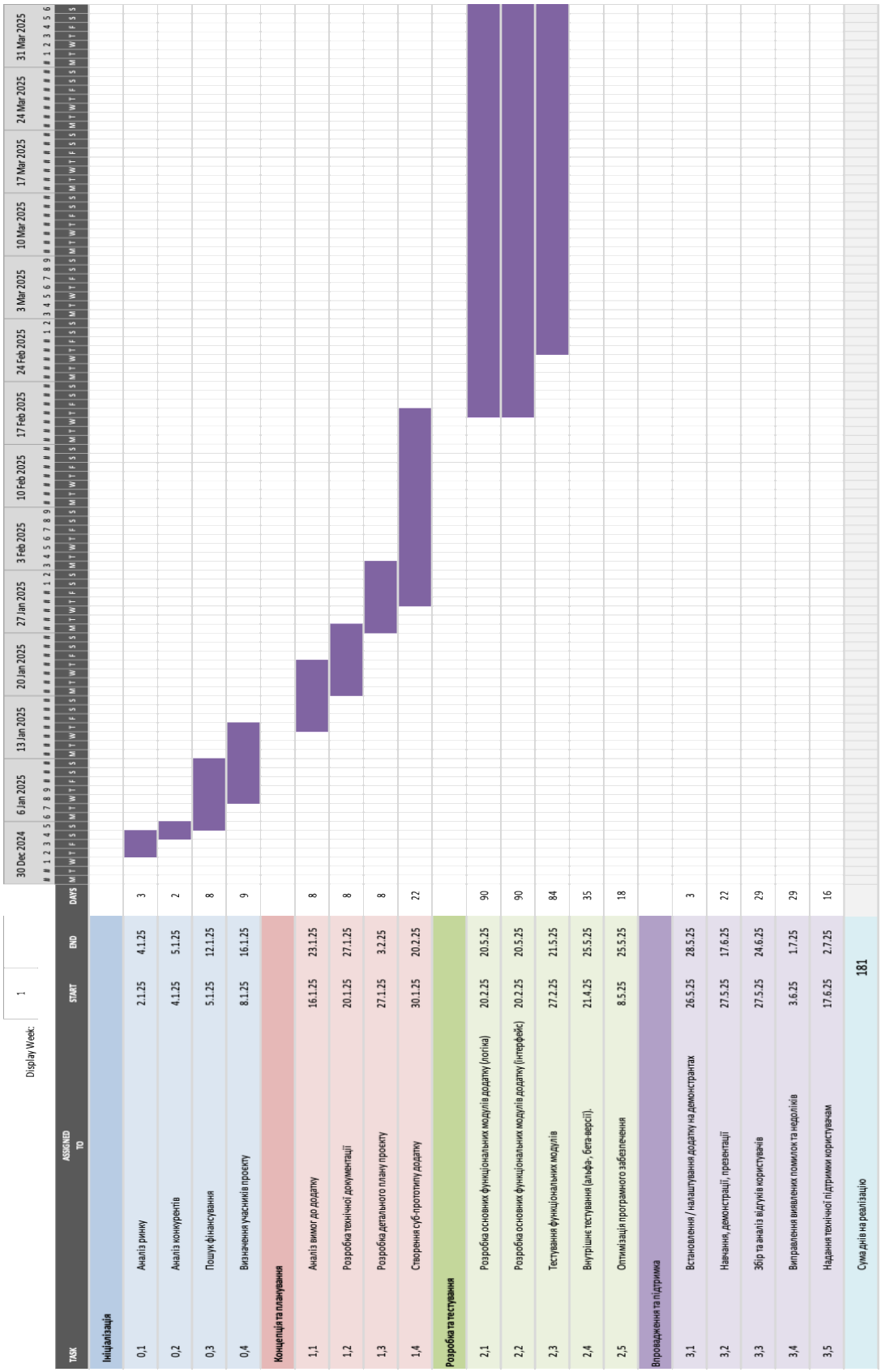
2. VPN (Virtual Private Network) віртуальна приватна мережа, що забезпечує захист даних під час їх передачі через Інтернет

3. Пентестинг (Penetration Testing) процес тестування системи на наявність вразливостей шляхом симуляції кібератак

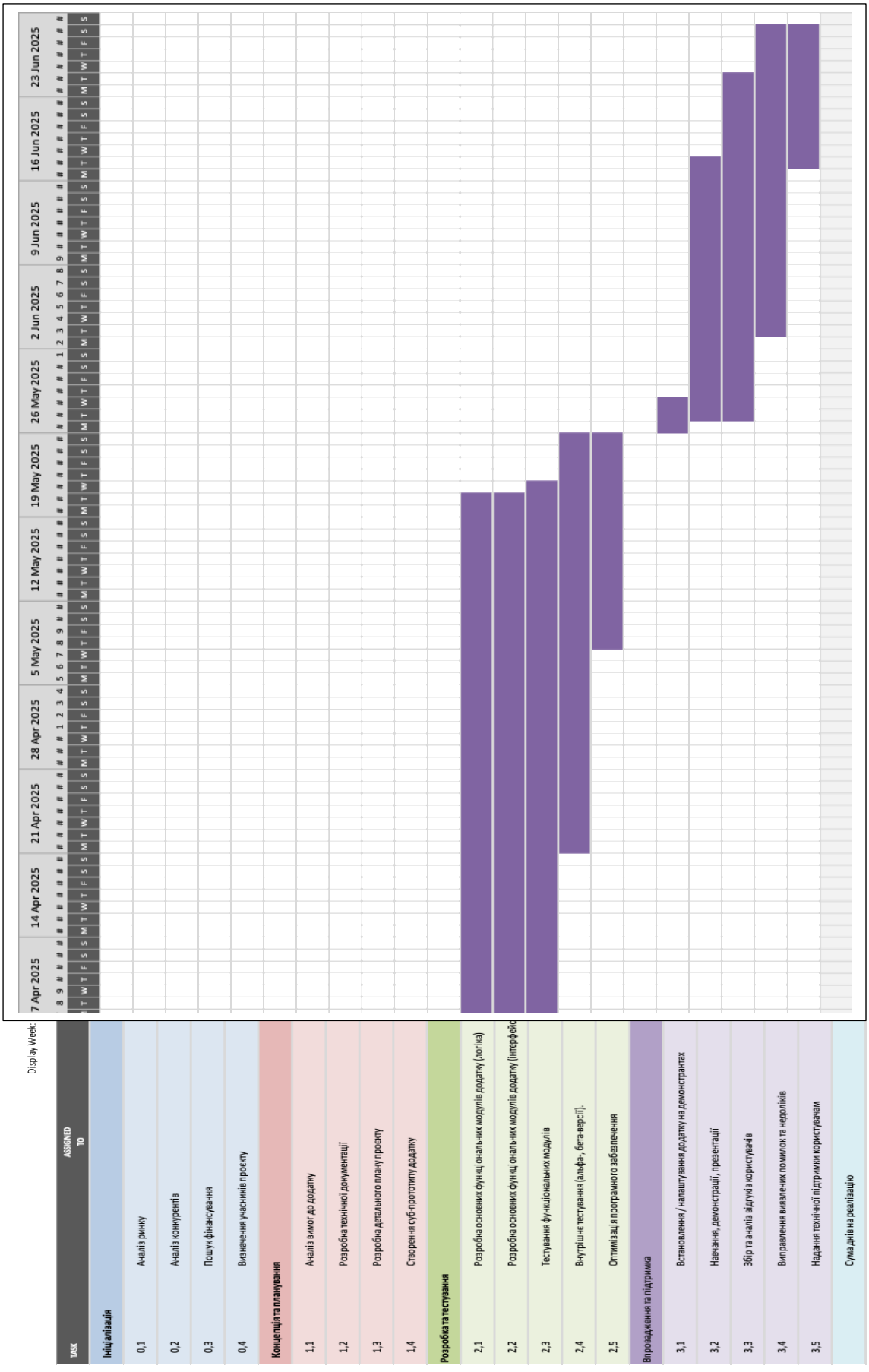
ДОДАТОК Б

Діаграма Ганта

Джерело: розроблено автором



Продовження ДОДАТКУ Б - Діаграма Ганта



ДОДАТОК В

Кошторис проєкту

Джерело: розроблено автором

N°	Стаття витрат	Одиниця виміру	Заплановані витрати			
			Кіль-ть	Ціна (USD)	Ціна (UAH)	Вартість (UAH)
1	Оплата праці					
1.1	Заробітна плата аналітикам	місяць	6	4800	192000	1152000
1.2	Заробітна плата програмістам-архітекторам		6	16000	640000	3840000
1.3	Заробітна плата інженерам-програмістам (Backend, iOS, Android)		12	40000	1600000	19200000
1.4	Заробітна плата тестувальникам		6	6000	240000	1440000
1.5	Заробітна плата менеджменту		6	5000	200000	1200000
1.6	Заробітна плата військовому експерту		6	4400	176000	1056000
1.7	Заробітна плата технічній підтримці		12	8000	320000	3840000
1.8	Заробітна плата UI / UX дизайнерам		12	2000	80000	960000
1.9	Заробітна плата технічному керівнику		12	3000	120000	1440000
2	Матеріально-технічні ресурси					
2.1	Закупівля комп’ютерів та тестових пристроїів (смартфони / планшети)	штук	26	3000	120000	3120000
2.2	Закупівля серверного обладнання		2	7000	280000	560000
2.3	Закупівля ліцензій на програмне забезпечення		20	2000	80000	1600000

Продовження ЗАСТОСУНКУ В - Кошторис проєкту

N°	Стаття витрат	Одиниця виміру	Заплановані витрати			
			Кіль-ть	Ціна (USD)	Ціна (UAH)	Вартість (UAH)
3	Інші витрати					
3.1	Рекламні кампанії	послуга	1	150000	6000000	6000000
3.2	Оренда приміщення	місяць	12	2000	80000	960000
3.3	Комунальні послуги		6	1000	40000	240000
3.4	Транзит		6	5000	200000	1200000
3.5	Канцелярія		6	3500	140000	840000
3.6	Психолог		6	8000	320000	1920000
3.7	Харчування		6	12000	480000	2880000