

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр

(назва освітнього ступеня)

на тему: Розробка застосунку для батьківського контролю при користуванні мобільними пристроями під управлінням ОС Android.

Виконав(ла): студент(ка) 4 курсу, групи СН-42
спеціальності 122 Комп'ютерні науки

(шифр і назва спеціальності)

	<u>Морозов В.В.</u> (підпис) (прізвище та ініціали)
Керівник	<u>Бреус Г.Б.</u> (підпис) (прізвище та ініціали)
Нормоконтроль	<u>Липак Г.І.</u> (підпис) (прізвище та ініціали)
Завідувач кафедри	<u>Боднарчук І.О.</u> (підпис) (прізвище та ініціали)
Рецензент	<u></u> (підпис) (прізвище та ініціали)

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ

Завідувач кафедри

Боднарчук І.О.
(підпис) (прізвище та ініціали)

"27" січня 2025 р.

**ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

на здобуття освітнього ступеня бакалавр
(назва освітнього ступеня)

за спеціальністю 122 Комп'ютерні науки
(шифр і назва спеціальності)

студенту Морозов Владислав Вячеславович
(прізвище, ім'я, по батькові)

1. Тема роботи **Розробка застосунку для батьківського контролю при користуванні мобільними пристроями під управлінням ОС Android.**

Керівник роботи **асист. каф. КН Бревус Г.Б.**

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

Затверджені наказом ректора від "07" травня 2025 року № 4/7-444

2. Термін подання студентом завершеної роботи 25 червня 2025 р.

3. Вихідні дані до роботи Літературні джерела з тематики роботи

4. Зміст роботи (перелік питань, які потрібно розробити)

ВСТУП; 1 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ; 1.1 Актуальність задачі розробки програм батьківського контролю 1.2 Переваги розробки додатків для батьківського контролю 1.3 Приклади успішних програм батьківського контролю 2 АНАЛІЗ ВИМОГ ДО ПРОГРАМИ 2.1 Основні характеристики програм батьківського контролю 2.2 Нефункціональні вимоги до програми 2.3 Можливі стратегії монетизації програми 2.4 Дотримання правил конфіденційності даних 2.5 Опис процесу розробки програми 3 РЕАЛІЗАЦІЯ АРХІТЕКТУРИ СИСТЕМИ 3.1 Загальний опис програмної архітектури 3.2 Архітектурні цілі та обмеження 3.3 Варіанти використання системи 3.4 Логічне подання архітектури 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ; ВИСНОВКИ; СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ; ДОДАТКИ

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

1. Тема; Актуальність роботи та основні загрози для дітей онлайн; Мета і завдання роботи; Ключові функції системи; Аналіз існуючих рішень; Функціональні вимоги до додатку; Нефункціональні вимоги; Архітектура системи (4+1); Сценарії використання батьківського додатку; Сценарії використання дитячого додатку; Логічне подання батьківського додатку; Логічне подання дитячого додатку; Рекомендовані технології розробки; Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Окіпний І.Б., к.т.н., доцент кафедри МТ		

7. Дата видачі завдання 27 січня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	27.01.2025 – 02.02.2025	Виконано
2.	Підбір джерел по темі роботи	03.02.2025 – 01.04.2025	Виконано
3.	Оформлення першого розділу	15.04.2025	Виконано
4.	Оформлення другого розділу	20.04.2025	
5.	Оформлення третього розділу	30.04.2025	Виконано
6.	Виконання завдання до підрозділу "Безпека		
7.	життєдіяльності, основи охорони праці"	15.05.2025	Виконано
8.	Оформлення кваліфікаційної роботи	07.06.2025	Виконано
9.	Перевірка на плагіат	07.06.2025	Виконано
10.	Нормоконтроль	09.06.2025	Виконано
11.	Попередній захист кваліфікаційної роботи	11.06.2025	Виконано
12.	Захист кваліфікаційної роботи	26.06.2025	
13.			
14.			
15.			

Студент

(підпис)

Морозов В.В.

(прізвище та ініціали)

Керівник роботи

(підпис)

Бревус Г.Б.

(прізвище та ініціали)

АНОТАЦІЯ

"Розробка застосунку для батьківського контролю при користуванні мобільними пристроями під управлінням ОС Android" // Кваліфікаційна робота освітнього рівня "Бакалавр" // Морозов Владислав Вячеславович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СН-42 // Тернопіль, 2025 // с. – 47, рис. – 6, джерел – 14, додатків – 1, сторінок додатків – 5.

Ключові слова: батьківський контроль, мобільний додаток, безпека дитини, керування часом за екраном, цифровий моніторинг, Android

У сучасному цифровому середовищі діти мають доступ до величезної кількості інформації та ресурсів. Водночас широке використання смартфонів, планшетів та інших гаджетів піддає їх ризикам, зокрема контактам із небажаним контентом, інтернет-хижаками та проявам кібербулінгу. У цьому контексті особливого значення набувають програми батьківського контролю. Вони створені для того, щоб допомогти дорослим відстежувати та регулювати онлайн-активність своїх дітей. Завдяки вбудованим інструментам безпеки та зручному інтерфейсу такі програми сприяють формуванню безпечнішого цифрового простору для підростаючого покоління.

Ці застосунки виконують функцію нагляду, що дозволяє батькам ефективно керувати тим, як їхні діти користуються цифровими технологіями, захищаючи їх в інтернеті та формуючи здорові звички взаємодії з екранами. Завдяки цим рішенням батьки можуть бути впевнені в тому, що дитина перебуває в безпечному середовищі. У цьому матеріалі буде розглянуто основні можливості програм батьківського контролю, критерії вибору платформи для створення таких застосунків без програмування, а також покроковий підхід до

розробки ефективного і зручного інструменту для контролю цифрової поведінки дитини.

ANNOTATION

"Development of a Parental Control Application for Mobile Devices Running Android OS" // Qualification work of the educational level "Bachelor" // Morozov Vladyslav // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Computer Science, Group CH-42 // Ternopil, 2025 // p. – 47, fig. – 6, references – 14, annexes – 1, pages for annexes – 5.

Keywords: parental control, mobile application, child safety, screen time management, digital monitoring, Android

In today's digital environment, children have access to an enormous amount of information and resources. At the same time, the widespread use of smartphones, tablets, and other gadgets exposes them to risks such as inappropriate content, online predators, and cyberbullying. In this context, parental control applications play a vital role. These tools are designed to help parents monitor and regulate their children's online activities. With built-in safety features and user-friendly interfaces, such apps help create a safer digital space for the younger generation.

These applications serve as monitoring tools that allow parents to effectively manage how their children interact with digital technologies, protect them online, and encourage healthy screen time habits. With these solutions, parents can feel more confident about their child's safety in the digital world. This guide will explore the key features of parental control apps, how to choose a no-code platform for development, and provide a step-by-step approach to creating an effective and user-friendly tool for monitoring and managing a child's digital behavior.

ЗМІСТ

ВСТУП.....	7
1 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ.....	8
1.1 Актуальність задачі розробки програм батьківського контролю.....	8
1.2 Переваги розробки додатків для батьківського контролю.....	10
1.3 Приклади успішних програм батьківського контролю	11
2 АНАЛІЗ ВИМОГ ДО ПРОГРАМИ.....	17
2.1 Основні характеристики програм батьківського контролю.....	17
2.2 Нефункціональні вимоги до програми.....	19
2.3 Можливі стратегії монетизації програми	20
2.4 Дотримання правил конфіденційності даних.....	21
2.5 Опис процесу розробки програми	22
3 РЕАЛІЗАЦІЯ АРХІТЕКТУРИ СИСТЕМИ.....	28
3.1 Загальний опис програмної архітектури.....	28
3.2 Архітектурні цілі та обмеження	30
3.3 Варіанти використання системи	31
3.4 Логічне подання архітектури	34
4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ	37
4.1 Аналіз небезпеки і шкідливості при розробці програмного забезпечення	37
4.2 Інформаційно-психологічні небезпеки	39
ВИСНОВКИ	44
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	46
ДОДАТКИ	

ВСТУП

Прогнозується, що обсяг світового ринку програмного забезпечення для батьківського контролю зросте з 1,4 мільярда доларів у 2024 році до 3,54 мільярда доларів до 2032 року [4].

У Сполучених Штатах 42% дітей мають телефон до 9 років [5]. У тому ж звіті йдеться, що до 14 років володіння смартфонами в США досягає 91%.

Згідно зі звітом регулятора ЗМІ Ofcom, кожна п'ята дитина ясельного віку у Великій Британії має смартфон [6]. У цьому звіті зазначається, що 98% дітей у Великій Британії віком від 16 до 17 років мали мобільний пристрій (смартфон) у 2023 році.

Таке широке використання смартфонів дітьми, природно, викликає тривогу у їхніх батьків; тому батьки намагаються допомогти дітям досягти здорового балансу між онлайн-світом та сімейним.

Згадані щойно звіти показують, наскільки батьки намагаються контролювати онлайн-активність своїх дітей. Дослідження показало, що 48% американських батьків намагалися обмежити час, який їхні діти проводять за комп'ютерами та відеоіграми.

З огляду на всі ці цифри та тенденції, створення багатофункціонального додатка батьківського контролю є актуальною задачею.

Розробкою програмного забезпечення, процесами контролю якості для різних галузей займалися науковці ТНТУ, зокрема це відображено в роботах [1, 2, 3].

1 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Актуальність задачі розробки програм батьківського контролю

Зараз, як ніколи раніше, діти активно користуються інтернет-контентом. Однак, це нерозривно пов'язане з онлайн-загрозами, такими як кібербулінг, публікація особистих даних, шахрайство та фішинг. Це змусило батьків шукати рішення для найкращого захисту в Інтернеті.

Статистика стверджує, що 70% дітей бачили насильницький або сексуальний контент в Інтернеті під час виконання домашніх завдань. Тим часом 65% дітей віком від 8 до 14 років були втягнуті в кібербулінг. І, за словами дітей, найпоширеніші онлайн-ризики включають контакт з незнайомцями, завантаження вірусу, перегляд неприйняттого контенту. Якщо ваша дитина зіткнулася хоча б з однією з цих проблем, вам слід дізнатися більше про рішення батьківського контролю.

У цій роботі ми детально розглянемо основні переваги програми батьківського контролю. Тепер почнемо з розгляду необхідних функцій, які роблять програму батьківського контролю чудовою (див. рис. 1.1).

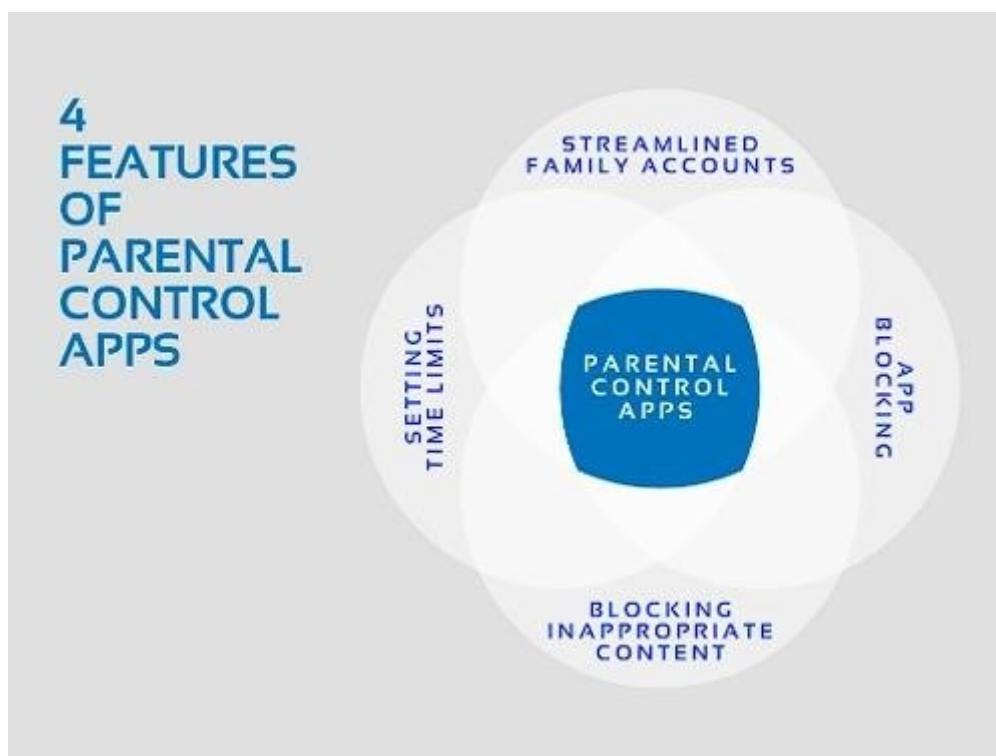


Рисунок 1.1 – Чотири важливі функції додатків для догляду за дітьми

- Встановлення часових обмежень.

Замість того, щоб сперечатися про те, коли час припинити перегляд веб-сайтів, ви можете встановити конкретні часові рамки. Наприклад, додаток не дозволяє вашій дитині шукати в Інтернеті під час їжі або сну. У такому разі додаток вимикається у потрібний час і блокує вашу дитину від використання гаджетів. Крім того, ви можете налаштувати загальний час, який ваша дитина може проводити за телефоном або ноутбуком, мінімізуючи його до кількох годин на день.

- Оптимізовані сімейні облікові записи.

Як правило, діти мають кілька пристроїв, наприклад, планшет і смартфон. Створення програми батьківського контролю не є повним без оптимізованих сімейних облікових записів, особливо якщо у вас кілька дітей. Такий тип облікових записів допомагає батькам оперативно контролювати веб-сайти та керувати часом, який діти проводять перед екраном. Оптимізовані записи для входу легко запам'ятовують десять або більше паролів та імен користувачів.

- Блокування додатків.

Ще однією важливою особливістю є блокування потенційно небезпечних програм або сервісів, з якими ваша дитина може зіткнутися з проблемами, наприклад, під час продажу. Також важливо тимчасово блокувати програми, якщо вам це потрібно. Уявімо, що ваші діти користуються соціальними мережами на уроці під час шкільних годин. Не дивно, що вони вже майже не можуть зосередитися на роботі. Тому блокування соціальних програм та мобільних ігор є ключем до підвищення ефективності під час навчання. Водночас, освітні веб-продукти повністю функціональні на всіх пристроях. Програми легкодоступні, практичні та зручні у використанні.

- Блокування неприйняттого контенту.

Додаток батьківського контролю для Android може фільтрувати інтернет-активність ваших дітей у режимі реального часу. Використовуючи батьківський контроль, ви можете блокувати веб-сайти, які не підходять для вашої дитини. Ця функція також дозволяє блокувати доступ до неприйняттого контенту, а саме до зображень і відео, пов'язаних із насильством, та порнографічних файлів. Крім того, ви можете блокувати певні категорії платформ.

1.2 Переваги розробки додатків для батьківського контролю

Ми вже згадували деякі з цих переваг у попередньому підпункті. Але це далеко не повний список. Розглянемо ключові переваги програм батьківського контролю детальніше.

- Запобігання кібербулінгу.

Статистика свідчить про те, що діти часто стають жертвами кібербулінгу під час користування соціальними мережами. Набір функцій, включаючи моніторинг повідомлень та перегляд активності в соціальних мережах, захищає дітей від таких загроз.

- Побудова міцних стосунків.

Програми батьківського контролю допомагають вам відчувати себе ближче до ваших дітей. По-перше, це чудова можливість для батьків зрозуміти, якими

платформами цікавляться їхні діти. По-друге, програми батьківського контролю заохочують батьків і дітей встановлювати правила та рекомендації щодо безпеки в Інтернеті. Налагодження співпраці з вашими дітьми є важливою частиною побудови довірливих стосунків та підвищення комп'ютерної грамотності.

- Отримання батьківського задоволення.

Коли ви розумієте, що ваша дитина не має доступу до сумнівного контенту, це економить ваші нерви. Фільтрація контенту та налаштування сповіщень є ключем до відновлення душевного спокою. А з іншого боку, діти можуть повною мірою використовувати портативні гаджети для навчання та розваг.

- Ефективне управління часом.

Що ж, не лише дорослі сьогодні відчують брак балансу між роботою та особистим життям. Іноді діти та підлітки вдаються до крайнощів. Вони годинами намагаються виконати домашнє завдання або просто витрачають свій час на цікаві додатки. Численні додатки з функціями управління часом перетворюють домашнє завдання на захопливу гру. Таким чином, діти мотивуються виконувати завдання та проводити більше часу з родиною.

1.3 Приклади успішних програм батьківського контролю

Аналіз успішних програм батьківського контролю може допомогти зрозуміти, які функції та дизайни резонують з користувачами. Ось кілька прикладів успішних програм батьківського контролю.

- Qustodio – це популярний додаток для батьківського контролю з повним набором функцій, таких як відстеження місцезнаходження, керування часом використання екрана, блокування додатків та фільтрація Інтернету. Qustodio пропонує зручний інтерфейс і підтримує різні пристрої та платформи. Додаток використовує модель на основі підписки, пропонуючи низку варіантів ціноутворення для сімей та бізнесу.

- Net Nanny – це добре зарекомендував себе додаток батьківського контролю з розширеними можливостями фільтрації інтернету. Він дозволяє

батькам застосовувати фільтри контенту, відповідні віку, та керувати обмеженнями часу використання екрана. Net Nanny також пропонує функції відстеження місцезнаходження та блокування додатків. Додаток використовує модель на основі підписки з різними ціновими рівнями залежно від кількості захищених пристроїв.

- Norton Family – це комплексний додаток для батьківського контролю від надійного виробника в галузі кібербезпеки. Додаток пропонує відстеження місцезнаходження, фільтрацію інтернету, керування часом використання екрана та блокування додатків. Завдяки інтуїтивно зрозумілому інтерфейсу та розширеним можливостям звітності, Norton Family допомагає батькам бути в курсі онлайн-активності своїх дітей. Додаток працює на основі підписки та пропонує низку варіантів ціноутворення.

- MMGuardian зосереджується на захисті дітей від різних онлайн-загроз, таких як кібербулінг та секстинг. Додаток пропонує низку функцій, включаючи відстеження місцезнаходження, блокування програм, фільтрацію Інтернету та керування часом використання екрану. MMGuardian використовує модель підписки з варіантами ціноутворення для окремих пристроїв та сімейних планів.

Розробляючи додаток батьківського контролю, пам'ятайте, що фактори успіху кожного додатка полягають у його відмінних рисах, привабливому дизайні та бездоганному взаємодії з користувачем. Використовуйте платформи без написання коду, такі як AppMaster.io, щоб оптимізувати процес розробки, водночас гарантуючи, що ваш додаток пропонує переконливий набір функцій та відповідає правилам конфіденційності даних. Дотримуючись цих рекомендацій, ви можете створити ефективний та зручний додаток батьківського контролю, який виділятиметься на ринку.

Переглянемо деякі з найкращих програм батьківського контролю, щоб зрозуміти, що вам варто запропонувати:

1. Додаток FamilyTime.

- Батьки можуть контролювати час, який їхні діти проводять за смартфонами та планшетами.

- Вони можуть обмежити доступ до пристроїв під час навчання або в години, відведені для виконання домашніх справ.
- Дітям потрібен міцний сон, і FamilyTime допомагає в цьому, дозволяючи батькам обмежувати час, проведений перед екраном, протягом ночі.
- Додаток дозволяє батькам блокувати пристрої своїх дітей під час виконання домашніх завдань.
- Батьки можуть блокувати програми та вебсайти з контентом для дорослих. Крім того, вони можуть активувати Безпечний пошук, щоб діти не потрапляли на небажаний контент. Функція веб-фільтра дозволяє батькам блокувати доступ дітей до певних категорій контенту.

Батьки не хочуть, щоб їхні діти відвідували небезпечні місця, і FamilyTime допомагає їм у цьому. Додаток має функцію геозонування, і батьки отримують сповіщення, щойно їхні діти потрапляють у місця, які їм не слід відвідувати.

FamilyTime дозволяє батькам отримувати детальну історію місцезнаходження всіх місць, які відвідують їхні діти.

Соціальні мережі викликають неймовірну залежність і тому можуть відволікати дітей від важливих аспектів життя, таких як навчання чи розваги з родиною. Батьки можуть блокувати соціальні мережі чи ігри на пристрої своєї дитини за допомогою FamilyTime.

Цей додаток також допомагає батькам контролювати дзвінки та текстові повідомлення своїх дітей.

Додаток серйозно ставиться до конфіденційності даних як для дітей, так і для батьків.

Батьки можуть керувати кількома пристроями за допомогою FamilyTime, ділитися керуванням з партнерами та забороняти дітям видаляти FamilyTime.

Діти можуть повідомити батькам, де їх забрати, лише натиснувши одну кнопку.

FamilyTime має як безкоштовну, так і преміум-версії; крім того, додаток доступний на Android, iPhone та iPad.

2. Додаток Qustodio.

Qustodio – ще один хороший додаток для батьківського контролю. Він доступний на таких платформах:

- Windows.
- Chromebook.
- Пристрої Android.
- Операційні системи Apple, такі як macOS та iOS.
- Амазон Kindle.

Цей додаток дозволяє батькам здійснювати такі налаштування батьківського контролю:

- Контролювати онлайн-активність своїх дітей.
- Фільтрація контенту.
- Встановити обмеження часу, проведеного перед екраном.
- Блокувати певні програми.
- Отримувати звіти.
- Відстежуйте місцезнаходження дітей у режимі реального часу.

Цей додаток для моніторингу дозволяє батькам контролювати використання соціальних мереж. Qustodio дає змогу батькам відстежувати дзвінки та SMS-повідомлення на пристрої Android їхньої дитини.

Батьки можуть почати з безкоштовної версії. Qustodio пропонує кілька преміум-планів, які дозволяють відстежувати більшу кількість пристроїв.

3. Norton Family.

Norton Family – ще один приклад найкращих програм батьківського контролю. Він доступний на пристроях Windows, Android та iOS. Цей додаток для моніторингу пропонує такі функції.

- Батьки можуть відстежувати, що їхні діти шукають в Інтернеті та які відео вони дивляться.
- Вони можуть встановлювати обмеження на час, проведений перед екраном.

- Батьки можуть допомогти дітям управляти часом, уникаючи відволікаючих факторів.

- Вони можуть знаходити мобільні пристрої своїх дітей.
- Norton Family допомагає з фільтрацією контенту.
- Батьки можуть контролювати використання додатків і блокувати певні додатки.

Norton Family пропонує 30-денну безкоштовну пробну версію.

4. Google Family Link.

Google Family Link – це відомий додаток батьківського контролю, який працює на пристроях iOS та Android. За допомогою Family Link ви можете налаштувати батьківський контроль для виконання таких дій:

- Моніторинг онлайн-активності, такої як використання соціальних мереж;
- Фільтрація контенту;
- Блокування доступу до певних програм;
- Встановіть обмеження часу, проведеного перед екраном;
- Керування дозволами на використання пристроїв;
- Відстеження місцезнаходження.

5. Microsoft Family Safety

Microsoft Family Safety – це багатофункціональний додаток батьківського контролю. Він працює на Windows, Android та Xbox. Хоча Microsoft Family Safety працює на деяких платформах Apple, ви не можете контролювати комп'ютери MacOS за його допомогою.

Microsoft Family Safety пропонує такі функції:

- Батьки можуть встановлювати обмеження на час, проведений перед екраном.
- Безпека сім'ї Microsoft дозволяє фільтрувати вміст.
- Батьки можуть переглядати звіти про онлайн-активність дітей.
- Ця програма дозволяє відстежувати місцезнаходження.
- Батьки можуть встановлювати обмеження на використання додатків.

Цей список не є вичерпним і містить лише кілька прикладів найкращих програм батьківського контролю. На ринку є багато інших програм батьківського контролю.

Створюючи додаток батьківського контролю на платформі Android, варто зосередитися на включенні таких ключових функцій, як відстеження місцезнаходження в режимі реального часу, фільтрація інтернету, блокування додатків та керування часом використання екрана. Створіть інтуїтивно зрозумілий інтерфейс користувача/користувацький інтерфейс, який задовольняє потреби як батьків, так і дітей, і використовуйте вбудовані інструменти платформи для легкої реалізації необхідних функцій. Слід пам'ятати про ретельне тестування додатка, а коли він буде готовий, розгорнути його та монетизувати за допомогою відповідної бізнес-моделі. Завжди переконайтеся, що ваш додаток відповідає правилам конфіденційності даних та добре інтегрується з будь-якими необхідними сторонніми сервісами.

Дотримуючись цих рекомендацій, можна створити високоефективний додаток батьківського контролю, який допоможе батькам забезпечити безпеку своїх дітей в цифрову епоху та утвердить вашу позицію відповідального та надійного гравця на ринку.

2 АНАЛІЗ ВИМОГ ДО ПРОГРАМИ

2.1 Основні характеристики програм батьківського контролю

Перш ніж заглиблюватися в розробку додатків, важливо визначити ключові функції, які повинен мати ваш додаток батьківського контролю. Ці функції будуть рушійною силою, яка зробить ваш додаток корисним та актуальним для батьків. Ось деякі критично важливі функції, які повинен забезпечувати успішний додаток батьківського контролю:

- Відстеження місцезнаходження в режимі реального часу. Використовуючи GPS або інші служби визначення місцезнаходження, програми батьківського контролю повинні пропонувати батькам можливість відстежувати місцезнаходження своїх дітей у режимі реального часу. Крім того, програма може надавати такі функції, як геозони та історія місцезнаходжень, щоб допомогти батькам відстежувати переміщення своїх дітей та встановлювати безпечні зони.

- Фільтрація інтернет-контенту. Фільтрація інтернет-контенту є критично важливим аспектом програми батьківського контролю. Програма повинна дозволяти батькам блокувати певні веб-сайти, категорії або типи онлайн-контенту, які вони вважають недоречними або шкідливими для своїх дітей. Це гарантує, що діти матимуть доступ лише до відповідного віку та безпечного контенту під час перегляду веб-сторінок.

- Блокування та керування додатками. Додаток повинен пропонувати опції для контролю доступу до певних додатків та ігор на пристрої дитини. Батьки повинні мати можливість блокувати або розблоковувати додатки, встановлювати часові обмеження або обмежувати їх використання залежно від потреб та уподобань дитини.

- Керування часом використання екрану. програми батьківського контролю повинні мати функції, які допомагають батькам керувати часом, який їхні діти проводять перед екраном, такі як встановлення щоденних обмежень

часу, розкладів та винятків для певних програм або дій. Ця функція життєво важлива для сприяння здоровим цифровим звичкам та запобігання надмірному використанню пристроїв.

- Налаштування безпечного пошуку та фільтрація контенту відповідно до віку. Для дітей молодшого віку налаштування безпечного пошуку та фільтри можуть бути життєво важливими для забезпечення додаткового рівня безпеки. Додаток має гарантувати, що діти можуть безпечно шукати в Інтернеті, блокуючи відвертий контент та забезпечуючи обмеження щодо контенту відповідно до віку.

- Моніторинг та звітність. Нарешті, додаток має надавати батькам детальні опції моніторингу та звітності, надаючи їм уявлення про цифрову активність їхньої дитини, таку як історія переглядів, використання додатків та тенденції. Ця функція є надзвичайно важливою для того, щоб допомогти батькам приймати обґрунтовані рішення щодо онлайн-активності своїх дітей.

Таким чином сформулюємо остаточний перелік функціональних вимог.

Батьки хочуть бути спокійними щодо фізичного та емоційного здоров'я своїх дітей. Вони відчують потребу робити наступне.

- контролювати використання пристрою дитиною;
- відстежувати місцезнаходження своїх дітей;
- веб-фільтрація для перевірки контенту перед наданням дозволів на його використання дітям;
- встановлення обмеження часу, проведеного перед екраном;
- допомога дітям з управлінням часом;
- моніторинг використання програми;
- блокування доступ до загрозливого або неприйняттого контенту.

Програмні продукти батьківського контролю допомагають у цьому. Саме тому ринок програмного забезпечення для батьківського контролю стрімко зростає.

Тепер, коли встановлено основні функції програми батьківського контролю, наступним кроком є вибір правильної платформи розробки. Серед них

можливий вибір платформи без коду, які змінили спосіб створення програм, давши змогу будь-кому створювати та налаштовувати програми, не написавши жодного рядка коду. Платформи без коду пропонують численні переваги з точки зору швидкості розробки, вартості та масштабованості. Деякі фактори, які слід враховувати під час вибору платформи для розробки без коду:

Платформи без коду повинні забезпечувати візуально привабливий, простий у використанні інтерфейс перетягування. Це спрощує процес створення додатків, дозволяючи вам зосередитися на їхньому розробці, не турбуючись про складні мови кодування.

Платформа без коду повинна пропонувати низку шаблонів та попередньо створених компонентів, які можна налаштувати відповідно до конкретних вимог вашого додатка. Ця функція заощаджує ваш час та зусилля під час процесу розробки, дозволяючи вам зосередитися на включенні основних функцій та можливостей у ваш додаток батьківського контролю.

Важливо вибрати платформу з високими можливостями налаштування, щоб створити індивідуальний додаток, який відповідає унікальним потребам вашої цільової аудиторії. Платформа повинна підтримувати налаштування брендингу, тематики та модифікацію різних елементів додатку відповідно до бажаного користувацького досвіду.

2.2 Нефункціональні вимоги до програми

Масштабованість. Розробляючи додаток батьківського контролю, важливо враховувати його довгостроковий потенціал для зростання та адаптивності. Платформа без коду повинна забезпечувати легке налаштування та додавання функцій, оскільки вимоги до вашого додатка масштабуються або змінюються з часом.

Можливості інтеграції. Гарна платформа без написання коду повинна підтримувати інтеграцію з різними сторонніми сервісами та API. Це дозволить додатку батьківського контролю безперешкодно взаємодіяти з іншими програмами та сервісами, якими можуть користуватися батьки та діти.

Економічно ефективність. Вибір платформи для розробки без коду, яка пропонує економічно ефективні тарифні плани та рівні підписки, є важливим для управління бюджетом під час розробки додатків.

2.3 Можливі стратегії монетизації програми

Створення програми батьківського контролю з винятковими функціями та зручним дизайном – це лише перший крок, ефективна монетизація програми має вирішальне значення для її довгострокового успіху. Стратегії монетизації спрямовані на отримання доходу від програми, що дозволяє вам підтримувати та вдосконалювати її, тим самим залучаючи та утримуючи користувачів. Ось деякі популярні стратегії монетизації програм батьківського контролю:

- **Модель Freemium.** Ця модель дозволяє користувачам отримати доступ до основних функцій програми безкоштовно, тоді як преміум-функції доступні за платною підпискою. Модель Freemium – це чудовий спосіб залучити користувачів спочатку, оскільки вони можуть протестувати програму без будь-яких фінансових вкладень. Як тільки вони вважають основні функції корисними, вони з більшою ймовірністю оновляться до преміум-версії, щоб розблокувати розширені можливості.
- **Модель на основі підписки.** У цій моделі користувачі сплачують періодичну плату (щомісяця, щокварталу або щорічно) за доступ до програми та її функцій. Забезпечуючи стабільний та надійний потік доходу, моделі на основі підписки можуть допомогти вам більш передбачувано керувати витратами на розробку та обслуговування вашої програми. Щоб зробити модель підписки більш привабливою, ви можете пропонувати знижки або ексклюзивні пропозиції користувачам, які обирають довші періоди підписки.
- **Покупки в додатку.** Можна пропонувати додаткові покупки в додатку у вашому додатку батьківського контролю. Ці покупки можуть включати розблокування певних функцій, розширення можливостей додатка або придбання доповнень, що покращують взаємодію з користувачем.

Переконайтеся, що ці покупки в додатку є цінними для ваших користувачів, водночас генеруючи додатковий дохід.

- Плата за додаткові функції. Ще один спосіб монетизувати додаток – це стягувати плату з користувачів за доступ до певних функцій. Ця модель оплати за функцію дозволяє користувачам налаштовувати роботу з додатком і платити лише за ті функції, які їм потрібні. Ви можете створювати різні цінові рівні або пакети, щоб задовольнити різноманітні потреби ваших користувачів.

2.4 Дотримання правил конфіденційності даних

Програми батьківського контролю обробляють конфіденційну інформацію користувачів, зокрема дані про місцезнаходження дітей, історію переглядів та використання програм. Важливо дотримуватися правил конфіденційності даних та забезпечувати безпеку й конфіденційність даних користувача. Ось кілька кроків, які допоможуть програмі дотримуватися правил конфіденційності даних.

1. Впровадження шифрування. Потрібно використовувати надійні методи шифрування для захисту даних, що передаються між додатком і сервером. Наскрізне шифрування захищає інформацію, що робить практично неможливим доступ до неї або її втручання неавторизованими користувачами.

2. Безпечне зберігання даних. Зберігайте дані користувачів безпечно відповідно до законів про захист даних та найкращих галузевих практик. Виберіть надійний та безпечний хостинг-сервіс і розгляньте можливість впровадження додаткових заходів безпеки, таких як контроль доступу до даних та механізми виявлення вторгнень.

3. Чітка політика конфіденційності. Варто розробити чітку та лаконічну політику конфіденційності, яка описує, як додаток збирає, обробляє та зберігає дані користувачів. Політика повинна містити детальну інформацію про мету збору даних, терміни зберігання даних та будь-які практики обміну даними зі сторонніми сторонами. Переконайтеся, що політика конфіденційності легкодоступна для користувачів, і запитуйте їхню активну згоду під час реєстрації в додатку.

4. Згода користувача. Завжди потрібно отримувати згоду користувача перед збором, зберіганням або обробкою персональних даних, особливо від неповнолітніх. Забезпечте, щоб процес отримання згоди був простим і прозорим, а також щоб користувачі могли відкликати згоду або вимагати видалення даних у разі потреби.

5. Дотримання правових норм. Завжди варто знайомитись з правовими нормами та інструкціями, що застосовуються до програм батьківського контролю на цільових ринках, такими як Закон про захист конфіденційності дітей в Інтернеті (COPPA) у Сполучених Штатах. Варто співпрацювати з експертами-юристами, щоб забезпечити повну відповідність додатка вимогам, та оновлювати методи роботи в міру розвитку та зміни правил.

2.5 Опис процесу розробки програми

1. Формування специфікації вимог до програми здійснено в попередніх розділах.

2. Вибір правильної методології проекту.

Додаток батьківського контролю може мати ще кілька функцій, як показано на прикладі FamilyTime. Найкращим рішенням буде вам запустити «мінімально життєздатний продукт» (MVP) із згаданими вище функціями та спочатку запустити додаток в одному регіоні.

Пізніше розробники мобільних пристроїв можуть удосконалити застосунок на основі відгуків ринку, наприклад, можна додати функцію геозонування. Agile – це правильна методологія для такого виду ітеративної розробки, і рекомендовано використовувати її в цьому проекті.

3. План розширення діяльності в інші регіони в майбутньому.

Додаток батьківського контролю може мати світовий ринок, і слід розробляти додаток таким чином, щоб його можна було легко запускати в інших регіонах. Існує кілька найкращих практик для цього, наприклад, відокремлення контенту від коду.

4. Вибір підходу до розробки програми батьківського контролю для Android.

Можна використовувати наступний підхід до розробки цього проєкту.

- Використання платформи «Мобільний бекенд як послуга» (MBaaS), оскільки вона звільняє від завдань розробки та управління мобільним бекендом. Це пришвидшує розробку.

- Використання «комплектів розробки програмного забезпечення» (SDK) та «інтерфейсів прикладного програмування» (API) для реалізації ключових функцій, що заощаджує час.

5. Формування команди розробників.

Потрібна команда розробників з такими ролями:

- Бізнес-аналітики (BA).
- Дизайнери інтерфейсу користувача.
- Розробники Android.
- Тестери.
- Керівник проєкту (PM).

Доцільно використовувати техніку «Scrum» для виконання цього проєкту, яка підходить для Agile-розробки. Слід організувати свою команду в невеликі, міжфункціональні «scrum-команди», де розробники та тестувальники працюють разом над «Спринтами», тобто ітераціями.

6. Реєстрація у постачальника MBaaS.

Одним з варіантів є зареєструватися в AWS Amplify, тобто на платформі MBaaS від AWS, та отримати такі переваги:

- Можна зосередитися на дизайні інтерфейсу користувача та розробці бізнес-логіки, а не на розробці та управлінні мобільним бекендом. Таким чином, не потрібно наймати розробників мобільного бекенду, архітекторів хмарних платформ та інженерів інфраструктури.

- MBaaS керують хмарною інфраструктурою та постійним сховищем.

- Існують різні мобільні платформи та пристрої, які можуть ускладнювати розробку мобільних додатків. Використання платформи MBaaS допомагає впоратися з цією складністю.

- Можна легко інтегрувати сторонні API; крім того, можна легко впроваджувати функції керування користувачами, безпеки та push-сповіщень, використовуючи платформу MBaaS.

- Масштабування застосунку простіше за допомогою платформи MBaaS.

7. Розробку проекту спростить отримання рішення SDK/API для реалізації функції батьківського контролю

Для розробки цього додатка для Android можна використовувати Allow2, проект з відкритим кодом, який пропонує рішення для батьківського контролю. Allow2 має запатентоване рішення для батьківського контролю, яке пропонує такі функції та переваги:

- Можна додати швидкі та прості механізми батьківського контролю до свого застосунку.

- Користувачі додатків можуть запровадити батьківський контроль у мобільних додатках, веб-сайтах та соціальних мережах.

- Батьки можуть застосовувати обмеження, наприклад, вони можуть позбавляти привілеїв.

- Вони також можуть встановити в календарі дні, коли діятимуть обмеження. Більше того, вони можуть послаблювати ці обмеження в певні дні.

- Батьки можуть розділити контроль зі своїми партнерами.

Allow2 має кілька SDK, і можна переглянути їх на порталі розробника. Використовуйте API Allow2. Це продукт з відкритим кодом; однак, перед його використанням слід ознайомитися з правилами ліцензування. В цьому випадку використання API потрібно буде створити обліковий запис розробника.

8. Слід придбати рішення SDK/API для шифрування.

Слід вжити відповідних заходів для захисту даних користувачів. Тому можна використовувати AWS Encryption SDK для цього проекту. Опишемо коротко цей SDK.

- Він використовує «Advanced Encryption Standard» (AES) з 256-бітним шифруванням.
- У цьому проєкті потрібно використовувати AWS Encryption SDK для Java.
- AWS також надає зразок коду.

9. Слід зареєструватися для масового SMS-розсилання через API.

Потрібно впровадити функцію push-сповіщень у додатку. Тому можна використовувати Twilio, відомого постачальника рішень API для масових SMS.

10. Отримання рішення для інтеграції платіжних шлюзів.

На цьому етапі потрібно отримати SDK/API рішення для інтеграції платіжних шлюзів. В міжнародних проєктах рекомендується використовувати Stripe, в тому числі і для цього проєкту, оскільки він забезпечує швидку, масштабовану та безпечну інтеграцію платіжних шлюзів.

11. Дизайн інтерфейсу користувача програми батьківського контролю для Android.

Тепер, коли ми визначилися з платформами, SDK, API та фреймворками, можна перейти до дизайну інтерфейсу мобільного додатку. Для цього слід скористатися наступними посібниками:

- Рекомендації щодо матеріального дизайну [7], які важливі для дизайну інтерфейсу користувача додатків для Android.
- Вичерпний посібник з дизайну мобільних додатків [8].
- «10 порад щодо дизайну мобільних додатків» – корисний посібник від Adobe [9].

12. Написання та тестування коду, публікація додатку батьківського контролю для Android.

Тепер можна розпочати розробку програми батьківського контролю для Android, яка включає такі кроки.

- Використання Android Studio, яке є «інтегрованим середовищем розробки» (IDE) для розробників Android.

- Написання програми за допомогою Java з дотриманням ліцензійних вимог.
- Інтеграція в додаток SDK/API Allow2, шифрування AWS, Twilio та Stripe.
- Використання Espresso з лабораторією мобільних пристроїв Experitest, щоб протестувати застосунок.
- Публікація додатку у магазині додатків Google Play.

Таким чином буде готовий MVP.

Під час створення нового додатка для батьківського контролю слід пам'ятати, що він оброблятиме конфіденційну інформацію. Це може включати активність у соціальних мережах, відстеження місцезнаходження, дзвінки, здійснені на телефон дитини тощо.

Неможливо переоцінити важливість безпеки. Потрібно не лише дотримуватися правил конфіденційності та безпеки даних, але й вселяти впевненість користувачам. Батьки завантажуватимуть додаток лише з Google Play Store.

Тому слід виконати наступне.

- Використання сучасних методів, такі як MFA (багатофакторна автентифікація).
- Ретельний перегляд коду додатку, щоб знайти помилки. Ретельне тестування додатку, щоб хакери не могли скористатися помилками.
- Краще розробляти нативні додатки замість кросплатформних. Нативні додатки найкраще використовують апаратні функції та можливості операційної системи пристроїв Android. Вони забезпечують кращий користувацький досвід, продуктивність та безпеку, ніж кросплатформні додатки.

Цифровий світ часто є небезпечним для дітей. Популярні соціальні мережі та додатки для спілкування, такі як Snapchat, дозволяють налаштувати батьківський контроль. Батьки можуть переглядати інструкції в Інтернеті, щоб налаштувати батьківський контроль у додатках своїх дітей.

Це показує, що ринок буде надзвичайно зростати в найближчі кілька років.

Платформи, SDK, API, фреймворки та інструменти, безумовно, допомагають у розробці MVP для таких програм батьківського контролю для Android. Однак, якщо метою є розробити найкращу програму батьківського контролю, треба бути готовим до складнощів.

Додавання таких функцій, як геозонування, блокування програм тощо, збільшує складність розробки додатка, тому, можливо, слід звернутися за допомогою до авторитетної компанії з розробки програмного забезпечення.

3 РЕАЛІЗАЦІЯ АРХІТЕКТУРИ СИСТЕМИ

3.1 Загальний опис програмної архітектури

У цьому розділі описано огляд Батьківського контролера з точки зору його основних технологій, збірку компонентів програми та огляд архітектури для послідовної розробки проекту. Прикладне програмне забезпечення, що працює на ОС Android, має можливості керування одним пристроєм Android (дочірнім дроїдом) іншим пристроєм Android (батьківським дроїдом) та передачі інформації між двома пристроями.

Документ з архітектури програмного забезпечення (SAD) надає вичерпний огляд архітектури програми батьківського контролю для Android. Він представляє низку різних архітектурних подань для зображення різних аспектів системи. Він призначений для того, щоб відобразити та передати важливі архітектурні рішення, прийняті в системі.

Для якомога точніше відображення програмного забезпечення структура цього документа базується на моделі архітектури «4+1» [10] (рис. 3.1).

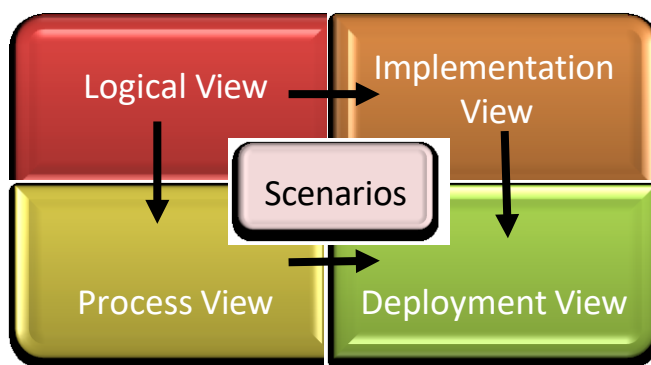


Рисунок 3.1 – Модель архітектурного подання «4+1»

Модель подання «4+1» дозволяє різним зацікавленим сторонам знаходити те, що їм потрібно в архітектурі програмного забезпечення.

Архітектура проєкту повинна брати участь в управлінні змінами в системі та вносити зміни до документації відповідно до виниклих проблем. Розробник проєкту повинен використовувати цю документацію для впровадження проєкту

на ОС Android. Також оцінювач проєкту повинен перевіряти та аналізувати документацію та надавати відгуки щодо поточної оцінки стану та майбутніх удосконалень.

Цей опис архітектури програмного забезпечення містить огляд архітектури програми батьківського контролю для Android і містить наступні подання архітектури.

1. Перегляд варіантів використання.

Представлення варіантів використання описує набір сценаріїв та/або варіантів використання, які представляють певну важливу, центральну функціональність системи. Воно використовує акторів та варіанти використання для опису системи, представляє потреби користувача та додатково розробляється на рівні проєктування для детальнішого опису дискретних потоків та обмежень. Цей словник предметної області не залежить від будь-якої моделі обробки або репрезентативного синтаксису.

2. Логічне подання.

Логічне подання зосереджується на функціональних вимогах до програми. Воно описує об'єктну модель дизайну та найважливіші реалізації варіантів використання.

3. Подання процесу.

У режимі подання процесу будуть описані нефункціональні вимоги до додатку для Android. Також будуть описані аспекти паралельності та синхронізації дизайну. Це вплине на інтеграцію системи.

4. Подання розгортання.

У режимі розгортання описується відображення програмного забезпечення на апаратному забезпеченні та показано розподілені аспекти системи. Також він описує потенційні структури розгортання. Включаючи відомі та очікувані сценарії розгортання в архітектуру, ми дозволяємо розробникам робити певні припущення щодо продуктивності мережі, взаємодії системи тощо.

5 Подання реалізації.

Подання реалізації розкладає додаток на програмні компоненти та показує їхню взаємодію, включаючи шари та підсистеми додатку. Це надасть програмістам модель реалізації компонентів.

3.2 Архітектурні цілі та обмеження

Існують деякі ключові вимоги та системні обмеження, які суттєво впливають на системну архітектуру Батьківського контролера для Android.

1. Технічна платформа.

Батьківський контроль буде розгорнуто на платформі Android з версією 10.0 і новіші.

Потрібно використовувати протоколи зв'язку, які підтримуються версією Android 10.0.

Потрібно турбуватися про функції безпеки платформи, пов'язані з доступом до апаратного рівня та обмеженнями моніторингу привілеїв нижчого рівня.

2. Безпека.

Система повинна бути достатньо захищена для зв'язку між двома програмами. Система повинна досягати більшої безпеки щодо продуктивності, щоб уникнути конфліктів компромісів. Щоб забезпечити безпеку щодо локального/фізичного доступу до системи, вона повинна мати:

Автентифікацію для Parentdroid (телефону батьків).

Автентифікація для Childroid (телефону дитини). Для входу в додаток Childroid необхідно використовувати ім'я користувача та пароль, які використовуються в Parentdroid, а також виконати перевірку автентифікації для доступу до налаштувань додатка Childroid. Сповіщення про доступ до додатка Childroid надсилається до Parentdroid.

Для доступу до Інтернету обов'язкові такі вимоги.

Конфіденційність: конфіденційні дані (ім'я користувача та пароль) мають бути зашифровані.

Дві програми повинні бути достатньо безпечними, щоб запускатися окремо та продовжувати працювати.

Безпека дитини не повинна впливати на апаратні компоненти, такі як SIM-картка та чіпи даних.

4. Доступність.

Цільова доступність – 12/7: 12 годин на добу, 7 днів на тиждень. Якщо Childroid не відповідає, користувач Parentdroid повинен перевірити поточну ситуацію.

3.3 Варіанти використання системи

Опис подання варіантів використання архітектури програмного забезпечення. Подання варіантів використання є важливим вхідним елементом для вибору набору сценаріїв та/або варіантів використання, які є фокусом ітерації. Воно описує набір сценаріїв та/або варіантів використання, що представляють певну значну, центральну функціональність. Воно також описує набір сценаріїв та/або варіантів використання, які мають суттєве архітектурне покриття (які реалізують багато архітектурних елементів) або які підкреслюють чи ілюструють певний, делікатний момент архітектури.

- Отримання місцезнаходження телефону через Google API.
- Вхід.
- Налаштувати запити.
- Зробити знімок.
- Надсилання SMS/MMS через MSP.
- Переслати зображення.
- Запис голосу.
- Запис телефонних дзвінків.
- Зберегти у файлі.
- Надсилання електронної пошти через Інтернет.
- Показати місцезнаходження дитини.
- Переглянути сповіщення.

- Переглянути фотографії.
- Переглянути SMS-повідомлення дитини.

На рисунку 3.2 показано сценарій використання системи коли користувач Parent має доступ до застосунку Child

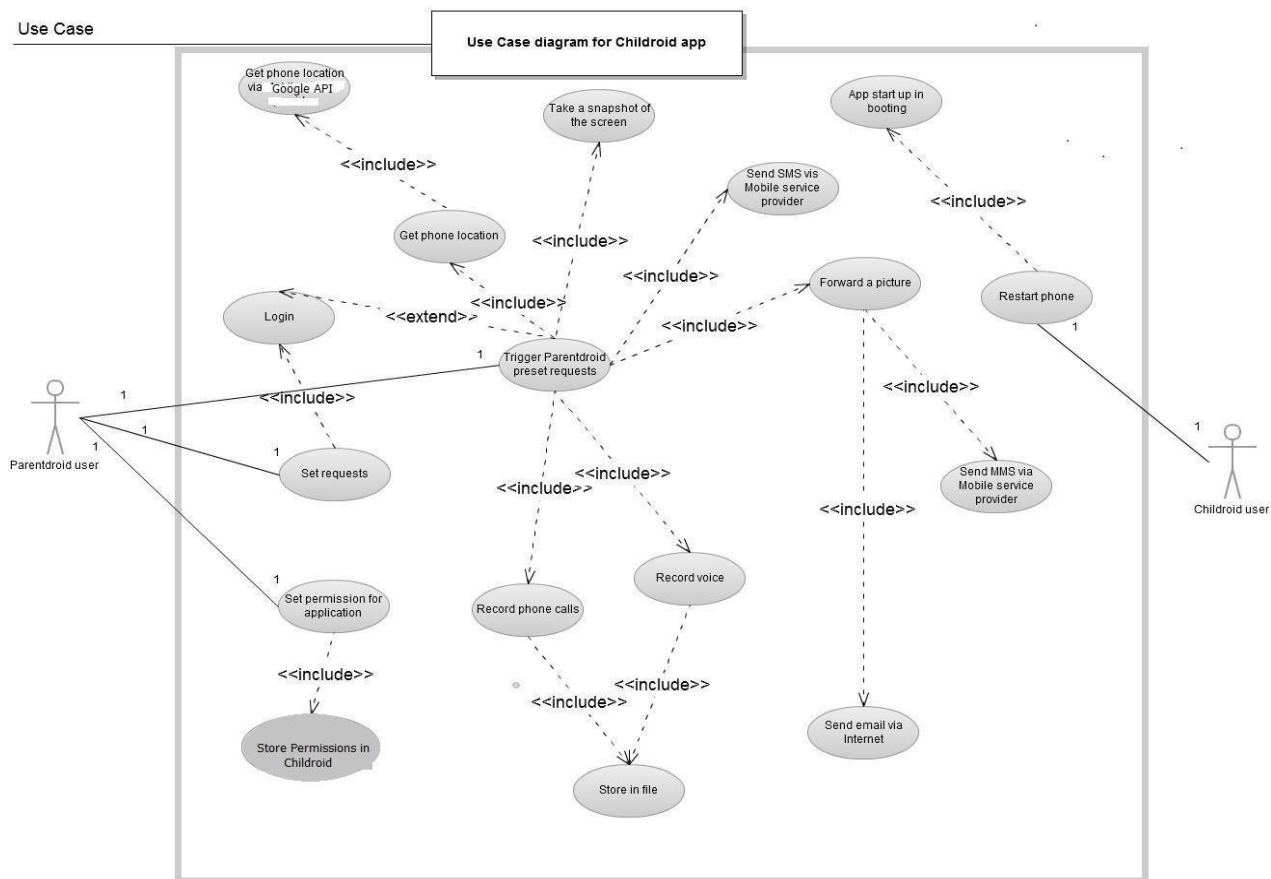


Рисунок 3.2 – Сценарій використання користувача Parent у застосунку Childroid

На рисунку 3.3 наведено сценарій використання батьківського застосунку. Опишемо інші сценарії використання програми у текстовому вигляді.

Отримати місцезнаходження телефону через MSP. Отримати місцезнаходження пристрою Childroid за допомогою методу Google API. Тоді батьки зможуть отримати інформацію про місцезнаходження своєї дитини.

Вхід. Тільки Батьки мають обліковий запис користувача в додатку Childroid, а пароль зберігається в додатку Childroid у зашифрованому форматі XML. Для встановлення будь-яких змін у Childroid потрібна автентифікація користувача.

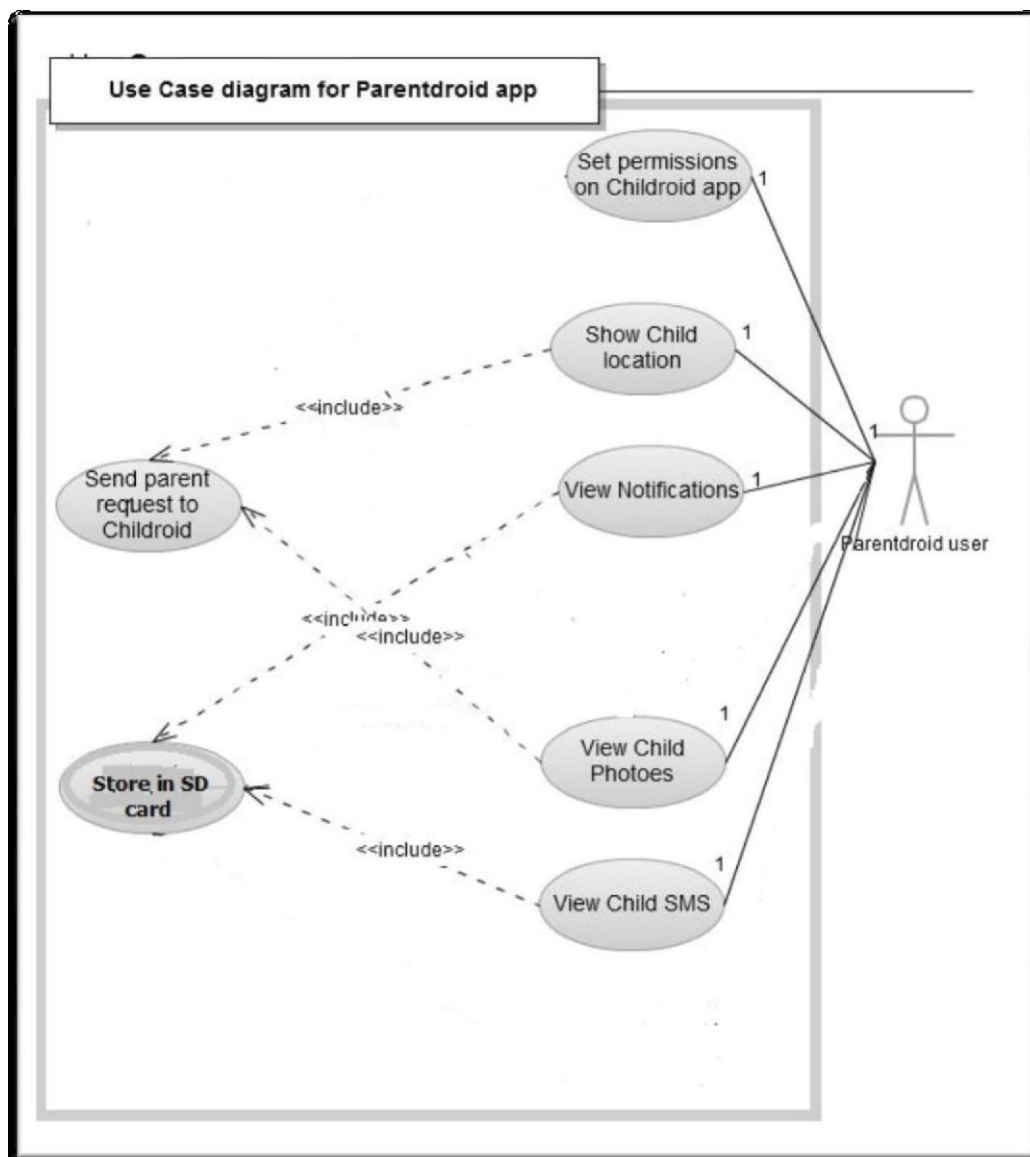


Рисунок 3.3 – Діаграма варіантів використання для батьківського користувача в застосунку Parent

Налаштувати запити. Parent може надіслати SMS-запит для уточнення інформації про Child. Після цього Child негайно відповість батькам.

Зробити знімок. Випадкові часові інтервали, Child отримує миттєвий знімок пристрою. Складно реалізувати за допомогою емулятора.

Надсилення SMS/MMS через MSP. Створення SMS/MMS та надсилення їх на Parentd.

Переслати зображення. Пересилати зображення, що зберігаються в Child, на електронну пошту батьків.

Запис голосу. Записувати та тимчасово зберігати голос у миттєвий час і надсилати його на електронну пошту батьків.

Запис телефонних дзвінків.

Запис телефонних дзвінків та тимчасово зберігання їх у файлі, а потім надсилання на електронну пошту батьків.

Показати місцезнаходження дитини. Показати місцезнаходження дитини за допомогою карти.

Переглянути сповіщення. Показувати сповіщення, надіслані Child.

Переглянути фотографії. Перегляд фотографій, зроблених дитиною.

Переглянути SMS-повідомлення дитини. Перегляд SMS-повідомлень, надісланих та отриманих дитиною.

3.4 Логічне подання архітектури

У цьому розділі описується логічний вигляд архітектури. Будуть описані найважливіші класи, їхня організація в пакетах послуг та підсистемах, а також організація цих підсистем за рівнями. Подальші модифікації будуть виконані мною та внесені до архітектури програмного забезпечення під час процесу розробки.

Зокрема, на рисунках 3.4 та 3.5 подано логічне представлення архітектури для батьківської та дитячої програм відповідно.

Логічне представлення системи батьківського контролю складається з 6 основних пакетів у кожному додатку, які можна розділити на три рівні.

Це система, яка працює на основі взаємодії між двома програмами, що працюють на платформі Android. Вони мають такі функції та опис їхніх обов'язків, операцій та атрибутів.

Графічний інтерфейс автентифікації. Графічний інтерфейс автентифікації містить класи для отримання доступу до системи.

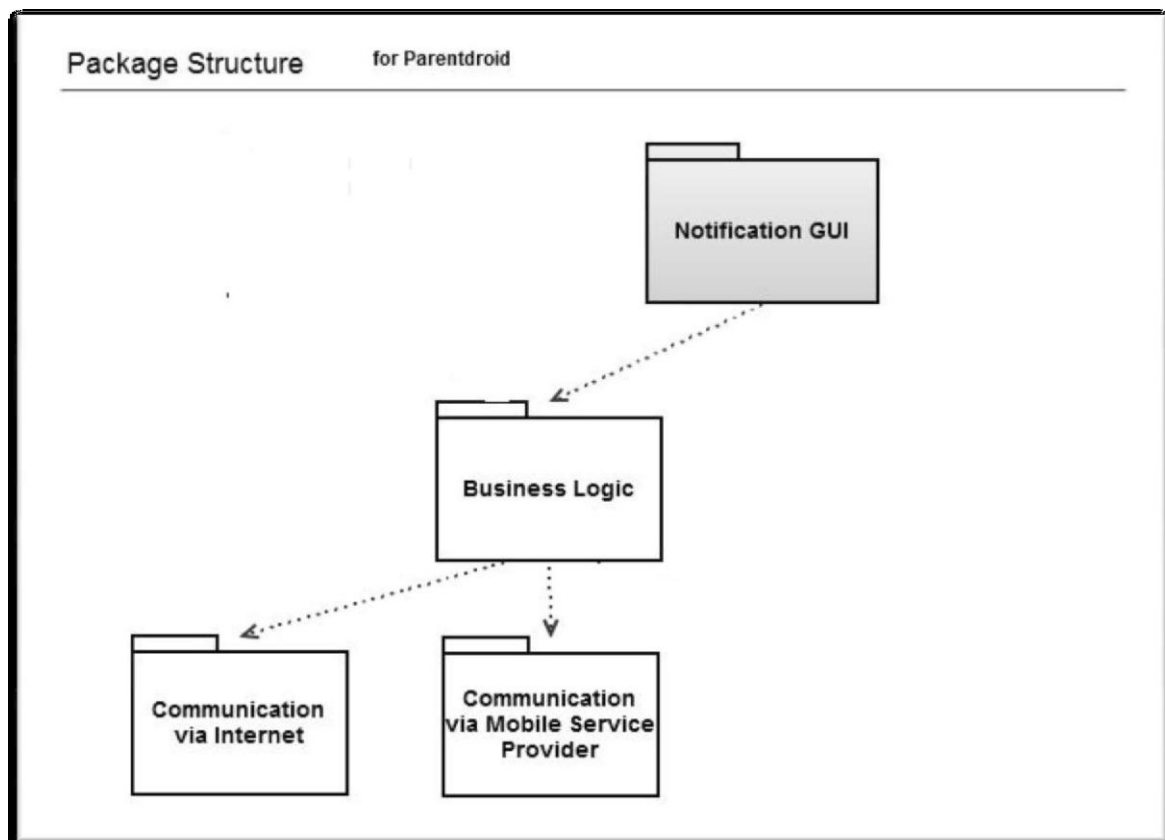


Рисунок 3.4 – Структура пакета для Parent

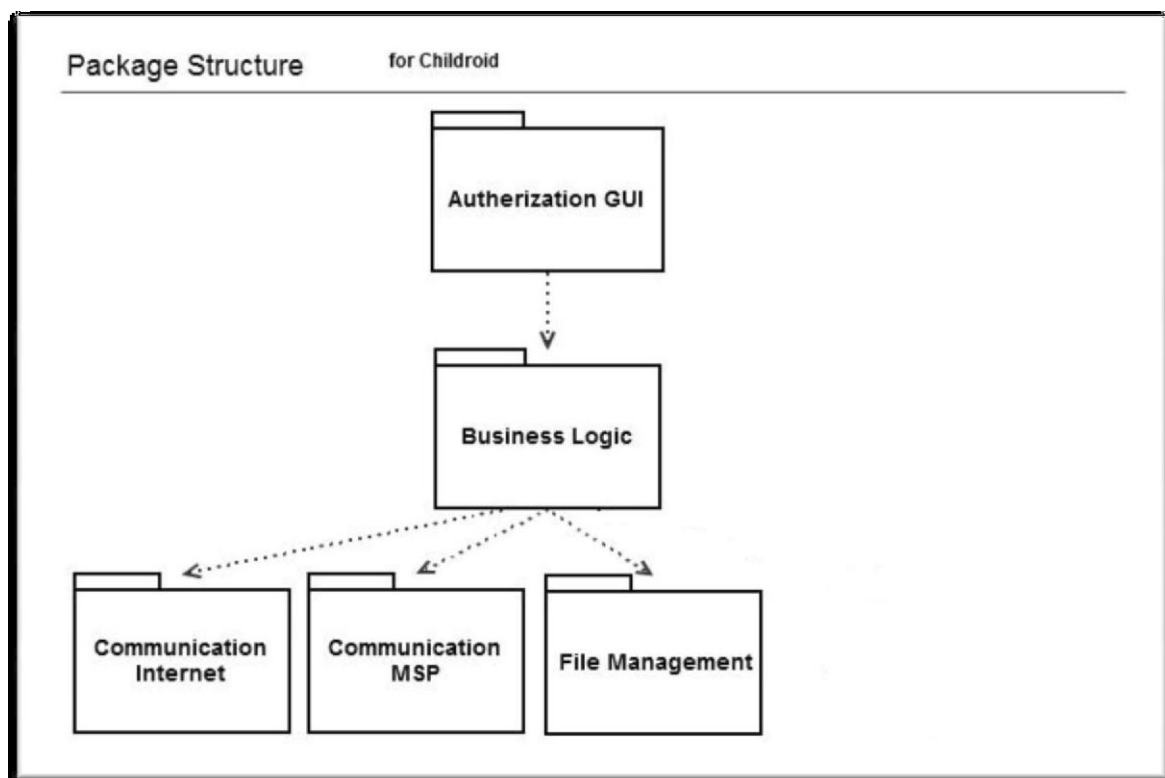


Рисунок 3.5 – Структура пакета для Child

Графічний інтерфейс сповіщень. Графічний інтерфейс сповіщень містить класи для кожної форми, яку батьківський елемент використовує для зв'язку з системою. Граничні класи існують для підтримки ведення діяльності дочірніх об'єктів, ведення нагадувань, отримання інформації шляхом миттєвого доступу та отримання попередньо встановлених сповіщень про дочірній елемент тощо.

Бізнес-логіка. Пакет бізнес-логіки містить класи керування для взаємодії з подіями, що запускають процес, підтримки доступності та керування за допомогою штучного інтелекту.

Зв'язок через Інтернет. Це проміжне програмне забезпечення для комунікації. Воно містить класи для створення електронних листів, отримання доступу до Інтернету тощо.

Зв'язок через MSP. Це проміжне програмне забезпечення для комунікації. Воно містить класи для створення SMS/MMS, отримання місцезнаходження телефону тощо.

Управління файлами. Цей пакет містить класи для доступу до файлової системи на платформі Android та отримання цих даних у будь-який час.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Аналіз небезпеки і шкідливості при розробці програмного забезпечення

Організація робочого місця розробника ПЗ впливає на його працездатність.

У своїй діяльності розробник використовує комп'ютер, пристрої збереження інформації, а тому є необхідність забезпечення зручного доступу до всіх технічних засобів. Тому в даному розділі докладніше розглянемо відомості про систему ергономічних норм і принципів організації робочого місця, на котрому проводяться роботи зі створення модуля збору статистики.

Під робочим місцем розуміється зона, оснащена необхідними технічними засобами, у якій відбувається трудова діяльність виконавця або групи виконавців, які спільно виконують одну роботу або операцію.

Організація робочого місця полягає у виконанні заходів, які забезпечують безпечний і раціональний трудовий процес і ефективне використання знарядь та предметів праці, що підвищує продуктивність праці і знижує стомлюваність працівника.

Організація робочого місця залежить від характеру розв'язуваних задач і особливостей предметно-просторового оточення, що визначають робоче положення тіла і можливість пауз для відпочинку, типи і способи засобів відображення і керування, необхідність у засобах захисту, спецодягу, простору для налагодження і ремонту устаткування.

Одним з компонентів діяльності на робочому місці є робочі рухи. Їхня раціональна організація створює умови для зниження стомлення, резерви для підвищеної працездатності. Просторові характеристики руху оператора визначаються траєкторіями руху і розмірами моторного поля (зони досяжності).

При організації робочого місця необхідно забезпечити нормальні умови огляду. Зону огляду описує кут, вершина якого знаходиться в центрі ока, а

сторони складають границі, в яких людина при фіксованому положенні голови й ока добре розрізняє їхнє місцезнаходження.

У горизонтальній площині цей кут складає 300 – 400. При організації робочого місця кут огляду можна взяти 500 – 600, включаючи зону менш ясного огляду. Допустимий кут огляду по горизонталі 900. У вертикальній площині оптимальний кут огляду 100 вгору і 300 вниз від лінії погляду, а допустимий 300 вгору і 400 вниз від лінії погляду.

Щоб зберегти нормальну гостроту зору, робочу поверхню розташовують від очей на відстані від 0,3 м до 0,75 м. Робочі меблі повинні бути зручними для виконання робочих операцій. В даному випадку робочий стіл є основним устаткуванням. Особливо важливе значення має висота столу, його конструкція, яка повинна передбачати шухляди для розміщення інструментів, документації.

Важливе значення має конструкція робочих крісел. Погано підібрані крісла можуть бути причиною надмірної стомлюваності.

Нахил і висота крісла повинні регулюватися відповідно до висоти робочої поверхні і росту працюючого. Рекомендована ширина крісла 370 – 400 мм, глибина 370 – 420 мм, висота спинки 370 – 1000 мм від рівня крісла. Для розміщення ніг необхідно передбачити вільний простір під робочою площиною [11].

Праця людини, що протікає в умовах надмірного нервово-емоційного напруження, довготривалих статичних навантажень, обмеженої рухової активності призводить до неврозів, відхилень у психіці, захворювань опорно-рухового апарату, серцево-судинної системи тощо. Комп'ютери, телебачення, системи зв'язку та інші засоби, що використовують досягнення радіоелектроніки, є генераторами цілої низки електромагнітних випромінювань, вплив яких на організм людини ще не зовсім вивчений.

З широким впровадженням автоматизації та комп'ютеризації виникла потреба врахування психологічних можливостей людини, таких як швидкість реакції, особливості пам'яті та уваги, емоційний стан та ін. Поява операторської діяльності призвела до суттєвих змін у фаховій структурі праці. Зменшилися

фізична важкість праці, ризик виробничого травматизму, однак разом з тим, на працюючу людину посилюється вплив нових, раніше не відомих чи мало вивчених несприятливих виробничих факторів фізичного, хімічного і особливо психофізіологічного характеру.

Проте, розвиток сучасної обчислювальної техніки відбувається не лише у бік покращення її технічних параметрів, але також звертається увага безпеку використання цієї техніки людиною шляхом зменшення потужності випромінювачів, зменшенням рівня випромінювання з моніторів, зменшення напруг живлення, покращення ергономічних характеристик.

Таким чином, в розділі з охорони праці виконано огляд питань безпечної роботи при створенні сайту та встановлено, що умови такої роботи відповідають вимогам з охорони праці, які застосовуються в галузі інформаційних технологій.

4.2 Інформаційно-психологічні небезпеки

Сучасні реалії постіндустріального суспільства, зумовлені значним ростом інформації, відкривають ще одну сферу життєдіяльності людини – інформаційну. Сучасні засоби комунікації і обробки інформації створили принципово нові умови існування людини, що зумовило появу грандіозного проекту об'єднання національних інформаційних і телекомунікаційних структур в глобальну інформаційну інфраструктуру.

Життєдіяльність людини реалізується одночасно зі світом природи і у специфічному для людського суспільства інформаційному середовищі, що має свої закономірності розвитку і функціонування. Інформаційна сфера стає такою ж важливою складовою суспільного життя, як економічна, виробнича, побутова, політична, військова та ін. Нові інформаційні технології, засоби масової комунікації багатократно підсилили можливості впливу на свідомість і підсвідомість як окремої людини, так і на великі групи людей та населення країни загалом.

Інформаційна сфера – сукупність таких елементів:

- об'єкти інформаційної взаємодії чи впливу;

- особисто інформація, призначена для використання суб'єктами інформаційної сфери;
- інформаційна інфраструктура, що забезпечує можливість здійснення обміну інформацією між суб'єктами;
- суспільні відносини, що складаються у зв'язку з формуванням, переданням, розповсюдженням і збереженням інформації.

Особистість, активний соціальний суб'єкт, його психіка піддаються безпосередньому впливу інформаційних чинників (передумов, що чинять опір чи утруднюють формування і функціонування адекватної інформаційно-орієнтуючої основи суспільної поведінки людини (життєдіяльності у суспільстві)), які трансформуються, через його поведінку, діяльність (бездіяльність), здійснюють деструктивний, дисфункційний вплив на його життєдіяльність.

До основних загроз інформаційно-психологічної безпеки відносять можливість настання негативних наслідків для суб'єктів, що піддаються інформаційно-психологічному впливу, які виражаються в таких формах:

- нанесення шкоди здоров'ю людини;
- блокування на неусвідомленому рівні волі, волевиявлення людини, штучне привиття їй синдрому залежності;
- втрата здатності до політичної, культурної, моральної самоідентифікації людини;
- маніпуляція суспільною свідомістю;
- руйнування єдиного інформаційного і духовного простору України, традиційних устроїв суспільства і суспільної моральності, а також порушення інших життєво важливих інтересів особистості, суспільства, держави.

Наприклад, культ жорстокості, насильства, порнографії, розбещеності тощо, які пропагують у засобах масової інформації, друкованих виданнях, комп'ютерних іграх, мережі Інтернет веде до неусвідомленого бажання у підлітків і молоді, а також дорослих з нестійкою психікою, копіювати запропоновані моделі поведінки. Цей вид пропаганди знижує рівень порогових

обмежень і правових заборон, що поряд з іншими умовами відкриває шлях для багатьох правопорушень. Це своєю чергою наносить непоправну шкоду не тільки окремій особистості, але й суттєві збитки національним інтересам країни.

Отже, джерелом інформаційно-психологічної небезпеки є та частина інформаційного середовища, яка через визначені причини неадекватно відображає реальність, вводить в оману людину, засліплює її ілюзією.

Інформаційно-психологічні загрози зумовлені розробкою, виготовленням, розповсюдженням та використанням суб'єктами негативних інформаційно-психологічних впливів, спеціальних засобів і методів такого впливу.

Концепція інформаційно-психологічної безпеки.

Сучасне розуміння безпеки в контексті врахування відношення інтересів особистості, суспільства і держави висуває завдання розгляду нового аспекту цієї проблеми – безпеки в інформаційній сфері життєдіяльності людини, тобто інформаційно-психологічної безпеки.

В інформаційному середовищі, що є складовим системним утворенням, виділяється процесуальна складова як найбільш динамічна і змінна її частина – інформаційно-комунікативні процеси, які активно впливають на індивідуальну, групову і суспільну психологію (індивідуальну, групову, масову свідомість). Маніпулюючи станом інформаційного середовища, змінюється стан духовної сфери суспільства, деформація і деструктивні зміни якої у формі психоемоційної і соціальної напруженості, спотворених норм і неадекватних соціальних стереотипів і установок, оманливих і неприродних орієнтацій та цінностей. Це своєю чергою впливає на стан і процеси у всіх основних сферах суспільного життя, в тому числі політичній і економічній.

Вперше у пострадянському просторі про проблему інформаційно-психологічної безпеки було зазначено в листопаді 1995 р. на науково-практичній конференції, організованій Інститутом психології Російської академії наук. На цій та подальших конференціях було розкрито роль знання технологій інформаційно-психологічного впливу, метою якого є маніпуляція, для

вироблення напрямів реформування психологічного захисту особистості і особистої інформаційно-психологічної безпеки.

Інформаційно-психологічну безпеку особистості визначають такими основними причинами.

Зростання тиску інформаційного середовища визначає необхідність формування нових механізмів та засобів виживання людини як особистості й активного соціального суб'єкта у сучасному суспільстві.

Взаємодія психіки людини з інформаційним середовищем відрізняється якісною специфікою і не має аналогів у комунікації інших біологічних, технічних, соціальних і соціотехнічних структур.

Основною і центральною "мішенню" інформаційного впливу є людина, її психіка.

Отже, інформаційно-психологічну безпеку можливо розглядати як стан захищеності особистості, різних соціальних груп і об'єднань людей від дій, впливів, які здатні проти їхньої волі і бажання змінити психічні стани та психологічні характеристики людини, модифікувати її поведінку і обмежувати свободу вибору, зумовило потребу переосмислення інформаційної взаємодії, а також деяких інших соціально-психологічних процесів і явищ у сучасному суспільстві.

Інформаційно-психологічна безпека – стан захищеності окремих осіб чи груп осіб від негативних інформаційно-психологічних впливів і пов'язаних з цим інших життєво важливих інтересів особистості, суспільства, держави в інформаційному середовищі.

Негативний інформаційно-психологічний вплив – процес зміни психічних станів і характеристик людей під впливом інформаційно-комунікативних процесів як динамічного компонента інформаційного середовища. Цей вплив спрямований на людину чи групу осіб (у тому числі без їхньої згоди) з метою примусу до визначеної поведінки, оцінки ситуації, керування та корекції індивідуальної та колективної свідомості. Він здійснюється з використанням

спеціальних засобів і методів впливу на психіку людини, унаслідок чого він приводить до негативних наслідків для особистості, суспільства і держави.

Спеціальні засоби впливу – технічні і програмні засоби, що використовують для використання з метою негативного інформаційно-психологічного впливу на людину чи групу людей.

Спеціальні методи впливу – послідовність прийомів впливу на психіку людини, використання яких приводить до негативних наслідків для особистості, суспільства та держави.

Головним об'єктом забезпечення інформаційно-психологічної безпеки в інформаційному середовищі у сфері індивідуальної безпеки є усвідомлення інформації, здатність людини адекватно сприймати навколишню дійсність, своє місце в зовнішньому світі, формувати відповідно до свого життєвого досвіду визначені переконання і приймати стосовно них рішення.

Інформаційно-психологічна безпека має спиратися на стандарти інформаційно-психологічної безпеки – затверджені у визначеному порядку інформаційно-психологічного впливу, який не викликає негативних наслідків для психіки людини.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було підтверджено актуальність створення застосунків батьківського контролю, зважаючи на стрімке зростання використання мобільних пристроїв серед дітей. Статистичні дані та аналітичні звіти засвідчують, що більшість дітей у розвинених країнах мають смартфони вже у віці до 10 років, що підвищує ризики взаємодії з неприйнятним контентом, кібербулінгом та іншими цифровими загрозами. У цьому контексті розробка ефективного мобільного додатку для контролю дитячої активності в інтернеті є вкрай важливою і соціально значущою задачею.

У першому розділі роботи проведено ґрунтовний огляд предметної області. Визначено ключові функції, які має реалізовувати якісний застосунок для батьківського контролю, серед яких – блокування додатків, фільтрація контенту, контроль екранного часу, відстеження місцезнаходження та моніторинг цифрової активності. Наведено приклади провідних рішень, які вже представлені на ринку, таких як Qustodio, FamilyTime, Norton Family, Net Nanny та інші, що дозволило сформулювати цілісний погляд на функціональні стандарти подібних систем.

Другий розділ зосереджено на аналізі функціональних і нефункціональних вимог до розроблюваного програмного забезпечення. Встановлено необхідність підтримки масштабованості, безпеки даних, інтеграції з іншими сервісами (через API/SDK), економічної ефективності, зручності інтерфейсу та підтримки різних моделей монетизації (freemium, підписка, покупки в додатку). Значну увагу приділено дотриманню вимог конфіденційності, зокрема використанню шифрування, політик згоди користувача, а також відповідності локальним і міжнародним нормам захисту даних.

У третьому розділі було розроблено архітектурну модель додатку згідно з підходом «4+1», що включає логічне, процесне, фізичне, реалізаційне та сценарне подання системи. Створено розподілену систему, яка передбачає взаємодію двох окремих додатків – на пристрої батьків та на пристрої дитини.

Розглянуто детальний перелік сценаріїв використання, включаючи зчитування місцезнаходження, запис дзвінків, моніторинг SMS, керування додатками та контентом. Розробка враховувала використання сучасних інструментів, таких як MBaaS (наприклад, AWS Amplify), SDK для шифрування (AWS Encryption SDK), API для повідомлень (Twilio) та платіжних систем (Stripe).

Отже, проведене дослідження, аналіз ринку та архітектурна розробка створили підґрунтя для реалізації повноцінного, безпечного, функціонального застосунку батьківського контролю, орієнтованого на платформу Android. Отримані результати можуть бути основою для подальшої розробки MVP-продукту з перспективою масштабування, доповнення функціоналу та комерціалізації на глобальному рівні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kharchenko, A., Raichev, I., Bodnarchuk, I., & Matsiuk, O. (2021, October). The Survey of Global Software Design Processes. In 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T) (pp. 291-294). IEEE.
2. Боднарчук, І. О., Карнаухов, О., Лобур, Т. Б., & Марценко, С. В. (2025). Порівняння мов програмування Julia та Python для вирішення наукових і математичних задач. Матеріали Міжнародної науково-технічної конференції „Фундаментальні та прикладні проблеми сучасних технологій“, присвячена 180-річчю з дня народження Івана Пулюя та 65-річчю з дня заснування Тернопільського національного технічного університету імені Івана Пулюя, 180-181.
3. Orobchuk, B., Buniak, O., Sysak, I., Babiuk, S., Bodnarchuk, I., & Koval, V. (2024). Development of Software for the Implementation of Automated Reserve Input Modes Operation. In 2nd International Workshop on Computer Information Technologies in Industry (Vol. 4, pp. 12-14).
4. Parental Control Software Market Size, Share & Growth [2032]. Fortune Business Insights™ | Global Market Research Reports & Consulting. URL: <https://www.fortunebusinessinsights.com/parental-control-software-market-104282> (date of access: 02.06.2025).
5. D N. B. M. What Is The Best Age For A Child's First Smartphone?. Forbes Health. URL: <https://www.forbes.com/health/family/best-age-for-first-cell-phone/#:~:text=Recent%20survey%20data%20suggests%2042,the%20complexity%20of%20this%20decision>. (date of access: 22.03.2025).
6. Ofcom. Children and Parents: Media Use and Attitudes. <https://www.ofcom.org.uk>. (date of access: 22.03.2025).
7. Material Design. Material Design. URL: <https://m3.material.io/> (date of access: 21.03.2025).

8. A Comprehensive Guide To Mobile App Design – Smashing Magazine.
Smashing Magazine. URL: <https://www.smashingmagazine.com/2018/02/comprehensive-guide-to-mobile-app-design/> (date of access: 12.04.2025).
9. Nick Babich. 10 Do's and Don'ts of Mobile UX Design | Adobe XD Ideas.
Ideas. URL: <https://xd.adobe.com/ideas/principles/app-design/10-dos-donts-mobile-app-design/> (date of access: 08.04.2025).
10. Kruchten, P. B. (1995). The 4+ 1 view model of architecture. IEEE software, 12(6), 42-50.
11. Стручок, В. С., Стручок, О. С., & Мудра, Д. В. (2017). Навчальний посібник до написання розділу дипломного проекту та дипломної роботи "Безпека в надзвичайних ситуаціях "для студентів всіх спец. денної, заочної (дистанційної) та екстернатної форм навчання.
12. Стручок, В. С. (2022). Техноекологія та цивільна безпека. Частина "Цивільна безпека". Навчальний посібник.
13. Жидецький, В. Ц., Джигирей, В. С., & Мельников, О. В. (2000). Основи охорони праці. Львів: Афіша, 350, 132-136.
14. Навакатікян, О. О., Кальниш, В. В., & Стрюков, С. М. (1997). Охорона праці користувачів комп'ютерних відеодисплейних терміналів. О. Навакатікян.

ДОДАТКИ

Програмний код

MapViewActivityTest.java

```
package parentalcontrol.parent.test.GUI;

import parentalcontrol.parent.GUI.MapViewActivity;
import android.test.SingleLaunchActivityTestCase;
import android.widget.TextView;

public class MapViewActivityTest extends
SingleLaunchActivityTestCase<MapViewActivity>{

    private MapViewActivity mActivity;
    private String resourceString;
    private TextView mView;
    private TextView map;

    public MapViewActivityTest() {
        super("parentalcontrol.parent.GUI",
MapViewActivity.class);
    }

    @Override
    protected void setUp() throws Exception {
        super.setUp();
        mActivity = this.getActivity();
        mView = (TextView)
mActivity.findViewById(parentalcontrol.parent.R.id.mapView);
        map = (TextView)
mActivity.findViewById(parentalcontrol.parent.R.id.txmapview);
        resourceString =
mActivity.getString(parentalcontrol.parent.R.string.mapviewtopi
c);
    }

    public void testPreconditions() {
        assertNotNull(mView);
    }

    public void testText() {
        assertEquals(resourceString, (String) map.getText());
    }
}
```

ParentdroidActivityTest.java

```
package parentalcontrol.parent.test.GUI;

import parentalcontrol.parent.GUI.ParentdroidActivity;
```

```

import android.test.SingleLaunchActivityTestCase;
import android.widget.TextView;

public class ParentdroidActivityTest extends
SingleLaunchActivityTestCase<ParentdroidActivity>{

    private ParentdroidActivity mActivity;
    private String resource1;
    private TextView mView1;
    private String resource2;
    private TextView mView2;

    public ParentdroidActivityTest() {
        super("parentalcontrol.parent.GUI",
ParentdroidActivity.class);
    }

    @Override
    protected void setUp() throws Exception {
        super.setUp();
        mActivity = this.getActivity();
        mView1 = (TextView)
mActivity.findViewById(parentalcontrol.parent.R.id.buttonMain);
        resource1 =
mActivity.getString(parentalcontrol.parent.R.string.showmsgbutt
on);
        mView2 = (TextView)
mActivity.findViewById(parentalcontrol.parent.R.id.showmsgbutto
n1);
        resource2 =
mActivity.getString(parentalcontrol.parent.R.string.showsmsrece
ive);
    }

    public void testPreconditions() {
        assertNotNull(mView1);
        assertNotNull(mView2);
    }

    public void testText() {
        assertEquals(resource1, (String) mView1.getText());
        assertEquals(resource2, (String) mView2.getText());
    }
}

```

SMSReceiveActivityTest.java

```

package parentalcontrol.parent.test.GUI;
import parentalcontrol.parent.GUI.SMSReceiveActivity;
import android.test.SingleLaunchActivityTestCase;
import android.widget.TextView;

```

```

public class SMSReceiveActivityTest extends
SingleLaunchActivityTestCase<SMSReceiveActivity>{

    private SMSReceiveActivity mActivity;
    private String resourceString;
    private TextView mView;

    public SMSReceiveActivityTest() {
        super("parentalcontrol.parent.GUI",
SMSReceiveActivity.class);
    }

    @Override
    protected void setUp() throws Exception {
        super.setUp();
        mActivity = this.getActivity();
        mView = (TextView)
mActivity.findViewById(parentalcontrol.parent.R.id.tvsmsreceive
);
        resourceString =
mActivity.getString(parentalcontrol.parent.R.string.smsreceivet
xt);
    }

    public void testPreconditions() {
        assertNotNull(mView);
    }

    public void testText() {
        assertEquals(resourceString, (String) mView.getText());
    }
}

```

SMSSendActivityTest.java

```

package parentalcontrol.parent.test.GUI;

import parentalcontrol.parent.GUI.ActionActivity;
import android.test.SingleLaunchActivityTestCase;
import android.widget.TextView;

public class SMSSendActivityTest extends
SingleLaunchActivityTestCase<ActionActivity> {

    private ActionActivity mActivity;
    private String resourceString;
    private TextView mView;

    public SMSSendActivityTest() {

```

```

        super("parentalcontrol.parent.GUI",
ActionActivity.class);
    }

    @Override
    protected void setUp() throws Exception {
        super.setUp();
        mActivity = this.getActivity();
        mView = (TextView) mActivity

.findViewById(parentalcontrol.parent.R.id.labelphonenum);
        resourceString = mActivity

.getString(parentalcontrol.parent.R.string.labelchildnum);
    }

    public void testPreconditions() {
        assertNotNull(mView);
    }

    public void testText() {
        assertEquals(resourceString, (String) mView.getText());
    }
}

```