

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы
«Ақпараттық қауіпсіздік жүйелері» кафедрасы

«ҚОРҒАУҒА ЖІБЕРІЛДІ»

Кафедра меңгерушісі с.ғ.к., доцент Бердібаев Р. Ш.
_____ « _____ » _____ 2019 ж.
(колы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: «Қорғалған мобильді қосымшаларды әзірлеу»
Мамандығы: 5В100200 – «Ақпараттық қауіпсіздік жүйелері»
Орындаған: Сарсембаев Мурат Тобы: СИБк-15-1
Ғылыми жетекші: с.ғ.к., доцент Бердібаев Р. Ш.

Кеңесшілер:

Экономикалық бөлім бойынша:

Э.ғ.к. профессор Бердібаев Р. Ш.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ « 13 » 05 2019 ж.
(колы)

Тіршілік қауіпсіздігі бөлімі бойынша:

ата оқушы Төртеев Ә. Ә.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ « 2 » 05 2019 ж.
(колы)

Есептеу техникасын қолдану бойынша:

т.ғ.к., доцент Шайкырова А. А.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ « 21 » 05 2019 ж.
(колы)

Мөлшер бақылаушы:

ата оқушы, т.ғ.к. Ақарова Н. Б.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ « 4 » 06 2019 ж.
(колы)

Пікір беруші:

т.ғ.к., ассистент-профессор Сетпиева Н. А.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ « 31 » 05 2019 ж.
(колы)

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы

Басқару және ақпараттық технологиялар институты
Ақпараттық қауіпсіздік жүйелері кафедрасы
5В100200 – «Ақпараттық қауіпсіздік жүйелері» мамандығы

Дипломдық жобаны орындауға берілген
ТАПСЫРМА

Студент: Сарсебайев Аурат Ахмедұлы
(аты-жөні)

Жобаның тақырыбы: Қорғалған мобильді қосымшаларға
Әзірлеу

2018 ж. «26» 10 № 124 университет бұйрығымен бекітілді.

Аяқталған жұмысты тапсыру мерзімі: « » 20 ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері):

Мобильді қосымша құрылым теориялық негіздерін іздеу.
Мобильді қосымшалардан артықшылықтар мен
кемшіліктерін қарау. Мобильді қосымшаларға
төнетін қауіптер және олардан қорғану алаңдары
Android операциялық жүйесі үшін қосымшаларға
Әзірлеу және оны іске қосу.

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны:

1. Мобильді қосымшалардан артықшылықтар мен
кемшіліктері
2. Мобильді қосымша құру процесі
3. Теориялық қалыптастыру әзірлеудің әзірлік циклі
4. Шабуылдар түрлері және оның категориялары
5. Табылған шабуылдар
6. Мобильді қосымшалар қауіпсіздігін қалыптасу

- 8) Үлгі әдістері мен куралдары
 9) Web-қосымша құрылымы
 8. Жаншаралық және экономикалық қарқынды
 9. Өміршілік қауіпсіздігі
 10. Қорытынды

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды қорсету) тізімі:

1. "AVIA 45" мобильдік қосымшасы
2. Web-қосымша құрылымы
3. Смартфонға қарайтын көрсеткіші
4. ОЖ бойынша смартфонға қарайтын сабақ көрсеткіші
5. Мобильді қосымшалар
6. Аралық қосымшалар

Негізгі ұсынылатын әдебиеттер:

1. Толочанов А. Google Android: программирование для мобильных устройств - СПб.: БХВ-Петербург, 2010. 448 с. - ISBN 978-5-97775-0562-8.
2. Дронов В. А. Разработка современных Web-сайтов - СПб.: БХВ-Петербург, 2013 - 414 с. 5.

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

Бөлімдері	Кеңесшілері	Мерзімі	Қолы
Өміршілік қауіпсіздігі	Шайкенова А.А.	12.02 - 21.05	Шайкенова А.А.
Экономика	Ибрагимов Д.Д.	01.04 - 20.05	Ибрагимов Д.Д.
	Ахмедов М.Г.	04.03 - 13.05.19	Ахмедов М.Г.

Диплом жобасын дайындау
КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелердің тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
1. Ресей және Қазақстандағы мобильді қосымшалар тарқатуына талдау.	12.02.2019	
2. Мобильді қосымшалар жасау құралдары мен әдістері	14.03.2019	
3. Мобильді қосымша құрудың теориялық негіздері	10.04.2019	
4. Мобильді қосымшаның құру және қауіпсіздік шарасын қадағалау	18.04.2019	
5. Мобильді қосымшаның іске қосу	26.04.2019	
6. Интернет желісінде мобильді қосымшаның оарату жобалары	29.04.2019	
7. Экономикалық-экономикалық негіздері	13.05.2019	
8. Әміртірінінің қауіпсіздігі	20.05.2019	
9. Қорытындылар, жұмыс нәтижесі	21.05.2019	

Тапсырманың берілген уақыты « _____ » _____ 20__ ж.

Кафедра меңгерушісі _____ (С.З.К. доцент Қаржибаев А.И.)
(қолы) (аты-жөні)

Жобаның ғылыми жетекшісі _____ (Майкирова А.А.)
(қолы) (аты-жөні)

Орындалатын тапсырманы қабылдаған студент _____ (Сарсаубаев М.Т.)
(қолы) (аты-жөні)

АНДАТПА

Дипломдық жоба қорғалған мобильді қосымша әзірлеуге арналған. Ресей және Қазақстандағы мақсатты аудиториямен байланыс процесіндегі заманауи мобильді қосымшалардың рөлі, мобильді қосымшаны әзірлеудің негізгі ұйымдастырушылық, экономикалық және технологиялық ерекшеліктері, мобильді қосымшаны құруға негіздеме беру және оны құру кезеңдерін зерттеу қарастырылған. Мобильді қосымшаларға төнетін қауіптерге талдау жасалып, қауіпсіздік мәселелерін шешу жолдары ұсынылған. Тақырыпқа сәйкес ойынға арналған мобильді қосымша әзірленіп, құрылған мобильді қосымшаның қауіпсіздігін қамтамасыз ету үшін парольдік қорғау механизмі және обфускация процедурасы қолданылған. Қосымша әзірлеуде Android Studio 3.1.3 интеграцияланған әзірлеу ортасы, ProGuard (коды Java тілінде жазылған) кодты бұрмалау жабдығы қолданылған.

АННОТАЦИЯ

Дипломный проект предназначен для разработки защищенного мобильного приложения. Предусмотрено изучение роли современных мобильных приложений в процессе связи с целевой аудиторией в России и Казахстане, основных организационных, экономических и технологических особенностей разработки мобильного приложения, этапов создания и обоснования создания мобильного приложения. Были проанализированы угрозы, угрожающие мобильным приложениям, предложены пути решения проблем безопасности. В соответствии с темой разработано мобильное приложение для игры с использованием механизма парольной защиты и процедуры обфускации для обеспечения безопасности созданного мобильного приложения. В разработке использовались интегрированная среда разработки Android Studio 3.1.3, оборудование для искажения кода ProGuard (код записан на языке Java).

ANNOTATION

The diploma project is designed to develop a secure mobile application. It is planned to study the role of modern mobile applications in the process of communication with the target audience in Russia and Kazakhstan, the main organizational, economic and technological features of mobile application development, the stages of creation and justification of mobile application creation. In accordance with the theme, a mobile application for the game was developed using the password protection mechanism and obfuscation procedure to ensure the security of the created mobile application. In the development used the integrated development environment Android Studio 3.1.3, equipment for the distortion of code ProGuard (code written in the Java language).

Мазмұны

Кіріспе.....	3
1 Мобильді қосымша құрудың теориялық негіздері.....	4
1.1 Ресей және Қазақстандағы мобильді қосымшалар нарықтарына талдау.....	6
1.2 Мобильді қосымшалардың артықшылықтары мен кемшіліктері.....	8
1.3 Forbes Kazakhstan нұсқасы бойынша мобильді қосымшалардың жыл сайынғы ахуалы туралы ақпарат.....	12
1.4 Мобильді қосымша нарығындағы бәсекелестік.....	15
1.5 Ұялы телефон иелері нені пайдаланады.....	17
1.6 Мобильді қосымшалар жасау кезеңдері. Оның ұйымдастырушылық, экономикалық, маркетингтік аспектілері. Мобильді қосымшалар жасау құралдары мен әдістері.....	20
1.6.1 Мобильді қосымшалардың түрлері.....	22
1.6.2 Мобильді қосымша құру процесі.....	25
1.6.3 Әзірлеме дайындау. Сипаттамасын талқылау және қажетті түзетулер енгізу.....	26
1.6.4 Мобильді қосымша құру кезеңдері.....	27
1.6.5 Программалық қамтама әзірлеудің өмірлік циклі.....	28
1.7 Мобильді қосымшалар жасау құралдары мен әдістері.....	29
1.7.1 Android Studio 3.1.3 интеграцияланған әзірлеу ортасы.....	30
1.7.2 Java тарихы, мүмкіндіктері.....	31
2 Мобильді қосымшаларға төнетін қауіптер. Олардан қорғану шаралары.....	32
2.1 Шабуылдар түрлері, категориялары.....	35
2.2 Веб-қосымшалардағы шабуылдар және оларға қарсы іс-қимыл әдістері.....	36
2.2.1 Пакеттер сиффері.....	37
2.2.2 IP-спуфинг.....	40
2.2.3 Қызмет көрсетуден бас тарту.....	43
2.2.4 Парольдік шабуылдар.....	46
2.2.5 Man-in-the-Middle типті шабуылдар.....	48
2.2.6 Деректерді жинау шабуылынан қорғау (Fingerprinting).....	49
2.2.7 Қауіпсіздік концепциясына жоғарғы деңгейде енгізу.....	50
2.2.8 XSS (сайт аралық скриптинг).....	53
2.2.9 SQL кодты енгізу (SQL-injection).....	55
2.2.10 Сессияны/сертификатты болжау (Credential/Session Prediction).....	56
2.2.11 Серверді дұрыс орнатпау (Server Misconfiguration).....	57
2.2.12 CSRF.....	59
2.3 Мобильді қосымшалар қауіпсіздігін қамтамасыз ету әдістері мен құралдары.....	60

2.4 Android ОЖ қорғау компоненттері.....	61
2.5 Реверс-инжинирингтен Android қосымшаларын қорғау.	
Обфускация.....	62
2.5.1 ProGuard.....	63
2.5.2 DexGuard.....	65
3 Мобильді қосымшаны құру және қауіпсіздік шарасын қамту.....	66
3.1 Web-қосымша құрылымы.....	68
3.2 Android ОЖ үшін қосымша әзірлеу.....	69
3.3 ProGuard – кодты бұрмалау процедурасы.....	70
3.4 Мобильді қосымшаны іске қосу.....	71
3.5 Интернет желісінде мобильді қосымшаны тарату жоспары.....	72
4 Техникалық және экономикалық негіздеме.....	73
4.1 Жобаның сипаттамасы.....	74
4.2 Еңбек сыйымдылығы.....	75
4.3 Әзірлеуге арналған шығындарды есептеу.....	76
4.4 Еңбекақы төлеу шығындарын есептеу.....	77
4.5 Әлеуметтік салық бойынша шығындарды есептеу.....	78
4.6 Негізгі қорлардың амортизациясы және өзге де шығындар.....	78
4.7 Ықтимал (шарттық) бағасын анықтау.....	79
Қорытынды.....	81
Әдебиеттер тізімі.....	82

Кіріспе

Кез келген кәсіпорынның болашағы үшін мобильді немесе веб-сервистерді дамыту компания үшін мобильді қосымшаны құру – бұл аудиторияның қызығушылығын арттыру және бизнесті жылжыту тәсілі.

Android, iOS немесе Windows платформаларға арналған қосымшаларды жасау – компанияның трендінде екенін айқын. Қолданушыға сайттың үлкен нұсқасында болу әрдайым ыңғайлы емес, сондықтан жеңіл және қолжетімді балама қажет.

Таңдалған тақырыптың өзектілігі Android, iOS және WindowsPhone операциялық жүйелеріндегі ұялы телефондарды пайдаланушылардың саны күн сайын өсуімен байланысты. Адамдар смартфон арқылы шексіз ақпаратқа қол жеткізетінін түсінеді: бухгалтерияны жүргізіп, медиаконтентті көріп, пайдалы бағдарламалар мен ойындар орната алады, сондай-ақ өз демалысын жоспарлай алады. Осы арқылы мобильді қосымшалар нарығын көптеген адамдар жұмыс істейтін перспективалы сала деп атауға болады.

Телефонмен күннің негізгі бөлігін өткізетін адам оның құрылғысында бар қосымшаның қол жетімді болғанын қалайды. Мысалы, ол қандай да бір бағдарламадан хабарларды көреді, жұмыс үстеліндегі белгішені пайдалана отырып, оған кіре алады және тиісінше оның мазмұнымен таныса алады. Осыны ескере отырып, әзірлеушілер қарапайым пайдаланушылардың смартфондары мен планшеттері үшін нағыз қажет программалар әзірлеуде жарысқа түсуде. Шын мәнінде, қазіргі заманғы технологиялардың көмегімен ойын-сауық бағдарламаларын таратуға немесе ойын-сауық бағдарламаларын шығаруға, оларда жарнамалап пайда табуға, сонымен қатар клиенттерге өз қызметтерін, өнімдерін ұсынуға, олардан пікірлер жинауға және т.б. мүмкіндік алуға болады. Мобильді қосымшалар кез келген бизнестің қуатты қозғалтқышы бола алады.

Мәселен, клиенттерге арналған мобильді қосымшалармен бүгінгі күні бұқаралық секторларда жұмыс істейтін ұйымдар да, корпоративтік нарықта шоғырланған ұйымдар да айналысады. Клиенттер үшін мобильді қосымшаны шығару – сәнге айналды, ол басқалары үшін – маңызды қажеттілік болса, үшіншіден – бизнес үшін жаңа мүмкіндіктерді игеру болып табылады.

Зерттеудің мақсаты мобильді қосымшаны әзірлеу және қолданысқа енгізу, қауіпсіздігін қамтамасыз ету процесі болып табылады.

Қойылған мақсатқа жету үшін бірқатар міндеттерді шешу қажет:

- мақсатты аудиториямен байланыс процесінде заманауи мобильді қосымшалардың рөлін қарастыру;
- мобильді қосымшаны әзірлеудің негізгі ұйымдастырушылық, экономикалық және маркетингтік ерекшеліктерін зерттеу;
- мобильді қосымшаны құруға негіздеме беру және оны құру кезеңдерін зерттеу;
- құрылған мобильді қосымшаның қауіпсіздігін қамтамасыз ету бағалау.

Бұл жұмыста зерттеу нысаны мобильді құрылғыларға арналған қосымшалар болып табылады.

Зерттеу тақырыбы – әлеуетті келушілердің санын арттыру үшін мобильді қосымшаны құру және қолданысқа енгізу бойынша іс-шаралар кешені болып табылады.

1 Мобильді қосымша құрудың теориялық негіздері

1.1 Ресей және Қазақстандағы мобильді қосымшалар нарықтарына талдау

Қазіргі уақытта мобильді технологияларды дамытуда айтарлықтай ілгерілеу байқалуда: планшеттік компьютерлер қаншалықты танымал болғанын атап өткен жөн, олар іс жүзінде Ноутбуктерді ығыстырды десе де болады. Компьютерлердің пайдаланушылары Интернет-мобильді нұсқаларға толыққанды шығуды қалайды.

Мобильді қосымша – мобильді серверге қосылатын және пайдаланушы интерфейсі мен құрылғының бизнес-логикасын басқаратын мобильді құрылғыға орнатылатын компонент.

Мобильді құрылғыларға арналған қосымшалар нарығының сегменті 2008 жылы толыққанды қалыптасты. Қосымшаларды таратудың жаңа үлгісін іске қосқан Apple компаниясы болды.

Біраз уақыттан кейін бұл нарыққа Google компаниясы шықты, ол Apple үшін елеулі бәсекелес болды. Бастапқыда vas (Value Added Services) моделі бойынша мобильді контентті таратқан ұялы байланыс операторлары – дауыс беруден басқа, ұялы байланыстың барлық қызметтері жататын ұялы байланыс желілеріндегі қосымша қызметтер жиынтығы. Бұл сервистерге: MMS-хабарламалар, әртүрлі контенттік қызметтер (тақырыптық тарату, күту гуілдерін әуендермен ауыстыру және т.б.), деректерді беру қызметтері (GPRS немесе 3G технологиясы бойынша), LBS – қызметтер (телефонның желіде орналасқан жері бойынша абоненттің орналасқан жерін анықтау), корпоративтік желі ресурстарына қашықтан қорғалған қатынау қызметтері және т. б. жатады. Олар ұялы құрылғыларға арналған қосымшалар нарығындағы өз әрекеттерін оған жаңа платформалардың келуі арқылы өзгертті және қазіргі уақытта контентті таратудың жаңа моделіне белсенді түрде кірісуде.

Мобильді қосымшалар нарығы кез келген нарық сияқты екі іргелі көрсеткішпен сипатталады: "сұраныс" және "ұсыныс". Егер консалтингтік агенттіктердің, атап айтқанда J'son & Partners Consulting деректеріне сенсек, 2016 жылдың соңына қарай мобильді қосымшалар нарығының көлемі 2015 жылмен салыстырғанда 167% - ға өскен және өсу үрдісі сақталуда, бұл мобильді технологиялардың өсіп келе жатқан танымалдылығымен және олардың қосымшалар дүкендері мен IT индустриясының көшбасшылары тарапынан белсенді жылжуымен түсіндіріледі. Ұсыныс тұрғысынан, мобильді қосымшалар нарығында барлық тапсырыстардың 80%-ға жуығын ірі әзірлеушілер иемденіп отыр, аз үлесі шағын компанияларға тиесілі [1].

Қазіргі уақытта Ресейдің мобильді жүйесі жақында енгізілген технологиялық бейтараптылық принципі нәтижесінде күшті өзгерістерге ұшырап отыр. Бұл ойыншылардың көп санына монополиялаған мобильді телекоммуникация нарығына кіруге мүмкіндік берді.

Ритейлдегі бизнес-қосымшалар сегментінің өсуі. Мысалы, 2014 жылы

Lifestyle and shopping санатындағы Мобильді қосымшаларды пайдалану 174%-ға артты – бұл барлық өзге санаттарға қарағанда көп. Ритейлерлер өз бизнесі үшін мобильді арнаның көптеген мүмкіндіктерін ашқан, шоппинг-қосымшалар сегментіндегі өсім Ресейде де, әлемде де жалғасуда.

Өсіп келе жатқан бәсекелестік нәтижесінде қызметтердің сапасы жақсарып, бағалар біртіндеп төмендеуде. Сонымен қатар, мобильдік операторлар бұдан былай заң бойынша өз лицензияларын алу және сақтау үшін халық саны 1000 және одан да көп адам болатын елді мекендерде таратылуға міндетті. Жақында Marketer зерттеуіне сәйкес 2014 жылы 80%-ды құраған ұялы байланыстың таралу деңгейі 2017 жылға қарай 6%-ға өскен, ал Ресейде мобильді интернетті пайдаланушылар саны 2014 жылы 61,5 млн. болса, 2017 жылы 88,1 млн. - ға дейін артқан.

Сонымен қатар, статистикаға сәйкес, осыдан бес жыл бұрын мобильді құрылғылар арқылы интернетті пайдаланушылардың пайызы 10%-дан аспаған, ал 2015 жылдың соңында Интернеттегі мобильді құрылғыларды пайдаланушылардың үлесі 65%-дан асып түсті. Ұзақ уақыт бойы зерттеу жүргізілген жоқ, оның есептері жақын арада, ал егер дәлірек айтар болсақ, 2020 жылға қарай мобильді интернетті қамту бүкіл жер шарының 90%-ын алады. Мобильді интернеттің танымалдылығының айтарлықтай секірісін, әрине, желілердің мобильді түрлерін қосу және дамытуға арналған құрылғылардың портативтілігімен байланыстыруға болады.

Осы статистикаға сәйкес, мобильді интернеттің өсу шамасына қарай осы интернет қосылатын түрлі смартфондар саны да өсетін болады. Егер зерттеулерге сенсек, смартфондар саны 50%-ға өседі. Бұл халықтың көпшілігі үшін смартфондардың қолжетімділігінің айтарлықтай артуына байланысты.

Қазақстанда смартфондар түрлі мақсатта пайдаланылады. Ең жиі қолданылатын сала – онлайн бейнероликтер көру, әлеуметтік желілермен жұмыс, сондай-ақ ақпарат іздеу.

Google тапсырысы бойынша TNS Infratest компаниясы жүргізген Connected Consumer Survey 2016 зерттеулерінің нәтижесі Қазақстандықтардың үштен екісінің смартфондар қолданатынын анықтаған. Бұл кеңестік заман кеңістігіндегі алдыңғы қатарлы көрсеткіштерді білдіреді.

25 пен 35 жас аралығындағы жастардың смартфондар қолдану көрсеткіші 91% және 85%-дық көрсеткіштер арасында болып отыр. Бір қазақстандық орташа есеппен интернетке 2,1 рет қосылады екен. Зерттеу нәтижелері бойынша мынадай мақсаттарда қолданылатыны белгілі болды:

- онлайн-видео (47%);
- әлеуметтік желілерде отыру (46%);
- ақпарат іздеу (41%).

86% қазақстандық интернет-қолданушылар онлайн режимде отырады екен. Оның ішінде жас ерекшеліктеріне байланысты мынадай көрсеткіштер анықталып отыр:

- 25 жасқа дейінгілердің күн сайын интернетті пайдалануы – 93%;
- 25-34 жастағылар – 94%;

- 55 және одан жоғары жастағылар – 66%.

Зерттеу барысында анықталғандай, 37% қазақстандық интернеттен қандай да бір өнім туралы, қызмет түрлері туралы сұраныс жасайды. Осы мақсатта смартфондарды қолданатындардың көрсеткіші 88% -ды құрап отыр (бұған барлық жас категориялары кіреді). Бұл деген мобильді қосымшалардың сұранысқа кең көлемде ие екендігін білдіреді [2].

1.2 Мобильді қосымшалардың артықшылықтары мен кемшіліктері

Мобильді қосымшалардың басты кемшілігі мобильді құрылғылардың пайдаланушылары интернет сайттардың өзгерістерін толық көлемде бағалау мүмкіндігін жоғалтады деп санауға болады. Барлық жаһандық өзгерістер мен модификациялар әдетте Сайттың толық түріне қатысты болғандықтан, ұялы платформада түбегейлі бірденені іске асыру өте қиын, сонымен қатар осы прогреске мобильді құрылғыларға арналған интернет қосылымдарының әлі де жоғары жылдамдығы жеткіліксіздігі кедергі келтіреді.

Осылайша, аудиториямен байланыс арнасы ретінде мобильді қосымшалардың негізгі артықшылықтарына келесі факторлар жатады:

- клиент өзіне қажетті ақпаратты өзі табады;
- клиенттің назар аударуы және тартылуы;
- өзара әрекеттесу интерактивтілігі;
- тікелей сату принципі;
- клиентпен байланыстың икемділігі;
- халықты кеңінен қамту.

Аудиториямен байланыс арнасы ретінде мобильді қосымшалардың кемшіліктеріне келесі факторлар жатады:

- байланыс мәселелері;
- болмашы технологиялық шектеулер;
- әлсіз бақылау және қауіпсіздік жүйесі;
- инновацияларды енгізудің күрделілігі.

Қорытынды ретінде бүгінгі күні жарнама коммуникациясының арналары туралы сөз болғанда, бизнес өкілдерінің көпшілігі оның мынадай түрлеріне баса назар аударатынын атап өтуге болады: жарнамалық блоктар және жергілікті газеттердегі хабарландырулар, журналдардағы мақалалар, радиодағы жарнама, теледидардағы жарнамалық ролик, ғаламтордағы баннерлік және мәтінмәндік жарнама, бұл ретте техникалық прогрестің бір орында тұрмайтынын және қолданыстағы "дәстүрлі" арналарға үнемі жаңа арналардың қосылып отыратындығы, олардың тиімділігі алдыңғылардан кем түспейтіндігі анық

Мобильді қосымшалар тұтынушымен ұзақ мерзімді байланыс орнатуға мүмкіндік береді: орнатқаннан кейін ол әрқашан тұтынушының ұялы телефонында болады, бұл оған ритейлермен жиі өзара іс-қимыл жасауға, ақпарат пен контентке қол жеткізуге мүмкіндік береді.

Мобильді қосымша тұтынушы туралы ақпарат жинау құралы бола алады, оның көмегімен тұтынушының белсенділігін бақылап қана қоймай,

сонымен бірге интерактивті диалогқа да кіруге болады.

1.3 Forbes Kazakhstan нұсқасы бойынша мобильді қосымшалардың жыл сайынғы ахуалы туралы ақпарат

Қазақстан республикасы ІТ-оқиғалар бойынша әлемнің назарында. Алайда соңғы экономикалық – саяси үрдістер ресейлік әзірлеушілерді (тек оларды ғана емес), неғұрлым тұрақты нарықтарда коммерциялық перспективаларды іздеуде басқа елдердің нарықтарына мұқият қарауға мәжбүр етеді.

Және Қазақстан осы мақсатта көптеген макроэкономикалық көрсеткіштер бойынша экс-КСРО-да үшінші мемлекет бола отырып, тек Ресей мен Украинаға ғана жол бере отырып, бірақ белсенді дамып келе жатқан (ал көптеген параметрлер бойынша көршілерден оза отырып) және сыртқы шектеу мән-жайларынан бос мемлекет бола отырып, өте үлкен қызығушылық тудырады. Қазақстан Кеден Одағы елдері арасында ЖІӨ-нің ең жоғары өсуін көрсетіп отыр, жылына 5% қарқыны негізгі капиталға инвестициялардың жоғары өсуімен де корреляциялауда. Мұнай бағасы үшін ең жоғары жылдары республика экономикасының өсуі жылына шамамен 10% - ды құрады!

ЖІӨ көлемі бойынша ел әлемде 46-орында тұр, алайда елдегі экономиканың қазіргі ресурстық моделі энергия тасымалдағыштарға әлемдік бағалардың конъюнктурасына өте байланысты екенін атап өткен жөн, осыған байланысты соңғы жылдары Қазақстан экономикасының өсуі әлемдік үрдістермен бірге баяулады.

Республика ұялы байланыстың енуінің жақсы көрсеткіштерімен мақтана алады: жиынтық абоненттік база 24,7 млн. адамды құрайды, бұл халықтың 150% - ын құрайды.

Бірнеше оператор республиканың ұялы байланыс нарығын өзара бөліседі, 2013 жылға сәйкес бөлу: Kcell – 48,7%, Beeline – 36,2%, Tele2 – 11,2%, Алтел – 3,7%.

Ұзақ уақыт нарықта тізімдегі алғашқы екі оператор басым болды, содан кейін TELE2 нарық үлесін өзгертті және жаңа ойыншының агрессивті экспансиясы одан әрі жалғасуда.

Қазақстандағы смартфон иелерінің нақты саны белгісіз, себебі операторлар да, вендорлар да, ритейлерлер де мұндай статистиканы ұсынбайды, нәтижесінде Мобильді қосымшаларды әзірлеуші компаниялардың бірі елдегі смартфондар санын есепке алуға мүмкіндік беретін жеке статистикалық жүйені құрды [3].

Олардың нәтижесі тек 355 000 дананы құрады, неғұрлым оптимистік және ықтимал болжамдар iKS-Consulting консалтингтік компаниясы – 4,5 млн. дана.

Алайда, "Технодом" жергілікті бөлшек сауда желісі 2013 жылы смартфондар сатылымының 80% - ға артқаны туралы хабарлайды, бұл аудиторияның жылдам өсуінің жақсы перспективаларын болжауға мүмкіндік береді. Қазақстандықтардың басымдылығы айқын:

- Android-87%;

- IOS-7%;

- Symbian-4%;

- Windows Phone-2%.

Әлеуетті әзірлеушілер үшін жүйені таңдау мәселесі күрделі емес.

Қазақстанда мобильді интернеттің жылдамдығы өте жоғары, 4,6 Mbps, бұл мүмкін және оның елдегі қол жетімділігі мен танымалдылығын анықтайды.

Елімізде 11,5 миллионға жуық адам мобильді қосылысты пайдаланады, оның енуі бойынша республика ТМД елдері арасында көш бастап келеді.

Сонымен қатар, кейбір деректер бойынша, қазақстандық мобильді интернет және Орталық Азия аймағы мен ТМД-дағы ең арзан интернет.

Бүгінгі таңда Қазақстанның кең 3G желісі бар, оның орнына ірі қалаларда 4G технологиясы келді және операторлар клиенттен белсенді бәсекелесе алады, өйткені абоненттік базаның өсу шегі таусылып қалды және ілгерілеу тек жаңа мобильді технологиялар есебінен ғана мүмкін болады.

Бірақ мобильді коммерцияның соншалықты қарқын алуы әзірге байқалмайды. Сонда да болса танымал мобильді қосымшаларды халық тұрмыста қолдана бастады.

Мобильді қосымшаларды дамыту-ақпараттық технологиялардың әлемдік нарығын дамытудың негізгі трендтерінің бірі. 2014 жылдың басында IDC халықаралық агенттігінің зерттеулеріне сәйкес мобильді технологияларды 1 миллиард 300 миллионнан астам маман пайдаланады. Қазақстан да сырт қалмайды. Республикада бұл таяуда ғана пайда болады және тар бағыттағы сипатқа ие. Қызметтің негізгі тұтынушылары – қаржы институттары, сақтандыру ұйымдары, автоәуесқойлар және БАҚ интернет. Мамандардың айтуынша, бүгінгі таңда пайдаланушылар электрондық төлемдер мен мобильді банкинг жөнінде ыңғайлы шешімдерді қажет етеді. Осы сұранысты қанағаттандыра отырып, қазақстандық мобильді қосымшалар нарығы салмақты едәуір арттыра алады.

Мобильді қосымшалар нарығы стандартты интернеттен әлдеқайда көп. Бұл не? Өйткені бәріне түсінікті – әрбір адам 24 сағат бойы ұялы телефонмен өткізеді. Мобильді қолданбаларды жасауға болады. Ірі ұйымдар үшін бюджет қарастырылуда. Бизнес үдерістерді автоматтандыру, ұйымдастыруда ішкі құрылымдардағы мәселе, және бұл оңай іс емес.

Gartner агенттігінің зерттеулеріне сәйкес, мобильді шешімдердің өсуі бұлтты есептеулерден кейін IT-тағы екінші орынды алып тұр. Сарапшылардың пайымдауынша 2015 жылдың соңына қарай мобильдік қосымшалар индустриясы 35 млрд. болмақ. Бүгін Қазақстанда мобильді қосымшаларды әзірлеумен 10 компания айналысады. Өндіріс құны шамамен 20 мың долларды құрайды [4].

Сонымен қатар, Қазақстандық интернет – бизнес және мобильді коммерция қауымдастығы (АКИБ) мен Intervale Kazakhstan компаниясының күшімен іске асырылған Қазақстанның мобильдік қосымшаларының алғашқы

жоба-рейтингісінің қорытындысы белгілі болды.

Осы мақсаттар үшін отандық нарыққа арналған мобильдік қосымшалардың әзірлеушілері мен иелерінен өтінімдер қабылдау жүзеге асырылды. Нәтижесінде зерттеуге коммерциялық және әлеуметтік бағыттағы 100-ден астам өнімдер қатысты, олардың ішінен топ-30 құрылды.

Рейтингте бірінші орынды Қазақстандағы ірі "Колеса"автомобиль сайтының мобильді қосымшасы иеленеді. Жеңімпаз айына 4 206 977 сессиялардың (бағдарламаға жүгінулердің) арқасында бәсекелестерден лайықты үзілді-кесілді қамтамасыз етті. Бұл көрсеткіш иеленушіге 50 балл алып, максимумға қабылданды. Ал қалған көрсеткіштер оған жалпы баға 79,3 баллға қол жеткізуге мүмкіндік берді.

Екінші орында Қазақстандағы OLX хабарландырулар сайтының мобильді қосымшасы орналасты. Естеріңізге сала кетейік, жыл басында аталған компания Slando жобасын өзіне қосты. Осылайша, американдық OLX ресурсы 100-ден астам елде таратылып, тегін хабарландыру сайттарының ең ірі отбасына айналды. Айына 3 270 175 сессияға тең орташа пайдалану көрсеткішіне ие бола отырып, қосымша басқа бағалармен 69,17 баллды ала алды. Сонымен қатар, күміс жүлдегер рейтинг жеңімпазын кезең ішіндегі сессиялар санының өсуі, сондай-ақ техникалық қолдаудың болуы сияқты параметрлер бойынша басып озды.

Бірінші үштікті ақпараттық порталдың мобильдік қосымшасы түйіндейді Tengrinews.kz ескерту. Жобаның web-нұсқасы Ұлттық интернет-сыйлықтың алғашқы орындарды иеленді AWARD.kz соңғы үш жыл бойы "массмедиа" категориясында. Қосымшаның өзіне келетін болсақ, ол рейтинг көшбасшыларының арасында сессиялар санының жоғары өсуімен ерекшеленді – 28%. Қорытынды баға-51,04 балл.

Айта кету керек, аталмыш рейтингтің жүлдегерлері жетістікке веб-ресурстардың арқасында қол жеткізіп отыр.

Мобильді қосымшалар нарығының толып кетуі. Мобильді қосымшаларды әзірлеушілердің шамамен алғандағы саны – 2.3 миллион адам, бұл әлемдегі барлық әзірлеушілердің әрбір сегізіншісі ұялы қосымшаларды жасайды деген сөз. 2013 жылы Apple компаниясы WorldWide Developer Conference кезінде AppStore-да 1.25 миллион қосымшалар жариялады, оларды пайдаланушылар 50 миллиард рет жүктеді, ал әзірлеушілер 5 миллиард доллар табыс алды. Әзірлеушінің орташа табысы төмендегі 1 – кестеде көрсетілген.

Кесте 1 – әзірлеушінің орташа табысы

Көрсеткіш/компания	Google	Apple	Microsoft
Қолданушылар саны (млн. адам.)	900	600	12
Қосымшалар саны (мың дана)	800	1250	160
Әзірлеушілер саны (мың адам)	150	235	45

1-кестенің жалғасы

Қосымшаны жүктеу саны (млрд. рет)	48	50	65
Әзірлеушілер табысы (млн. дол.)	900	5000	100
Қосымшаның орташа табысы	\$1125	\$4000	\$625
Әзірлеушінің орташа табысы	\$6.000	\$21.276	\$2.222

2019 жылға дейін мобильді қосымшалар секірісі жылына 212 миллиардқа дейін жетеді деген ой бар, ал одан түсетін табыс 72,5 млрд.долларды құрамақшы. Олай болса, мобильді қосымша әзірлеу мәселесі әлі де өзекті болып қала береді.

1.4 Мобильді қосымша нарығындағы бәсекелестік

Қазақстандық әзірлеушілерді тек ақша табу мүмкіндігі ғана қызықтырып қоймайды. Бұл туралы "АБАІ 45" (Сурет 1) мобильдік қосымшасы бойынша айтуға болады. Жоба авторлары – "ЛУЧ" тәуелсіз шығармашылық бірлестігі, Айсұлу Әзімбаева, Индира Сүлейменова және Шыңғыс Капин Қазақстанның жас кинематографистері мен актерлерінің қатысуымен Абай Құнанбаевтың "сөз кітабы" бірегей аудио – нұсқасын жасауға қатысты. Ең алдымен, қолданба Ұлы Абай Құнанбаевтың "Қара сөздерінің" аудиOVERсиясы болып табылады. Жоба қаржылық салымсыз және демеушілік көмексіз жүзеге асырылды [5].



Сурет 1 – "АБАІ 45" мобильдік қосымшасы

Тарихқа тағы бір ерекше құрмет – Kcell ұялы операторынан "Ұлы Жібек жолы" (Сурет 2) мобильдік қосымшасы осы жылдың ақпан айында пайда болды. Қосымшаға Қазақстан мен Орта Азияның мәдени-тарихи көрікті жерлері бойынша нағыз жолсерік болуға арналған (Кесте 2). Жобаның әзірлеушісі MobileAccessStudio компаниясы болды, ал тарихи деректерді, карталарды, дәйексөздерді, ескерткіштер мен фотосуреттерді қоса алғанда, ақпараттық материалдарды академик Карл Байпақов бастаған археологтар ұсынды. Пайдаланушылар Қазақстан, Қытай, Қырғызстан және бірнеше

еуропалық қалалар аумағында 45 тарихи ғимаратты барынша тереңірек игере алады. «Ұлы Жібек жолын» Play Market немесе App Store арқылы тегін көшіріп алуға болады. Қосымшаның интерфейсі өте қызықты, көңілді және барынша ыңғайлы.



Сурет 2 – Жібек жолы қосымшасы

Кесте 2 – Қазақстандағы кең қолданысқа ие веб-қосымшалар

№	Әзірлеме	әзірлеуші	Орнату саны	бағасы	Қолдану ортасы
1	Yvision — блог-платформа қосымшасы	BeeMobile	15 000	тегін	iPhone, және iPad
2	Такси шақыру (Қазақстанның 14 қаласына таралған)	Аскар Каримов/Нурлан Кани	25 000	тегін	iPhone
3	Tengrinews — iOS-ақпараттық портал қосымшасы (Android, iOS)	Smart Park	26 000-нан жоғары	тегін	iPhone/iPad.
4	Pit-stop.kz — Қазақстандағы жол қозғалысы ережесі	Crystal Spring	30 000-дай	тегін	iPhone/iPad
5	Kiwi — видео-сервис	Алмас Адильбек	30 000-нан астам	тегін	iPhone/iPad
6	iSozdk — қазақша-орысша, орысша-қазақша онлайн сөздігі	Асет Тусунбаев	34 000-нан астам	тегін	iPhone
7	Homebank.kz — интернет-банкінг мобильді қосымшасы	BeeMobile, Казкоммерцбанк үшін	33 000-ға жуық	тегін	iPhone/iPad
8	100 қазақ әнін	kaznetmedia	35 000-нан көп	тегін	iPhone/iPad
9	Kolesa.kz — ірі автомобиль порталының ресми қосымшасы	ТОО «Колеса».	100 000-нан астам	тегін	iPhone/iPad
10	Бонус: Kino.kz — Қазақстан кинохабарландыруы	BeeMobile, Казкоммерцбанк үшін	62 000-ға жуық.	тегін	iPhone

Қазақстандағы мобильді қосымшалар нарығы осындай көрсеткіштерге ие. Көп салада, әсіресе онлайн білім беру саласында мобильді қосымша көмегімен онлайн білім беру саласы ақсап жатыр. Алдағы уақытта осы қарқыннан таймаса, ол салада да онлайн оқу үдерісі кең қолданысқа енеді деп сенеміз.

Компьютерлік ойындар. Қазіргі уақытта компьютерлік технологиялар біздің өміріміздің әр түрлі салаларында белсенді қолданыла бастады. Әртүрлі білім салалары үшін әртүрлі қарапайым және күрделі компьютерлік бағдарламалар жасау үнемі даму үстінде. Баланың жасына байланысты компьютерлік бағдарлама ойын бойынша оппонент ретінде сөйлей алады, әңгімеші, репетитор, емтихан алушы болуы мүмкін. Мектепке дейінгі ересек және кіші мектеп жасындағы балаларға сәтті пайдаланылуы мүмкін визуалды және есту қабылдауы, назар, есте сақтау, сөздік және логикалық пайымдаулар және т. б. сияқты балалардың түрлі психикалық функцияларын дамытуға бағытталған компьютерлік бағдарламалар бар.

Ойын – бұл танымдық іс-әрекет, ол қоршаған баланың табиғаты туралы ойлаудың практикалық түрі болып табылады. Ойын ерекшелігіне байланысты, бала ойында алғаш рет абстрактілі ойлауға қатысады. Компьютерлік ойындар дамытушы оқытудың жаңа түрі. Компьютерлік технологиялар педагогикалық әдістерді қолдану үшін жаңа мүмкіндіктер ашады [6].

1.5 Ұялы телефон иелері нені пайдаланады

Мобильді қосымшалардың көптеп әзірленіп, таралуы оны орнататын құрылғыларға, сол құрылғылардың кең қолданысқа ие болуына байланысты.

Осыған байланыс ақпарат көздерінде (Сурет 3) мынадай мәліметтер келтірілген:

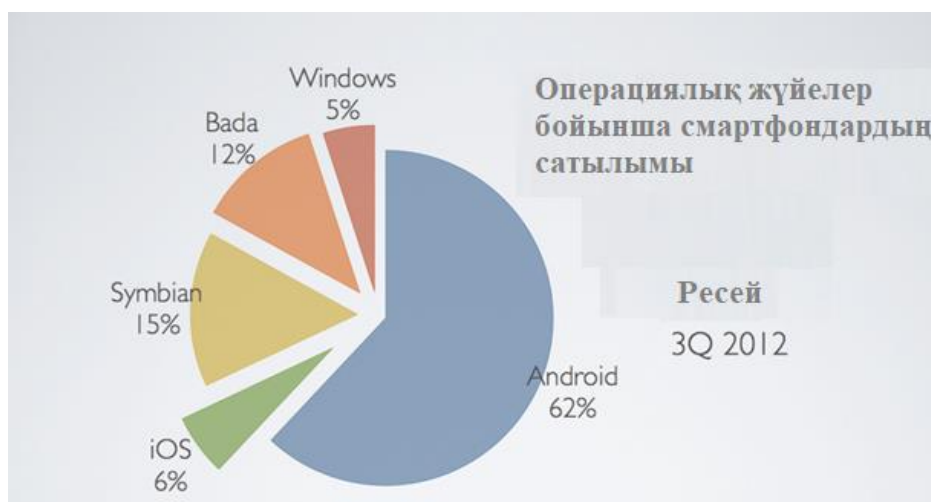
- жартысынан көбі жүктелген қолданбаларды пайдаланады - 53%;
- ұялы телефон арқылы шамамен сайттарға кіреді - 52%;
- адамдардың үштен бірінен астамы өз ұялы телефонынан әлеуметтік желілерді пайдаланады - 38%;
- аздаған адамдар ойын ойнайды - 34%;
- пайдаланушылардың төрттен үш бөлігі ұялы телефондар (қоңыраулардан басқа) арқылы сөйлеседі: бұл SMS, әлеуметтік желі қосымшасы, мессенджер болуы мүмкін.

Статистика бойынша смартфондарды қолдану көрсеткіштеріне талдау



Сурет 3 – Смартфондарды пайдалану көрсеткіші

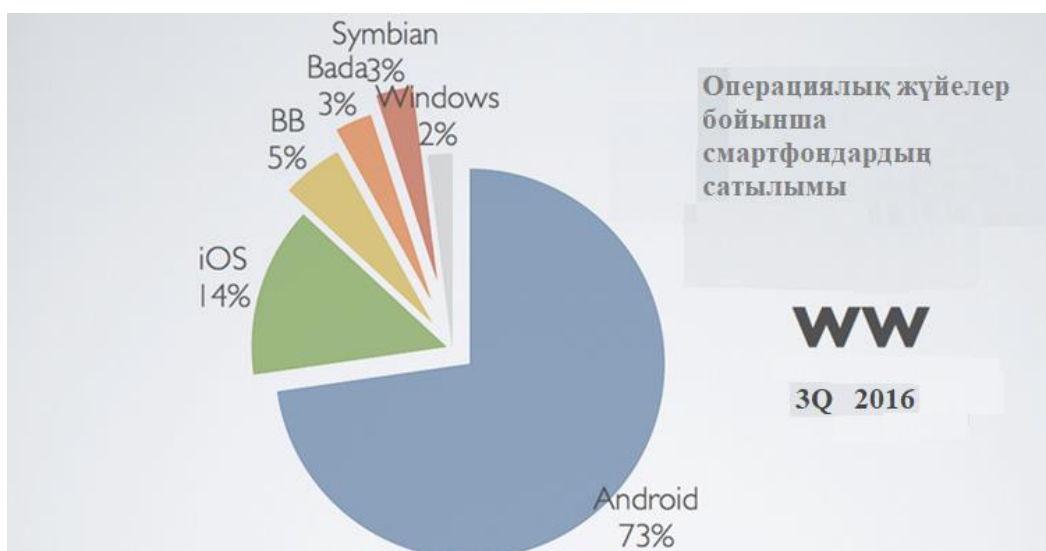
2016 жылы РФ-да шамамен 12,6 миллион смартфон сатылды: Ресей осы тұрғыдан тез дамып келе жатқан елдердің бірі болып саналады (Сурет 4).



Сурет 4 – ОЖ бойынша смартфондардың сатылу көрсеткіші

Егер біз операциялық жүйелер бойынша смартфондарды сату статистикасын қарайтын болсақ, (Сурет 5) келесілерді көресіз:

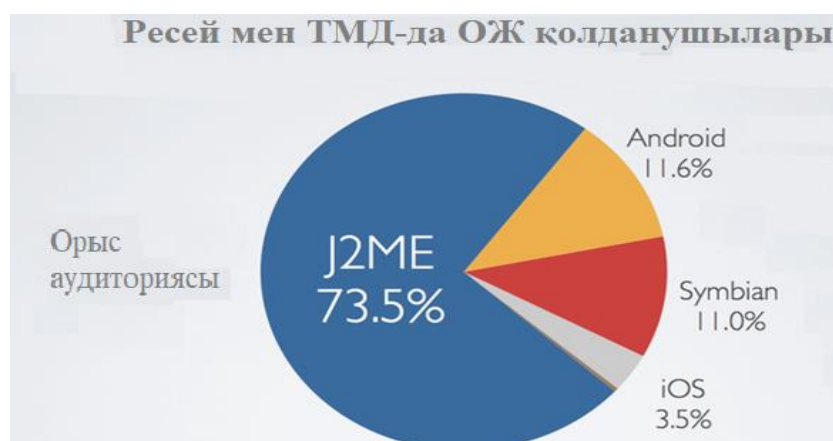
- сатылған смартфондардың 62%-ы – Android-құрылғылар;
- нарықтағы екінші орында Symbian – 15% ;
- смартфондардың қалған үлесін bada, iOS және Windows Phone (егер тек Мәскеу қаласы бойынша алатын болсақ, Apple өнімдеріне сұраныс көп).



Сурет 5 – Смартфондардың әлем бойынша сатылым көрсеткіші

Егер бүкіл әлем бойынша осындай кестеге қарайтын болсақ, онда бұл жерде нарықта алдыңғы қатарда $\frac{3}{4}$ көрсеткішті Android иемденіп отыр. 2016 жылдың екінші тоқсанында бүкіл әлем бойынша 104 миллион Android телефоны сатылды. Бірақ бізді мобильді әзірлеушілер ретінде смартфонның болуын ғана емес, онымен қалай жұмыс істейтінін де қызықтырады. Android құрылғысының иегерлерінің айтарлықтай үлесі оларды әдеттегі телефон: SMS, қоңыраулар — барлығы сияқты пайдаланады. Олар Google Play-де құрылғыны іске қоспайды, қолданбаларды жүктеп алмайды [7].

2016 жылы барлық адамдар телефонмен байланысқан жоқ, сондықтан мобильді операциялық жүйелер арасында күш бөлу біздің ішкі статистикамыз көрсетіп отыр. Бұл статистикаға Ресей және ТМД елдері кіреді: Украина, Белоруссия, Қазақстан, Өзбекстан (Сурет 7).



Сурет 6 –Ресей мен ТМД көлеміндегі ОЖ қолданушылары

- 73,5% – бұл Java-телефондар (Сурет 6);
- Android құрылғылары 11,6%-дан екінші орында;
- Nokia компаниясының мұрасы, Symbian, 11% Android мүлдем сәл артта;
- алма өнімінде Рунет қолданушыларының 3,5% - ы бар;

- Microsoft Windows Phone диаграммасында (1%-ден кем) .

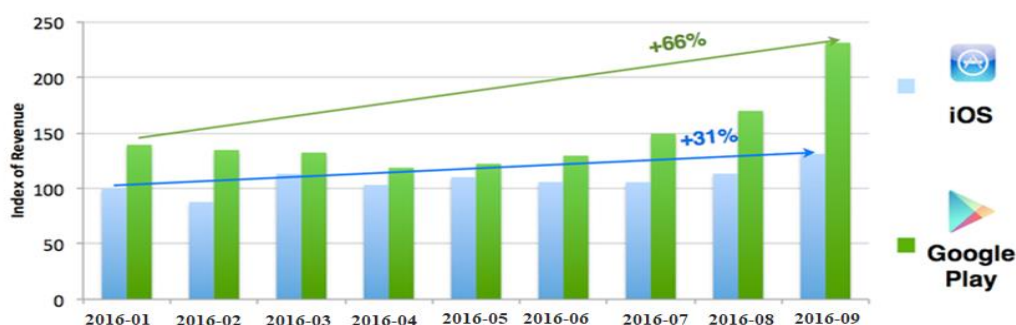


Сурет 7 –Рунеттегі мобильді платформалар көрсеткіші

Қосымшаларды орнату

Қолданба әзірленетін платформаны таңдау кезінде қолданыстағы қосымшалар бойынша статистиканы білу маңызды. 2016 жылдың қыркүйек айында App Annie компаниясының зерттеуі бойынша Apple және Google дүкендерінің көрсеткіштері (Сурет 8):

Russia: Growth of Downloads



Сурет 8 – App Annie компаниясының зерттеуі бойынша Apple және Google дүкендерінің көрсеткіштері.

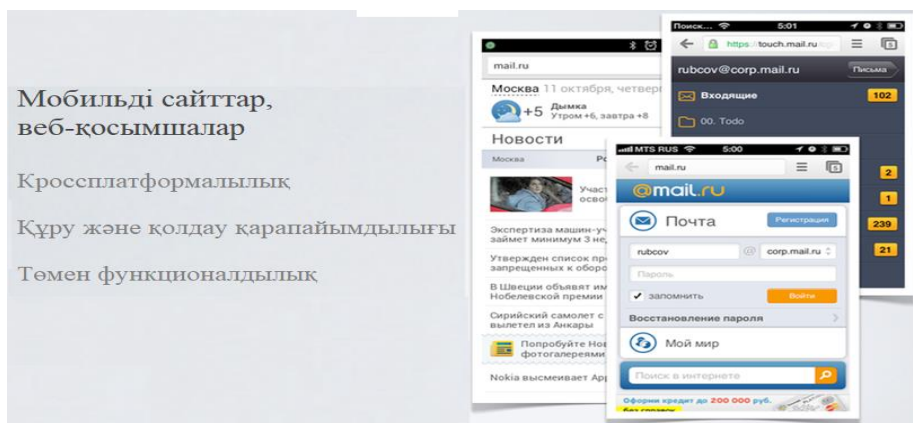
Қотарып алу бойынша бірінші орында Google Play: +66%-ды құрап отыр, екінші орында iOS – 30.

1.6 Мобильді қосымшалар жасау кезеңдері. Оның ұйымдастырушылық, экономикалық, маркетингтік аспектілері. Мобильді қосымшалар жасау құралдары мен әдістері

1.6.1 Мобильді қосымшалардың түрлері

Іс жүзінде мобильді құрылғыларға арналған қолданбаларды үш түрге бөлуге болады.

1) Мобильді сайттар, веб-қосымшалар



Мобильді сайттар,
веб-қосымшалар

Кроссплатформалылық

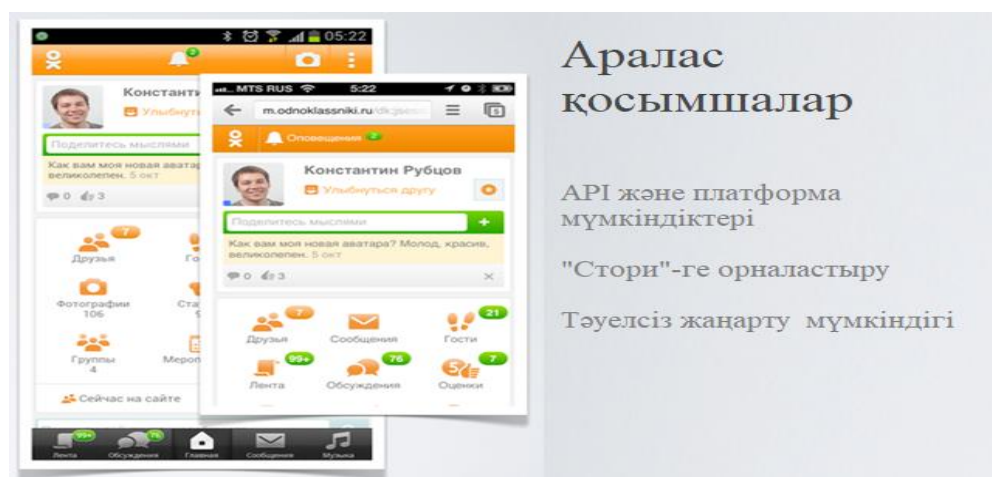
Құру және қолдау қарапайымдылығы

Төмен функционалдылық

Сурет 9 –Мобильді қосымшалар

Бұл ұялы құрылғыларға арналған қосымшалардың ең көп таралған түрі. Заманауи смартфондар әдеттегі сайтты көрсете алады (Сурет 9). HTML5 мүмкіндігі десктоп жасауға үлкен мүмкіндік береді. Веб-қосымшалар стартап үшін өте қолайлы: аз ақша шығарып, аз мерзімде үлкен нәтиже алуға болады. Басқа мобильді қосымшалармен салыстырғанда Мобильді сайттың тағы бір плюс жағы - бұл кроссплатформалығы, яғни программалық қамтаманың бірнеше операциялық жүйелермен жұмыс істей алу мүмкіндігі.

2) Гибридті қосымшалар



Аралас
қосымшалар

API және платформа
мүмкіндіктері

"Стори"-ге орналастыру

Тәуелсіз жаңарту мүмкіндігі

Сурет 10 – Аралас қосымшалар

Мұндай тәсілде сіз операциялық жүйенің API артықшылықтарының барлығына қол жеткізе аласыз (Сурет 10): қолданба push-хабарламалармен толықтырылған, өнімді сторларда орналастыруға болады. Сонымен қатар көптеген компоненттері серверде орналасқан платформаға тәуелсіз жұмыс істеуі де мүмкін. Гибридті қосымшалар – бизнес бастағысы келетін немесе өз идеясын тексергісі келетіндер үшін, инвесторға, достарына көрсету үшін тамаша шешім.

3) Нативті қосымшалар



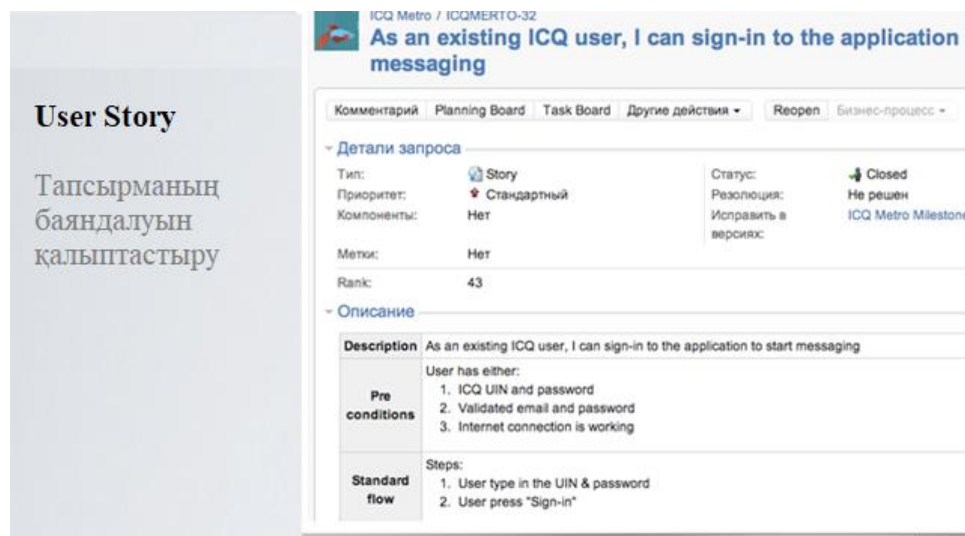
Сурет 11 – Нативті қосымшалар

Қосымшалардың бұл түрі ең көп ресурсты (Сурет 11), бірақ онымен бірге әрбір нақты операциялық жүйе ұсынатын мүмкіндіктерді барынша пайдалануға мүмкіндік береді. Нәтижесінде, нативті қосымшалар функционалдығы бойынша да, мобильді қосымшалардың басқа үлгілерінде жұмыс жылдамдығы бойынша да ұтады [8]. Дәл осындай тәсілді қазір аралас қосымшалар жасаған компаниялар қолдануда. Мысалы, Facebook аралас қолданбадан бастады: нативті бақылаулар және мазмұн ретінде веб-бет. Бұл жақсы шешім болғанына қарамастан, өнімділікке қатысты бірқатар мәселелер де жоқ емес, соған байланысты әзірлеушелір бұл әдісті көбніе қолдана бермейді.

1.6.2 Мобильді қосымша құру процесі

Мобильді қосымша құру процесі әзірлеушінің мақсаты мен ойлам мүмкіндігіне байланысты. Ол мынадай процестерден тұрады:

1) User Story



Сурет 12 – Трекердегі нақты тикетті көру

Ең алдымен, біз кімнің жазатынын анықтауымыз керек. Бұл сұрақтарға жауаптар User Story-да ресімделеді (Сурет 12). Суретте трекерде нақты тикетті

көре аласыз. Ол қолданыстағы ICQ пайдаланушысы бағдарламаға кіретінін және ол қандай мәселелерді кездестіретінін сипаттайды. Бұл кезеңде әзірлеудің кеш кезеңдерінде жағымсыз тосын сый болмас үшін барлық ықтимал сценарийлерді пысықтау маңызды.

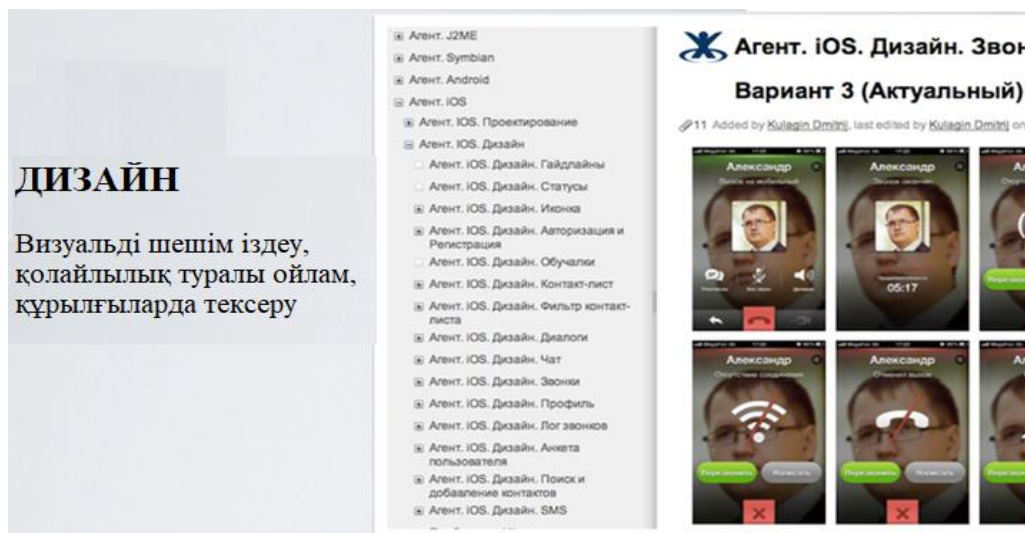
Сіздің to-do парағындағы әрбір тармақтың артында үлкен айсберг функционал жасырылады. Тапсырмаларды фрагменттеуге және нақтылауға тырысу керек.

2) Жобалау және дизайн

User Story құрастырғаннан кейін жобалау (Сурет 13) және дизайн (Сурет 14) жасау басталады.



Сурет 13 – Жобалау кезеңі



Сурет 14 – Дизайнын таңдау

Осы кезеңде тақтаға ілінген прототиптерді пайдаланып, бағыттарды айқындау навигациясын көрсету қажет [9].

Дизайнды жасау кезінде міндетті түрде гайдлайн қолданылады.

Гайдлайндар (Guidelines) – платформа, операциялық жүйелер құрушылардың кеңестерін, нұсқауларын, ережелері мен принциптерін

қамтитын жиын, осының арқасында осы платформада немесе операциялық жүйеде жұмыс істейтін қосымшалар біркелкі жұмыс істейді. Мобильді қосымшалардың гайдлайндары навигация және өзара әрекеттесу принциптерін, интерфейс элементтерін және олардың стилін, қолданылатын типография мен иконографияны, түсті палитрларды және т.б. сипаттайды.

Сонымен қатар, гайдлайндар мобильді қосымшаны әзірлеу уақыты мен құнын қысқартуға қабілетті, себебі гайдтарда сипатталғанның бәрі, әдетте, кодта дайын элемент түрінде іске асырылған және әзірлеушіге велосипедті нөлден ойлап табудың қажеті жоқ.

Екі түрлі платформадағы гайдты қарастырып өтелік:

- 1) Apple Human Interface Guidelines для iOS
- 2) Google Material Design System для Android

Google Material Design System. Google Material Design 2014 жылдың маусым айында Android 5.0 бірге ұсынылды, ал осы жылдың мамыр айынан бастап толық дизайн-жүйеге айналды және басқа платформаларда (мысалы, смарт-тв, десктоп немесе тіпті веб-қосымша, IOS-құрылғы) пайдаланылуы мүмкін. Бастапқыда тек Google: Android Wear, Android TV, Android Auto ОЖ-леріне бағытталған болатын.

Material Design негізгі идеялары – интерфейстің тереңдік принципі, оның интерактивтілігі (қайырымдылығы) және қозғалысы (күй өзгерісінің анимациясы).

Мұнда әр навигация элементі басқа элементке қатысты белгілі бір биіктікте болады және пайдаланушының әрекетіне жауап береді. Мысалы, бүйірлік мәзір навигация тақтасының үстінде, ал тізімдегі кәртішке астында орналасқан. Батырма оған басқан кезде төмен түсіріледі, түсетін көлеңкені өзгертеді және сия әсерімен түсі өзгереді.

Material Design бүкіл жүйе үшін үлгі ретінде оған қағаз және сия пайдаланады. Material канондары бойынша жасалған кез келген интерфейс бір-біріне жалатылған және көлеңке түсіретін жеке қағаз парағы түрінде ұсынуға болады.

Material Design System-де барлық мүмкіндік қамтылған.

Мұнда барлық жүйелік иконкалар, UI-киттер, қаріптер, түс бояғыштары, тіпті Sketch үшін кастом UI генерациясы үшін плагин бар. Және мұның бәрін мұнда жүктеп алуға болады. Мұнда сіз интерфейстің ең аз элементі үшін барлық өлшемдерді таба аласыз. Сіз қалай жасай аласыз, қалай жасай алмайсыз.

Apple Human Interface Guidelines. Apple Human Interface Guidelines жүйесі iOS 7-мен бірге ұсынылды (7 маусым 2013) және содан бері Apple (Watch, macOS, tvOS) басқа ОЖ пайдалану үшін кеңейтілді.

Human Interface Guidelines-тің негізгі идеясы интерфейстің қарапайымдылығы мен жеңілдігінде. Басты бұрышта контент тұрғызылады, ал интерфейс екінші жоспарға кетеді. Интерактивтілік (жауап) және интерфейс элементтерінің күйін өзгерту анимациясы қамтылған. Төменгі деңгейде

терезелерді жуу, градиентті құю, швейцариялық стильдің үздік дәстүрлеріндегі болдықты типографика қолдау табады.

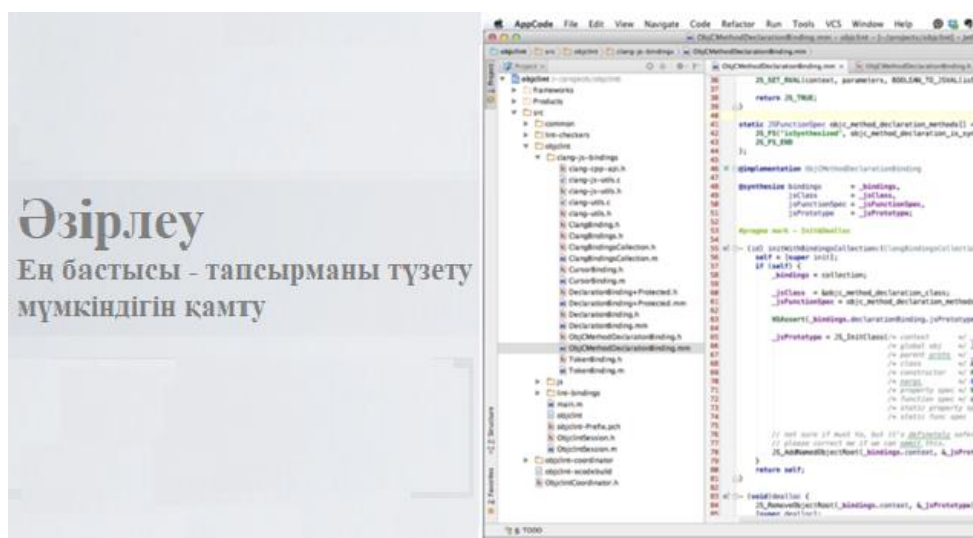
Human Interface Guidelines-те Material Design System-ге қарағанда нақты ережелер мен нақты ерекшеліктер жоқ. Мысалы, Apple гайдтарында түймелер өлшемін көре алмайсыз. Кейбір интерфейс элементтері тек қана гайдте жоқ, бірақ Apple ресми қосымшаларында қолданылады. Мұнда Google қарағанда, Apple дизайнерге "қаріптермен ойнауға" рұқсат етеді және платформа шеңберінде кастомизация үшін көбірек еркіндік береді.

Жүктеу бөлімінде барлық танымал құралдар мен қаріптер үшін UI-киттер бар. Қандай да бір себептерге байланысты Apple жүйелік белгішелерді көшіріп алуға мүмкіндік бермейді.

Гайдты қолдану не үшін керек деген сұраққа жауап беретін болсақ, оны мынадай төрт себеппен байланыстыруға болады:

- 1) Дизайн процесін жеделдетеді;
- 2) Әзірлеу процесін жеделдетеді;
- 3) Әзірлеу арзанға түседі;
- 4) Қолданушы жылдам да түсінікті интерфейске ие болады

1.6.3 Әзірлеме дайындау. Сипаттамасын талқылау және қажетті түзетулер енгізу



Сурет 15 – Қосымшаның әзірлемесін дайындау

Макеттерді, гайдлайн мен кесіндіні алғаннан кейін әзірлеушінің жұмысы басталады (Сурет 15). Біз ойлап тапқан нәрсенің барлығын әзірлеуге жібереміз және ерте нәтижені күтеміз. Бұл сәулет және пайдаланушы интерфейсін жұмысы аяқталды дегенді білдірмейді. Кейде әзірлеушілерде бастапқы жоспарға түзетулер енгізетін қызықты идеялар пайда болады. Әзірлеу аяқталған кезде тестілеу кезеңі басталады.

Тестілеу. Ұялы өңдеуде тестілеуші – айналасында бірнеше телефондар бар адам. Үлкен шкаф болады, онда ескі телефондар да, ең жаңа өнімдер де бар. Тест-кейстер бойынша тестілеуге тырыу керек. Егер жаңа фич енгізілсе, оның сипаттамасы бойынша тест-жоспар жасалады.

Тестілеуге көмектесетін қызметтер бар. Жалпы көп жағдайда бета – тестерлерге өнімді таратуға мүмкіндік беретін HockeyApp қолданбасы пайдаланылады. Әдетте әлеуметтік желілерде жазылады: "балалар, бізде жаңа қосымша бар. Келіп көріңіз!". Ниет білдірушілер билд алады, қосымшаны пайдаланады, ал сервис статистиканы жинайды, креш-репорт жасайды және осының барлығын тестілеушіге жібереді [10].

Сондай-ақ, түрлі операциялық жүйелерде қосымшаны тексеруге мүмкіндік беретін өз сервистерері болады. Қолданушы қосымшаны бере алады, сервис қолданушы қойған барлық жолды скриншоттап, суреттерді тестілеушіге жібереді, және ол барлық дұрыстықты тексере алады.

Мониторинг. Сонымен, сіз бағдарламаны әзірледіңіз, сынақтан өткіздіңіз, оны сторға құйыңыз. Жүктеу статистикасын бақылау үшін Distimo қызметін пайдалануға болады. Ол қолданбаларды жүктеу үшін стор келіп түсен пайдаланушылар бойынша статистиканы көрсетеді, және түсініктеме қалыптастырады.

Қызықты мониторинг қызметінің бірі – Flurry. Ол клиенттік статистиканы жинауға көмектеседі. Flurry пайдаланушы қолданбасында не істеп жатқаны туралы есеп береді: ол батырмаға қанша рет басылды, қосымшаға қанша рет қайтып келді және одан да көп мәліметтерді тестілейді. Жалпы параметрлер — аудитория, география, жынысы, жасы және т. б.

Кейбір мобильді өнімдерде сондай-ақ Google Analytics арқылы клиенттік статистиканы есептеуді пайдалануға болады. Flurry-мен салыстырғанда ешқандай айырмашылық жоқ. Жұмыс жылдамдығы мен логтарды өңдеу кемшіліктері екі жағдайда да бар, алайда, егер сіз Google интерфейсімен жұмыс істеуге үйренген болсаңыз, бұл құралды пайдалана аласыз.

Үшінші тарап қызметтерінің көптігіне қарамастан, бізде жеке статистика бар. Сыртқы көздер қандай жақсы болмаса да, оларды тексеру керек. Сондықтан бізге Flurry және Distimo сияқты сервистерді пайдалану оңайырақ, ал ішкі логтарға сұрақтар туындаған кезде хабарласу оңайырақ.

1.6.4 Мобильді қосымша құру кезеңдері

Мобильді қосымшаны құрудың негізгі кезеңдерін қарастырайық.

Мобильді қосымшаны құрудың бірінші кезеңі – техникалық тапсырма құру. Техникалық тапсырма (ТТ) - жүйеге қойылатын талаптар жиынтығын ескертетін және Тапсырыс беруші/пайдаланушы, сондай-ақ орындаушы/жүйе өндірушісі бекіткен техникалық құжат (спецификация). Мұндай ерекшелік сондай-ақ жүйелік талаптар мен тестілеуге қойылатын талаптарды қамтуы мүмкін.

Мобильді қосымшаны әзірлеудің екінші кезеңі – UI/UX жобалау. User Experience Design аудармада "өзара іс-қимыл тәжірибесі" дегенді білдіреді және әр түрлі ux-компоненттерді қамтиды: ақпараттық сәулет, өзара іс-қимылды жобалау, Графикалық дизайн және мазмұн. Осы кезеңде техникалық тапсырмада сипатталған барлық жұмыстар іске асырылады. Экрандар арасында өзара іс-қимылдың графикалық картасы жасалады. Сонымен қатар, осы кезеңде қолданба қалай жұмыс істейтінін және онымен пайдаланушының

жұмысы қалай өтетінін анықтау керек.

Үшінші кезең: дизайнмен жұмыс. Дизайн клиенттің қалауы негізінде жасалады және мақсатты аудиторияға бағытталған. Бастапқыда қосымшаның барлық негізін құрайтын 1-3 беттердің дизайны жасалады. Клиенттің қалауы бойынша, Тапсырыс берушінің ең жақсы нұсқасын анықтайтын бірнеше дизайн стилі жасалуы мүмкін.

Төртінші кезең: әзірлеу. Мамандар қосымшаны интерактивті үлгіге аударады. Мұны беттеу арқылы қол жеткізуге болады. Жұмыстың аяқталған нұсқасы клиентке жұмыстың қорытындысын бағалап, өз пікірін білдіру үшін жіберіледі.

Бірнеше күн ұялы бағдарлама Белсенді тестіленеді. Егер қандай да бір қателіктер анықталса, онда қосымша пысықталады.

Тестілеу. Қосымшаларды әзірлеудің әр түрлі кезеңдерінде симуляторларда да, нақты құрылғыларда да қосымшаларды ішкі тестілеу міндетті болып табылады. Тестілеу мақсаты-қосымшаның смартфондар мен планшеттердің аппараттық және бағдарламалық платформасымен өзара іс-қимылы прототиптеу кезеңінде көзделгендей болады деп көз жеткізу [11].

Тесттер сериясы мен қосымшаларды жетілдіру нәтижесінде қосымшаның жұмыс нұсқасы алынуы тиіс. Осы нұсқаны Apple App Store, Google Play, Windows Phone қолданбалар дүкені (қандай платформа әзірлену жүргізілетініне байланысты) немесе қосымшаларды дистрибуциялау үшін кез келген ұқсас қызмет дүкеніне қосу керек.

Дүкенге қолданбаны қосу. Студия жұмысының соңғы кезеңі - жоғарыда көрсетілген қолданбалар дүкендерінің біріне ревью қолданбасын қосу (Componentix жағдайында App Store немесе Google Play туралы әңгіме болады).

GooglePlay (алдыңғы атауы-Android Market) – Android операциялық жүйесі бар құрылғылардың иелеріне түрлі қосымшаларды орнатуға және сатып алуға мүмкіндік беретін Google компаниясының қосымшалар дүкені.

GooglePlay-да көптеген пайдалы және түрлі қосымшаларды табуға болады. Дүкенде ақылы және тегін бағдарламалар бар.

2015 жылдың 31 қазанында Google компаниясы қосымшалар саны 700 000-ға жетті және жүктеу саны 25 миллиардқа жетті. Дегенмен, сонымен бірге пайдаланушылар сапасы төмен бағдарламалар дүкенде жиі кездеседі деп шағымданады. Осыған сәйкес сапалы бағдарламалық өнімді әзірлеудің маңыздылығы зор. Әзірлеудің негізгі сәті ұқсас немесе тақырыбы бойынша ұқсас бағдарламалық өнімдерді, соның ішінде салыстырмалы өнімдерді іздеу және талдау болып табылады. Мұнда негізгі міндет - қолданушының көзқарасы бойынша қолданыстағы қосымшалардың артықшылықтары мен кемшіліктері қандай екенін анықтау.

1.6.5 Программалық қамтама әзірлеудің өмірлік циклі

Мобильді қосымшаларды әзірлеудің өмірлік циклі Веб және үстелдік қосымшалар үшін SDLC-тен ешқандай айырмашылығы жоқ. Олармен қалай болғанда да, процестің 5 негізгі фазасы бар:

1) Бастапқы кезең – барлық қосымшалар идеядан басталады. Бұл идея әдетте қолданба үшін берік негізге өңделеді.

2) Сонымен қатар, бұл бағдарлама жұмыс істейді және т.б. сияқты жалпы орналасуын анықтау, сондай-ақ бұл UX-ті графикалық дизайнердің көмегімен пайдаланушы интерфейсінің (UI) қолайлы дизайнына айналдыру.

3) Өңдеу – Бұл бағдарламаны нақты жасау.

4) Тәжірибелі эксплуатация (тұрақтандыру) - сапаны бақылау, әдетте, бағдарламаны тестілеу және қателерді түзету басталады. Кейбір уақытта қолданушылар кең ауқымда оны пайдалануға, кері байланысты жүзеге асыруға және өзгерістерді хабарлауға мүмкіндік алатын шектеулі бета-фазада пайдаланылатын болады.

5) Енгізу (тарату).

Осы фазалардың көпшілігі бір-бірін жабады, мысалы, әзірлеу толық жүріспен жүргенде, пайдаланушы интерфейсі әлі аяқталмаған уақытта әзірлеудің UI бастапқы нұсқасын өзгерте алады. Сонымен қатар, Бағдарлама тәжірибелік пайдалану кезеңінде болуы мүмкін, ал әзірлеу кезеңінде бағдарламаның жаңа нұсқасында бекітілетін жаңа функциялар қосылды.

Сонымен қатар, бұл фазалар SDLC әдістемелерінің кез келген санында қолданылуы мүмкін, мысалы, икемді әзірлеу әдістемесі, спиральды модель, каскадтық модель және т. б.

1.7 Мобильді қосымшалар жасау құралдары мен әдістері

Барлық мобильді операциялық жүйелер үшін мобильді қосымшалар жасау тілдері бар: iOS үшін ObjectiveC (қазір, әрине, Swift), Android үшін Java, Windows Phone үшін C#. Ең қарапайым қосымшаны жасай отырып, осы тілдердегі әзірлемелердің ерекшеліктері туралы ғана емес, сонымен қатар барлық платформаларда бірыңғай функционалдылықты қолдау қажет. Мұндай тәсілдегі проблемалар да әртүрлі, бұл қосымшаны әзірлеу мерзімі, және болашақта бағдарламаны қолдау күрделілігі, және кодты қайта пайдаланудың мүмкін еместігі. Деген мобильді қосымша әзірлеуде қолданылатын бірнешеуіне түсінік беріп кетуге болады.

1.7.1 Android Studio 3.1.3 интеграцияланған әзірлеу ортасы

Android Studio – Android платформамен жұмысқа арналған интеграцияланған әзірлеу ортасы (IDE), 2013 жылдың 16-мамырында Google I/O конференциясында ұсынылған.

IDE 2013 мамыр айында жарияланған 0.1 нұсқасынан бастап еркін таратылды, содан кейін 2014 жылдың маусым айында шығарылған 0.8 нұсқасынан бастап бета-тестілеу сатысына өтті. 1.0 бірінші тұрақты нұсқасы 2014 жылдың желтоқсанында шығарылды, сонда Eclipse үшін Android Development Tools (ADT) плагинін қолдау тоқтатылды. JetBrains компаниясының IntelliJ IDEA бағдарламалық қамтамасына негізделген Android Studio-Android қосымшаларын әзірлеудің ресми құралы. Бұл өңдеу ортасы Windows, OS X және Linux үшін қол жетімді. 17 мамыр 2017, Google I/O жыл сайынғы конференциясында, Google компаниясы Java және C++

тілдерімен қоса, Android платформасына арналған ресми бағдарламалау тілі ретінде Android Studio-да қолданылатын Kotlin тілін де анонстады [12].

Android Studio –ны орнатудағы техникалық және программалық талаптар.

Қарапайым жүктеу және жұмыс үшін осы конфигурация жеткілікті.

- 3 GB RAM – кем дегенде;

- 8 GB RAM ұсынылады+ 1 GB - Android Emulator эмуляторы үшін;

- 1280x800 пиксель - экранның минимум мүмкіндігі;

Күрделі жүйелер үшін ең басты қажетті 5 параметр бар:

- CPU өнімділігі;

- CPU аппараттық ағындарының саны;

- жедел жады саны;

- еркін оқу және Еркін жазу жылдамдығы;

- шағын блокты оқу және шағын блокты жазу жылдамдығы.

Қуатты конфигурация деректердің үлкен ағынымен жұмыс істеуге мүмкіндік береді:

1) Процессор – 4 ағынды және Core i5 HQ Skylake одан да қуаттырағы.

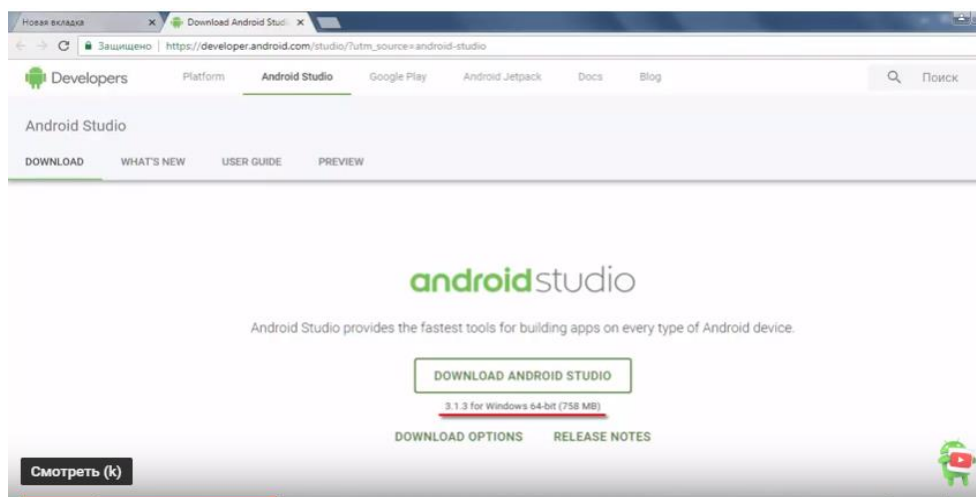
2) ЖЖ -12ГБ RAM және одан жоғары.

3) SSD- **IOPS** (неғұрлым үлкен –соғұрлым жақсы).

4) GPU- Intel HD 500 Series.

5) SATA3-120 GB және одан жоғары.

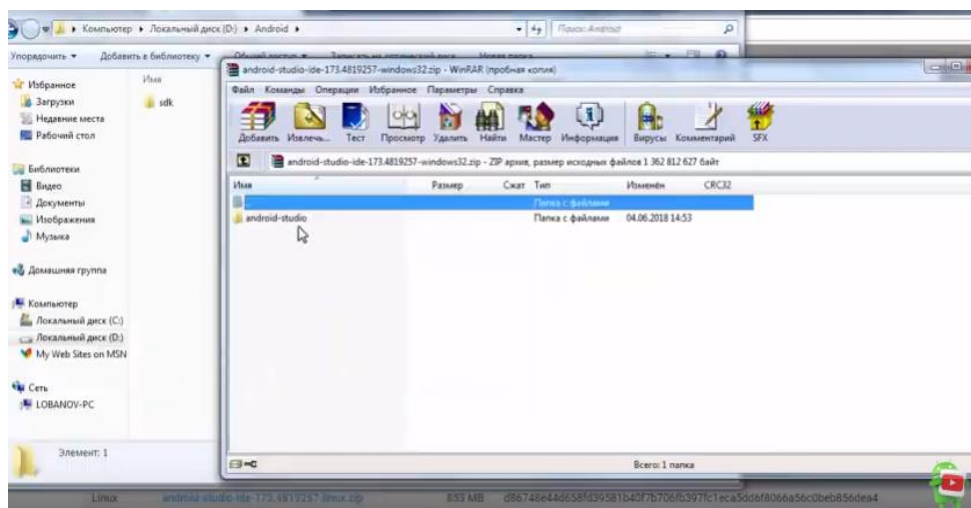
Android Studio 3.1.3 программасын орнатқаннан кейінгі процестер.Орнату, 32, 64 разрядты процессорларға арналған (Сурет 16).



Сурет 16 – Android Studio 3.1.3 программасы

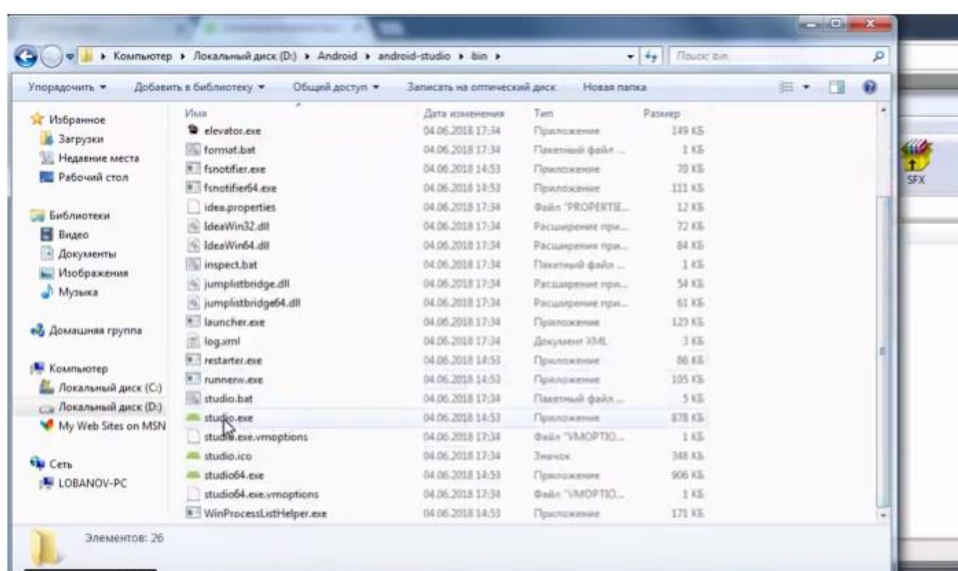
Қажетті процессор разрядтылығын таңдап, дайын архивтен қажетті версияны шығарып алуға болады.

Android Studio-ны пайдалану шарты беріледі (Сурет 17).



Сурет 17 – Android Studio-ны жүктеу

- дайын архивтік файлдан орнату файлы жүктеледі;
- орнату жолдары көрсетіліп, орнату файлы таңдалады (Сурет 18).

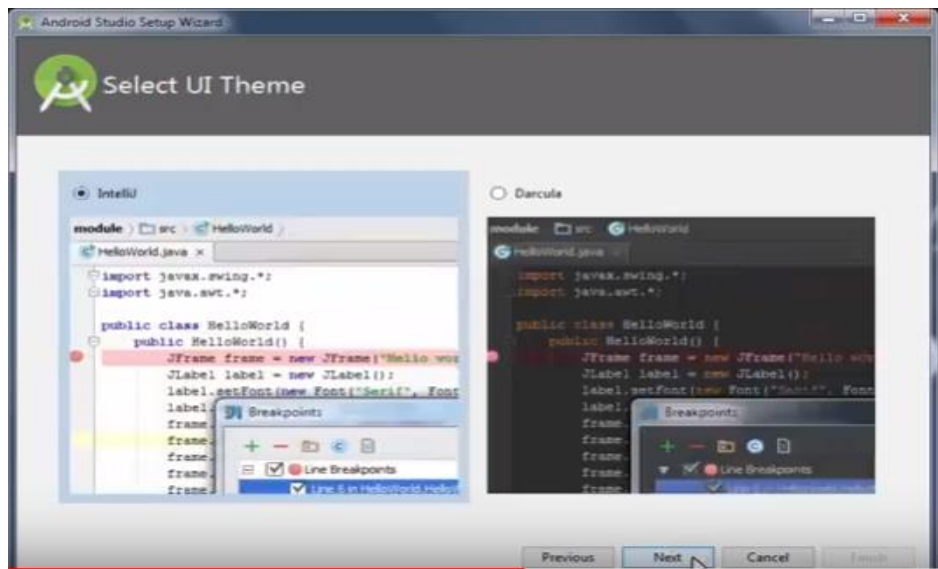


Сурет 18 – Орнату жолын көрсету

Осы жерде studio.exe файлы іске қосылады. Әрі қарайғы процесс дайын болғанға дейін Next батырмасын басу арқылы жалғасады. Баптаудың Стандартты және Қолданушылық нұсқасы ұсынылады. Егер сіз программа конфигурациясын жақсы білетін болсаңыз, онда Қолданушылық нұсқаны таңдауға болады. Программамен бұрын таныс емес қолданушылар Стандартты нұсқаны таңдаса қателеспейді [13].

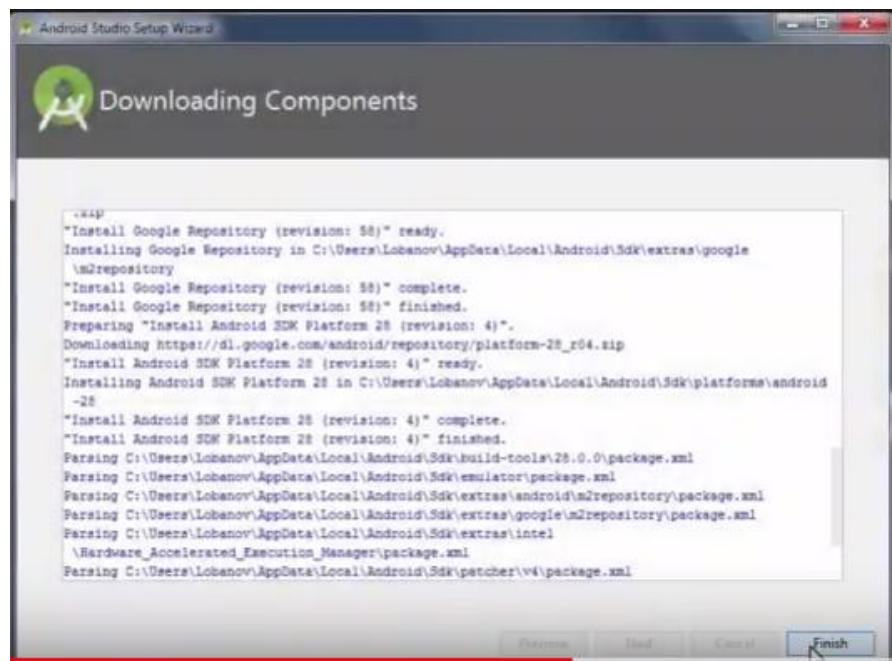
Әрі қарай интерфейс ті таңдау терезесі ашылады (Сурет 19). Онда екі түрлі интерфейс көрініс табады:

- ақ түсті интерфейс;
- қара түсті интерфейс;

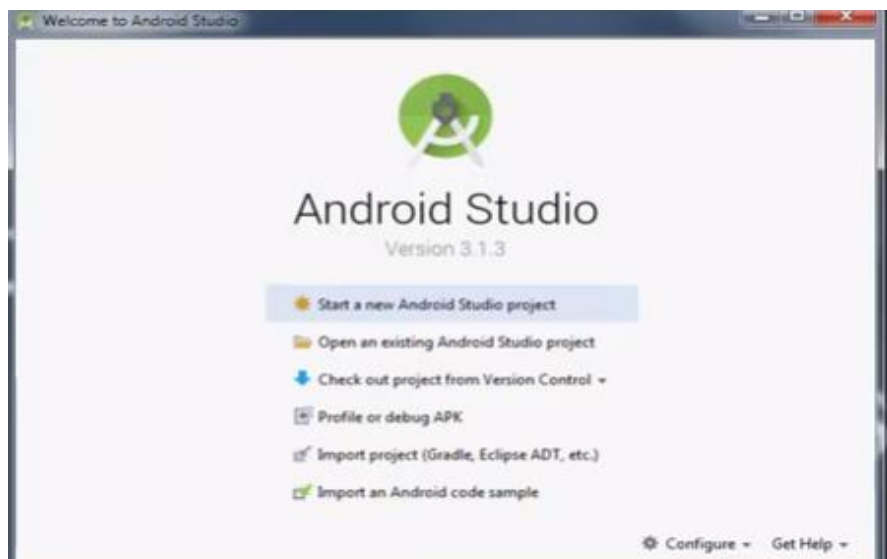


Сурет 19 – Программалау ортасының түсін таңдау

Программаның орнатылуы аяқталған кезде соңғы рет Finish батырмасы басылады (Сурет 20).



Сурет 20 – Программа жұмыс істеуге дайын

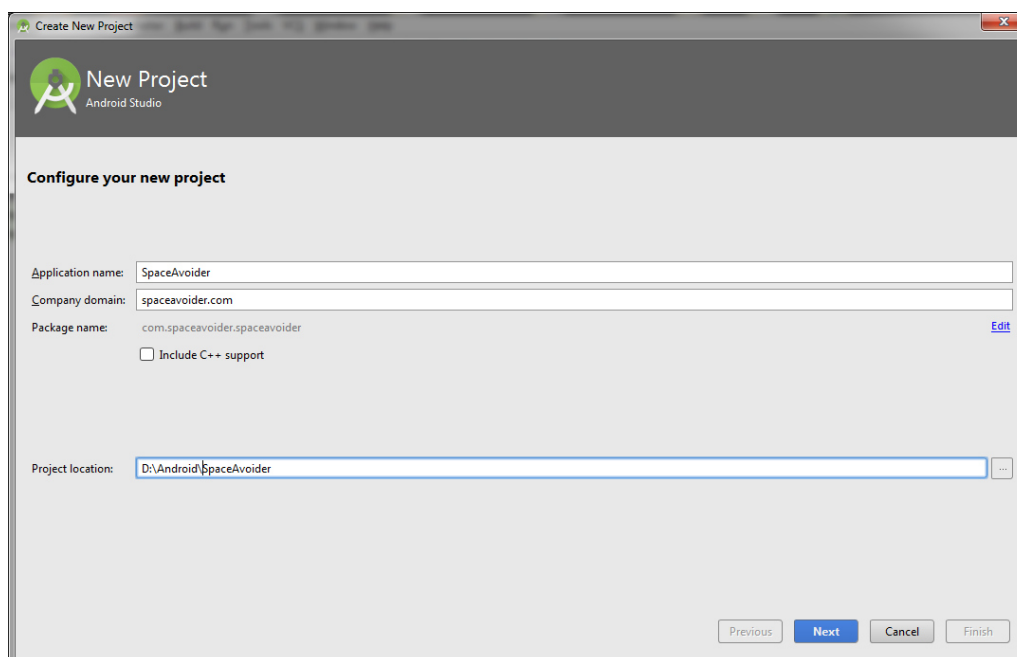


Сурет 21 – Орнатылған программа көрінісі

Әрі қажетті жобаны құрып, оның шаблондарын, форматын, стилін, дизайтын әзірлеуге болады (Сурет 21).

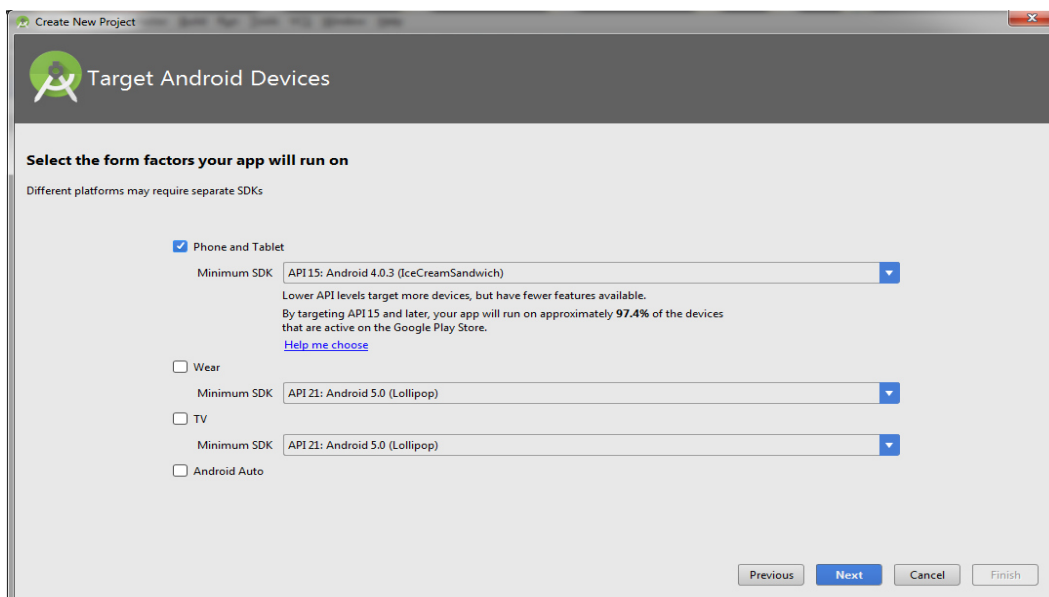
Жоба құру

Android Studio-ның жоғарғы жағындағы менюде File → New → New Project опциялары таңдалады (Сурет 22).



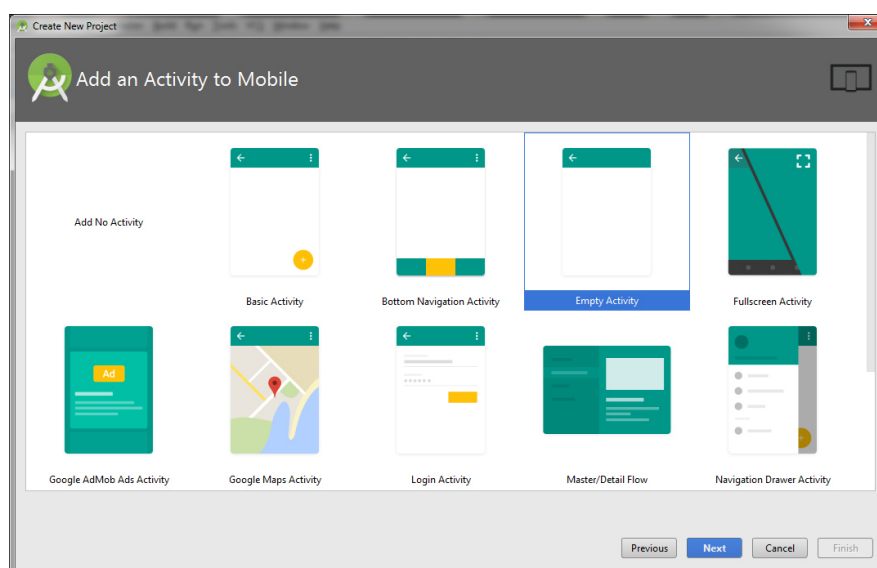
Сурет 22 – Жаңа жоба құру

Осы жерде қосымшаға атау беріп, доменін және жолын көрсету қажет. Әрі қарай Next батырмасы басылады (Сурет 23).



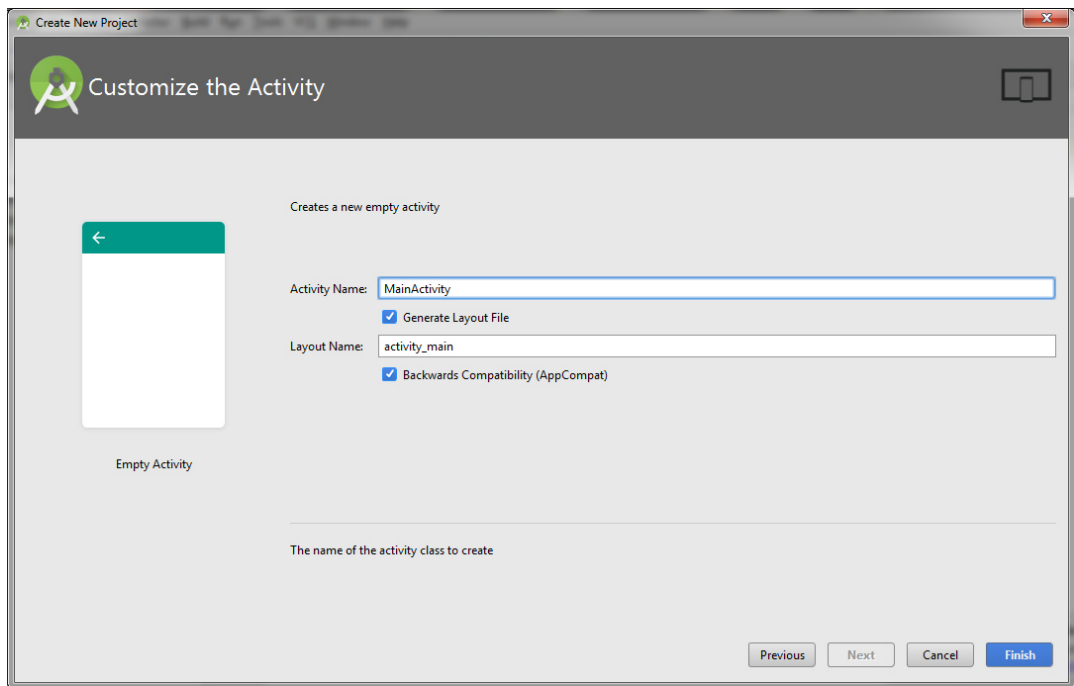
Сурет 23 – Программа версиясын таңдау

Осы жерде андройдтың қажетті версиясы көрсетіледі. Соынмен қатар андройд-сағат пен телевизорды таңдауға болады да Next батырмасы басылады (Сурет 24).



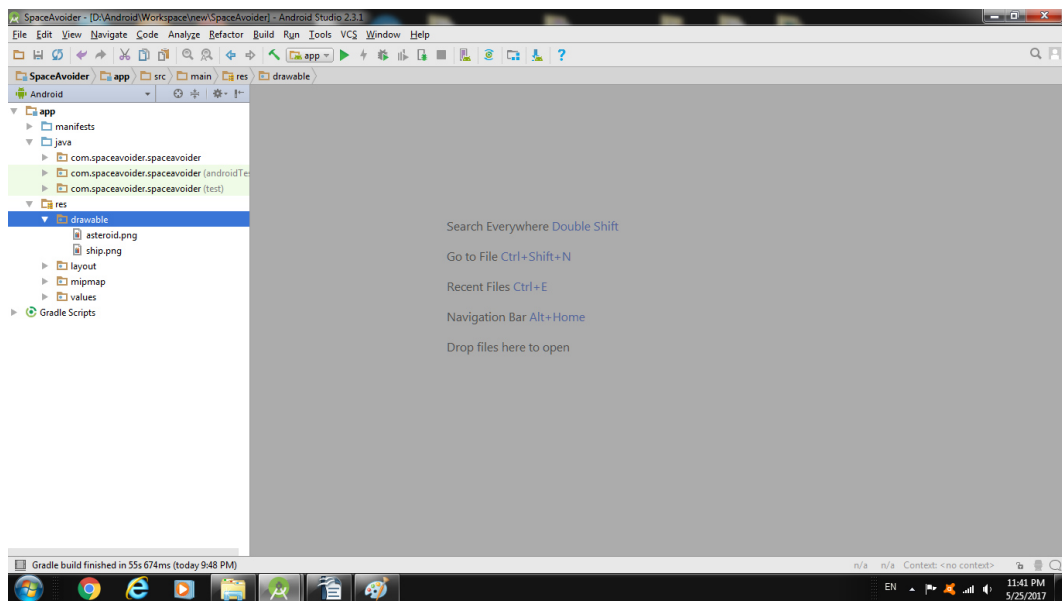
Сурет 24 – Шаблондар көрінісі

Бұл жерде міндетті түрде Empty Activity таңдалады және Next батырмасы басылады (Сурет 25).



Сурет 25 – Жобаны дайындауды аяқтау

Қажетті баптауларды енгізгеннен кейін немесе көрсетілген параметрлерді қалдыра отырып Finish басылады. Жоба құрылды деп есептейміз. Программа компоненттерінен архивті ашып (Сурет 26), одан қажетті суреттерді ашып, drawable папкасына көшіруге болады.



Сурет 26 - Программа компоненттерінен архивті ашып, одан қажетті суреттерді ашып, drawable папкасына көшіру

Әрі қарайғы жұмыс қолданушының таңдауына, көзқарасына және қалауына байланысты болмақ.

1.7.2 Java тарихы, мүмкіндіктері

Java 90-шы жылдардың басында пайда болды. Бұл бағдарламалау тілінің негізі C технологиясы (C, C++, C#). Бұл бағдарламалау барынша

жеңіл, барынша қауіпсіз болып табылады деуге болады.

Бастапқыда Java мобильдік қосымшаларды әзірлеу тілі ретінде пайдаланылды.

Java-дағы негізгі принцип файлдар компиляциясының орнына әр платформаға жарамды тиянақты бір рет код жазу, ол код қандай платформада болсын жұмыс істеу керек. Түрлі файлдар компиляциясының орнына барлық платформаға жарамды JAR-файл құру. Егер жүйе Java-ны қолдаса, файл орындалады. Осы принципті іске асыру үшін ауани Java машина немесе JVM жүзеге асырылған.

JVM – платформаға және оның әрі қарайғы қолданылуына байланысты компиляция барысын анықтаушы құралдар жиыны. Қазіргі нарықта Java тілі кең қолданысқа ие. Оның қызметі тек Android- қосымшалар әзірлеумен шектелмейді, ол мына бағыттарда да кең қолданысқа ие:

- 1) Android-қосымшалар құру;
- 2) десктоптық қосымшалар құру;
- 3) кәсіпорын жүйелері: жеке деректерді өңдеу, банк операциялары, қаржы, сауда салалары және т.б;
- 4) кіріктірілген жүйелер: смарт-сағаттар, контроллерлер, гибриді автолардың кейбір жүйелері;
- 5) Internet of Things,
- 6) ғылыми зерттеулер. Python және MATLAB-пен қатар, Java күрделі тапсырмаларды шешуде жақсы көрсеткіштер береді.

Java-технологияның артықшылықтары:

1) қолдануға жеңіл. C/C++ күрделі синтаксистерінен алынғанымен, Java тілінің технологиясы жеңіл де ықшам. Нәтижесінде қарапайым да қуатты программалау тілі пайда болады.

2) сенімділігі. Объектіге бағытталған программалау тілінің бір жақсы жері қате аз, Java деректерді мұқият талдап, қатені бірден анықтап отырады.

3) қауіпсіздік. Java бастапқыда мобильді қосымшалар қолданушыларының деректерімен жұмысқа арналған дегенді білдіреді. Яғни технология бастапқыда қауіпсіздіктің жоғары деңгейіне бағытталған, сондықтан қазіргі уақытта да осы принцип ұстанылады. Және ең қауіпсіз тіл деген пікір қалыптасқан.

4) платформаға тәуелсіздік. Java-да құрылған программалар платформаға (операциялық жүйелер, компьютердің аппараттық құраушылары) тәуелсіз жұмыс істейді.

5) абстрактылық. Java-да абстрактілі әдіс (модификатор abstract) деп, сол үшін параметрлер мен қайтарылатын мән түрі берілген әдіс аталады, бірақ дене емес. Абстрактілі әдіс Мұрагер кластарды анықталады. C++ таза виртуалды функция деп аталады. Класта абстрактілі әдістерді сипаттау үшін кластың өзі де абстрактілі ретінде сипатталуы тиіс. Абстрактілі класс объектілерін жасауға болмайды [14].

Класс кітапханалары:

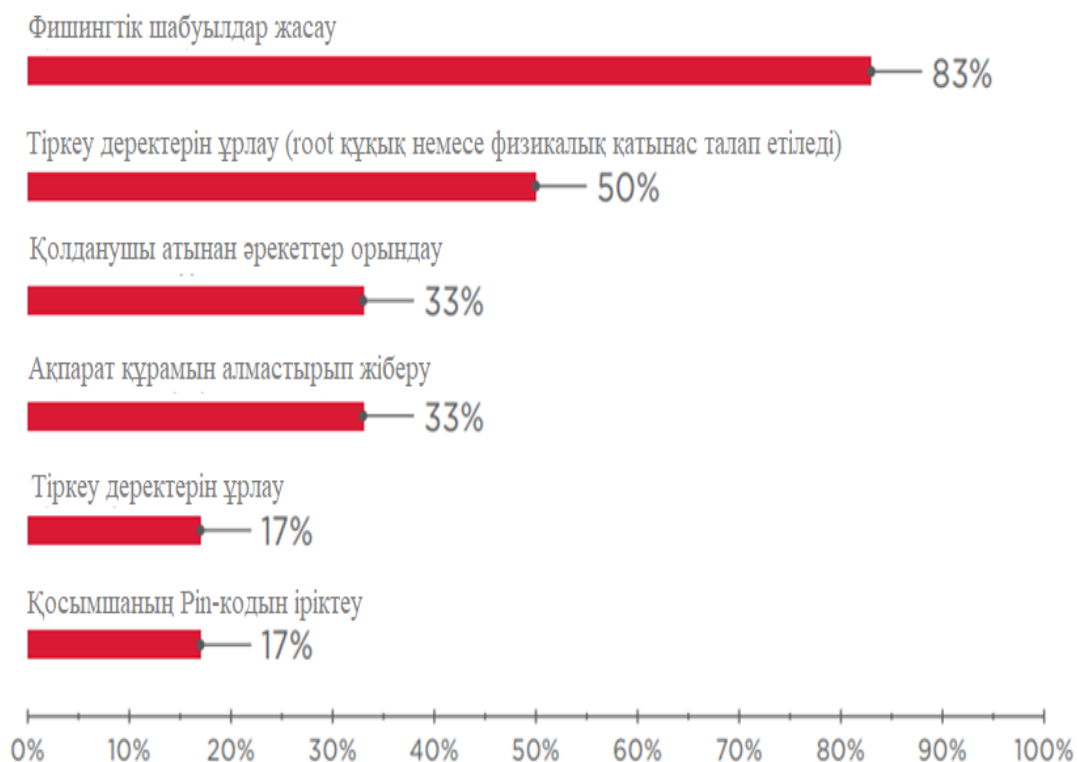
- JDK - Java SE және Java EE платформаларында барлығы үшін базалық кластар жиынтығын қамтиды;
- CDK - химиялық БҚ құру үшін қолданылады;
- JDOM - Java платформасының ерекшеліктерін ескеретін XML DOM іске асыру. БҚ әзірлеу құралдары;
- JDK - Java SE және Java EE платформаларына арналған кітапханалардан басқа, javac командалық жолының компиляторы және командалық жол режимінде жұмыс істейтін утилит жиынтығы бар;
- Net Beans IDE - барлық Java-Java ME, Java SE және Java EE платформалары үшін еркін интеграцияланған даму ортасы. Java әзірлеушісі Java тілінде және басқа тілдерде (C, C++, PHP, Fortran және т.б.) БҚ әзірлеуге арналған базалық құрал ретінде Sun Micro systems жүйесін насихаттайды;
- Eclipse IDE - Java SE, Java EE және Java ME үшін еркін интеграцияланған даму ортасы. IBM, Java тілінде және басқа тілдерде (C, C++, Ruby, Fortran және т. б.) БҚ әзірлеуге арналған негізгі құрал ретінде корпоративтік БҚ-ның аса маңызды әзірлеушілерінің бірі ретінде насихатталады;
- IntelliJ IDEA - Java SE, Java EE және Java ME платформаларына арналған даму ортасы
 - әзірлеуші - JetBrains компаниясы. Екі нұсқада таратылады: тегін (Community Edition) және коммерциялық (Ultimate Edition);
 - Jdeveloper - Java SE, Java EE және Java ME платформаларына арналған өңдеу ортасы. Әзірлеуші-Oracle компаниясы.
 - BlueJ - негізінен оқыту үшін құрылған, бірақ шағын бағдарламаларды әзірлеу үшін жарамды Java тілінде бағдарламалық жасақтаманы әзірлеу ортасы.

2 Мобильді қосымшаларға төнетін қауіптер. Олардан қорғану шаралары

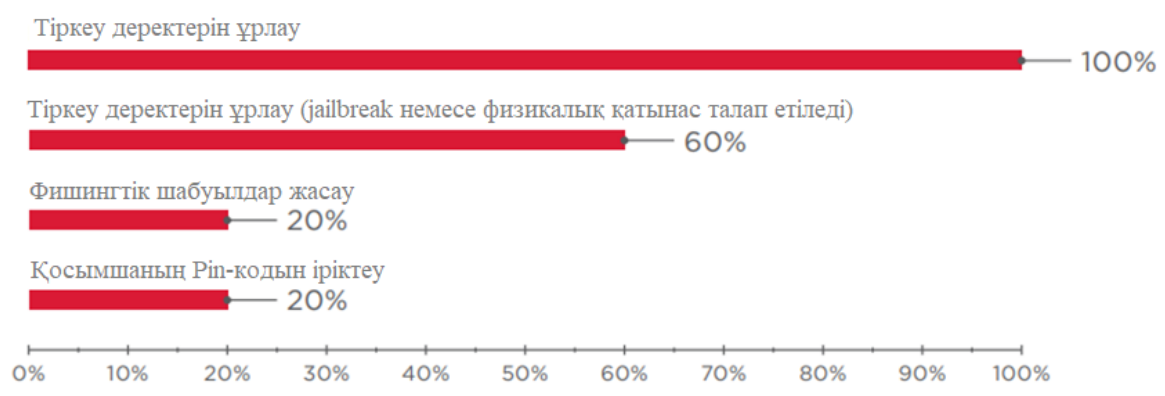
2.1 Шабуылдар түрлері, категориялары

Кез келген ақпараттық жүйе қатерге ұшырайды, бұл бір жағынан статистикалық деректермен расталады, екінші жағынан, кез келген басқа АЖ сияқты осалдықтар бар, оларды толығымен алып тастауға болмайды. Қандай ақпаратқа сұраныс бар, сол ақпаратқа қауіп бар. Көптеген аналитиктер ақпаратқа, соның ішінде мобильді қосымшаларға төнетін қауіптерге талдау жасай келіп, қауіптерді бірнеше бағыттарда қарастырып, жіктеуге болатындығын көрсетті. Ақпараттық қауіпсіздікті зерттеу үшін Android-қа арналған алты қосымша (Сурет 27), iOS үшін бес қосымшаны алып қарастырған(Сурет 28). Осы қосымшалардың қолданушылары келесі қауіп түрлеріне ұшыраған:

- пайдаланушы атынан әрекет жасау;
- есептік деректерді ұрлау;
- бағалар туралы ақпаратты ауыстыру;
- қосымшаның PIN-кодын іріктеу;
- фишингтік шабуылдар жасау.



Сурет 27 – Android қосымшаларын қолданушыларға жасалатын мүмкін шабуылдар (осал қосымшалар үлесі)



Сурет 28 – iOS үшін қосымшалар қолданушыларына жасалатын мүмкін шабуылдар (осал қосымшалар үлесі)

Анықталған осалдықтарды шарттардың бірін орындау кезінде пайдалануға болады:

- қаскүнем пайдаланушымен бір желіде орналасқан және трафик алуға мүмкіндігі бар;
- қаскүнем құрылғыға физикалық қол жеткізді;
- пайдаланушының құрылғысы зиянды БҚ жұқтырған (әсіресе root немесе jailbreak құқықтары бар болса).

"Improving Web Application Security" кітабында сипатталған үлгілер мен тәжірибеге сәйкес, төменде қосымшалар қауіпсіздігінің кең таралған қауіп-қатерлері / шабуылдары 3 – кестеде берілген:

Кесте 3 – "Improving Web Application Security" кітабында сипатталған қауіп категориялар

Категория	Қауіптер / Шабуылдар
Енгізуді тексеру	Буфердің аса толуы, сайттаралық скриптинг; SQL-кодты енгізу; стандарттау (канонизация)
Программалық қамтаманы бұрмалау	Қаскүнем екілік түзету, кодты ауыстыру немесе оны кеңейту арқылы рұқсатсыз әрекеттерді орындау үшін қосымшаның сипаттамаларын өзгертеді
Аутентификация	Желіні тыңдау; "өрескел күшпен" шабуыл; сөздік бойынша барлау; cookie файлдарын жұмысқа қосу; есептік деректерді ұрлау
Авторизация	Артықшылықтарды арттыру; құпия деректерді ашу; деректерді қолдан жасау
Конфигурацияны басқару	Әкімшілік интерфейстеріне рұқсатсыз кіру; параметрлер файлдарына рұқсатсыз кіру;

3-кестенің жалғасы

Құпия ақпарат	Қоймадағы маңызды кодқа немесе деректерге қол жеткізу; желіні тыңдау; зиянды кодты / деректерді енгізу
Сеансты басқару	Сеансты ұрлау; қайта жұмысқа қосу шабуылы; "ортадағы адам" шабуылы
Криптография	Криптографиялық тұрақты емес кілттерді генерациялау немесе кілттерді нашар басқару; нашар немесе стандартты емес шифрлау
Параметрлермен Манипуляция	Сұраныс қатары, форма өрістерімен манипуляция; cookie файлдарымен манипуляция; HTTP тақырыпшаларын манипуляциялау
Ерекшеліктерді басқару	Ақпаратты ашу, қызмет көрсетуден бас тарту (DoS)
Аудит және жүйеге кіру	Қолданушы операцияны орындауға тыйым салады: қаскүнем қосымшаны аңдатпай қолданады; қаскүнем өз ісін жасырады

OWASP қауымдастығы веб-қосымшалардың 10 ең осалдарының тізімін жариялады (Кесте 4) және сала үшін ашық стандарттарды жасауға ұмтыла отырып, ұйымдар үшін қауіпсіздікті қамтамасыз етудің үздік әдістерін сипаттайды.

Кесте 4 - 2017 жылғы жағдай бойынша қосымшалардың қауіпсіздігіне төнетін негізгі қауіп-қатерлер

Категория	Қауіптер / Шабуылдар
Енгізу	SQL-код енгізу; NoSQL; ОЖ командаларын енгізу; объектіге бағытталған көрсету (ORM); LDAP injection
Аутентификацияны бұзу	Есептік деректерді пайдаланумен жасалатын шабуылдар (деректер қорының жылыстауы / бұзылуы); "өрескел күшпен" шабуыл; әлсіз пароль
Маңызды деректерге әсер ету	Әлсіз криптография; шифрлаудың болмауы
XML сыртқы объекті	XML сыртқы объект шабуылы
Қатынасты бақылауды бұзу	CORS қате конфигурация; мәжбүрлі қарау; артықшылығын көтеру

4-кестенің жалғасы

Қауіпсіздікті дұрыс орнатпау	Түзетілмеген кемшіліктер; параметрлерде қауіпсіздік параметрлерін орнату мүмкін емес; ескірген немесе осал бағдарламалық жасақтама
Сайтаралық скриптинг (XSS)	Тұрақты, тұрақсыз (Сақталмаған); DOM-модельдер
Қауіпті десериализация	Деректер объектілері мен құрылымдарын өзгерту; деректерді қолдан жасау
Танымал осалдылықтарды қамтитын компоненттерді қолдану	Ескірген бағдарламалық қамтама; анықталмаған осалдықтар; базалық фреймворкаларды түзету қабілетсіздігі
Жеткіліксіз логиндеу және мониторинг	Тексерілетін оқиғаларды тіркеу қабілетсіздігі; журналдың түсінікті хабарламаларын генерациялау мүмкін еместігі: орынсыз ескертулер; нақты уақыт режимінде Белсенді шабуылдарды анықтау немесе ескерту қабілетсіздігі

Ақпарат қауіпсіздігін қамтамасыз ету әдістері

Әртүрлі АЖ-да қауіпсіздікті қамтамасыз ету бойынша талаптар айтарлықтай өзгеше болуы мүмкін, бірақ олар әрдайым үш негізгі қасиетке қол жеткізуге бағытталған:

1) құпиялылық-оған қол жеткізуді тек оған құқығы бар субъектілер ғана жүзеге асыратын ақпараттың жай-күйі.

2) тұтастық-ақпаратты рұқсатсыз өзгертуді болдырмау.

3) қол жетімділік-қол жеткізу құқығын алған пайдаланушылардан ақпаратты уақытша немесе тұрақты жасырмау.

Жоғарыда аталған қасиеттерді қамтамасыз ету үшін заңнамалық, ұйымдастырушылық және техникалық бірқатар шараларды орындау қажет.

Қауіптер модельдерін құру кезінде бірнеше анықтама беру қажет.

2012 жылдың қорытындысы бойынша Positive Technologies компаниясы АЖ веб-Қосымшаларының қорғалу деңгейіне талдау жүргізді, осыдан оларды іске асыру әдісі бойынша екі үлкен класты шабуылдарды бөліп көрсетуге болады:

- желілік шабуылдар;
- веб-қосымшалар осалдықтары.

2.2 Веб-қосымшалардағы шабуылдар және оларға қарсы іс-қимыл әдістері.

Интернет желісінің қарқынды дамуына бафланысты интернет-ресурстар шабуылдаушылар тарапынан келетін қауіпке толы. АЖ жұмысына әсер ету үшін хакерлерге АЖ құрылғысының технологиялары мен алгоритмдері туралы ерекше білім талап етілмейді, тек шабуыл бағытының IP-мекенжайын

білу жеткілікті. Интернет желісінің коммуникация құралдары бойынша жүзеге асырылатын шабуылдар оларға қарсы бағытталған жүйелер сияқты әртүрлі.

2.2.1 Пакеттер сниффері

Пакеттер сниффері – бұл программалық қамтама қазіргі уақытта желі арқылы берілетін барлық желілік пакеттерді ұстайды. Бұл программалар заңды болып табылады, бірақ кейбір хаттамалар ақпаратты шифрланбаған түрде береді және онда қаскүнемде пайдаланушылардың аттары немесе парольдер сияқты құпия ақпаратты, сондай-ақ пайдаланушылардың хабарламаларын ұстап қалу мүмкіндігі пайда болады. Қолданушылар әртүрлі АЖ-да бірдей деректерді жиі пайдаланады, сол арқылы осы деректерді ұстап алушы пайдаланатын көптеген қосымшалар мен жүйелерге қол жеткізе алады [15].

Пакеттер сниффингінен қорғау тәсілдері:

1) аутентификация. Парольдік криптографиялық сұлбаларды қолдану. Ол сниффер көмегімен ақпаратты ұстау мүмкіндігін болдырмайды, мысалы, Лэмпорт («Lamport hash chain») сұлбасы.

2) желілік жабдықты орнату. Егер бұл тәсілді тереңірек қарастырса, ол OSI (data link) моделінің 2 деңгейінде қауіпсіздікті қамтамасыз ету болып табылады, желілік жабдықтың дұрыс конфигурациясы кезінде қаскүнем желіге мүлдем қосыла алмайды немесе жабдықтың нақты желілік портына арналған ақпаратты алады, бұл тәсіл толық қорғануды бермейді, бірақ снифферді қаскүнемдердің пайдалану күрделілігін едәуір арттырады.

3) антиснифферлер. Бұл әдіс желіде жұмыс істейтін снифферлердің әрекеттерін танытын аппараттық немесе бағдарламалық құралдарды орнату болып табылады. Бұл тәсіл тиісті қорғауды қамтамасыз ете алмайды, бірақ қорғауды кешенді қамтамасыз ету кезінде қолданылады.

4) криптография. Пакеттердің сниффингімен күрестің ең тиімді жолы оларды ұстап қалуды болдырмайды, бірақ оны мағынасыз етеді. Ақпаратты ұстап қалу кезінде қаскүнем биттік мәндер түрінде пайдасыз деректер жинағын алады, олардан ақпаратты алу, есептеу қиын. Криптографиялық хаттамалардың мысалдары SSH (Secure Shell) және SSL (Secure Socket Layer).

2.2.2 IP-спуфинг

IP-спуфинг зиянкестер рұқсат етілген пайдаланушы ретінде өзін берген жағдайда орын алады. Бұл сондай-ақ IP хаттамасы негізінде жасалады. IP-спуфинг шабуылдары жиі басқа шабуылдардың бастапқы нүктесі болып табылады. Спуфинг қаупін төменде көрсетілген шаралар арқылы әлсіретуге (бірақ жоюға болмайды) болады.

Кіруді бақылау. Бұл әдіс мақсатты ресурсқа қосылу белгілі бір хостпен рұқсат етілген желі ішінде қорғау үшін өзекті, қалған трафик толығымен алынып тасталады.

Қосымша аутентификация құралдарын жасау. Сниффермен болған жағдайдағы сияқты, спуфинг шабуылшы үшін мағынасыз болады, мысалы пайдаланушы және пароль бойынша қосымша аутентификация қажет.

2.2.3 Қызмет көрсетуден бас тарту

Denial of Service (DoS), көп таралған шабуыл, оған толықтай қарсы тұру қиын. Бұл шабуыл ақпараттың қол жетімділік қасиетіне бағытталған, бұл үлкен ұйымдар үшін өте маңызды және оны іске асыру кезіндегі қаржылық шығындар көп. Көп таралған түрлері:

- 1) TCP SYN Flood;
- 2) Trinity;
- 3) Trinco;
- 4) Tribe Flood Network (TFN) және Tribe Flood Network 2000 (TFN2K);
- 5) Stacheldracht;
- 6) Ping of Death.

Шабуыл көптеген құрылғылар арқылы бір мезгілде жасалса, онда ол DoS (distributed DoS, DDoS) үлестірілген шабуылы болып табылады.

DoS типті шабуылдар қауіпін үш тәсілмен төмендетуге болады:

1) Антиспуфинг арқылы. Сіздің маршрутизаторлардағы және желіаралық экрандардағы антиспуфинг функциясының дұрыс конфигурациясы dos тәуекелін төмендетуге көмектеседі. Бұл функциялар кем дегенде RFC 2827 сүзгісін қамтуы тиіс. Егер хакер өзінің шынайы тұлғасын жасыра алмаса, ол шабуыл жасауға шешім қабылдай алмайды.

2) Анти-DoS қызметі. Маршрутизаторлардағы және желіаралық экрандардағы анти-DoS функциясының дұрыс конфигурациясы шабуылдардың тиімділігін шектеуге қабілетті.

2.2.4 Парольдік шабуылдар

Парольдік шабуылдарды ұйымдастыру жоғарыда сипатталған әртүрлі әдістермен жүргізілуі мүмкін. Қарапайым парольдерді қолданғанда қарапайым таңдау шабуылы өте маңызды (brute force attack). Көптеген жағдайларда осы шабуылды іске асыру үшін алдын ала анықталған анықтамалықтан мәндерді пайдалана отырып, кіру әрекеті арқылы ортақ пайдалану ресурсына қол жеткізуге тырысатын мамандандырылған бағдарлама пайдаланылады.

Егер мәтіндік формадағы парольдерді пайдаланбаса, құпия шабуылдарды болдырмауға болады. Бір реттік парольдер және/немесе криптографиялық аутентификация осындай шабуылдардың қауіп-қатерін іс жүзінде төндіруі мүмкін, бірақ барлық құрылғылар осы әдістерді қолдамайды. Әдетте жүйенің АЖ әртүрлі регистрлердегі символдар мен әріптер қамтылған ұзын парольдерді қолданатын саясатты ұстанады.

2.2.5 Man-in-the-Middle типті шабуылдар

Іске асыру тәсілі мен технологиялары бойынша бұл шабуыл өте әртүрлі. Оның мәні ақпаратты пайдакүнемдік мақсатта жою немесе өзгерту үшін беру хаттамасына араласуды жүзеге асыру болып табылады, олар сайып келгенде қалаған нәтиже береді. Осы шабуылдарға мысалдар

- 1) SQL-инъекциялар;
- 2) HTML/script-инъекция;

3) XSS-шабуылдар.

Man-in-the-Middle түріндегі шабуылдармен тек криптография арқылы тиімді күресуге болады. Бұл шабуылға мысал ретінде қаскүнем ақша қаражатын ұрлауға мүмкіндік алатын банк жүйелерін алуға болады.

2.2.6 Деректерді жинау шабуылынан қорғау (Fingerprinting)

Хакерлік шабуылдар fingerprinting-нен жиі басталады – операциялық жүйенің және жария сервистердің нақты нұсқасы туралы ақпарат жинау. Жүйенің іздерін алыстан алып тастауға қарсы әрекет ету үшін шаралар қабылдай отырып, сіз ең ерте кезеңде сіздің жүйеңізге шабуылдардың көпшілігін тоқтата аласыз

Сонымен қатар, fingerprinting қандай да бір статистикалық ақпаратты жинау кезінде қолданылады. Шабуылдарды анықтау жүйелерінде ол шабуылдаушы ОЖ-ні анықтауға немесе тіпті оны жалпы массадан бір мәнді бөлуге мүмкіндік береді (сондай-ақ саусақ іздері қылмыскерді сәйкестендіруге мүмкіндік береді).

Fingerprinting-тен қорғау тәсілдері

Ең дұрысы, желі, операциялық жүйелер мен қосымшалар деңгейінде, сондай-ақ қауіпсіздік рәсімдері деңгейінде кешенді шара ретінде fingerprinting-тен қорғауды енгізу қажет. Дегенмен, қорғаныс тіпті бір деңгейде де (мысалы, желіаралық экранды теңшеу) өз жемісін береді және ОЖ версиясын анықтауға мүмкіндік бермейді.

2.2.7 Қауіпсіздік концепциясына жоғарғы деңгейде енгізу

Қауіпсіздік саясатында ұйымның бағдарламалық қамтамасыз ету құпиясының статусын белгілеу қажет. Операциялық жүйенің нұсқасы, жария сервистің нұсқасы немесе серверде орнатылған басқа бағдарламалық қамтамалар туралы ақпаратты коммерциялық немесе құпия санатына жатқызу қажет. Желілік барлаудан қорғау процесін ұйымдастыруға қойылатын талаптарды осы процесс қандай рәсімдерде сипатталған және рәсімдерді іске асыруға кім жауапты, есептілік қандай көзделген, міне осы бағыттарда анықтау қажет.

Төменгі деңгейде рәсімдер мен нұсқауларға енгізу

Мысалы, желілік барлаудан қорғау арнайы процедурасын енгізу қажет. Онда таратылуы шектеулі ақпараттың сыртқа кетіп қалуын болдырмауды көздейтін мақсаттар, мақсатты орындау шарттары, қорғаудың түрлі профильдері (мысалы, көпшілік сервис, локальді сервис, сыни сервис), қызметкерлер міндеттерін үлестіру (мысалы, желі әкімшісі компьютерлік желі деңгейіндегі процедураларды жүзеге асыруға жауап береді, серверлер әкімшісі – жүйе деңгейіндегі, ақпараттық қауіпсіздік әкімшісі – орындалған шаралардың жеткіліктігін бақылау және бағалау), типімділікті және процедураларды тексеру тәртібі (мекеме ішінен де, сыртынан да қорғау әдістерін тестілеу), қызметкерлердің жауапкершіліктері (мысалы, мұрағатты сақтаушы – ақпараттың сыртқа таралып кетпеуіне, әкімшілер – шаралардың уақытылы өтіп тұруына жауап беру керек).

Бұдан басқа серверлер мен компьютерлік желінің қауіпсіздігін ұйымдастыру жөніндегі нұсқаулықта желілік барлаудан қорғау туралы тиісті пункттер енгізу қажет.

Желі деңгейінде практикалық іске асыру

Желінің сауатты топологиясы – бұл жүйені қашықтықтан зерттеудің ең тиімді контршарасы.

Бірінші мүмкін шара – желіаралық экранды пайдалана отырып трафикті сүзгіден өткізу. Тек бір ашық сервис портына қол жеткізу, стандартты емес желілік сұрауларды сүзгіден өткізу, ісmp-трафик. Желіаралық экранды пайдалана отырып, трафиктің бір бөлігін қосымшалар деңгейінде ауыстыруға болады.

2.2.8 XSS (сайттаралық скриптинг)

Шабуыл түрі сервер беретін зиянды кодты веб-бетке енгізуден тұрады, ол пайдаланушы осы бетті ашқан кезде орындалады. Бұл шабуыл пайдаланушының жеке деректерін алу немесе басқа сайттарға сілтемелер енгізу үшін пайдаланылуы мүмкін. Берілген Positive Technologies статистикасы бойынша шабуылдардың 63% пайызы XSS осалдығының көмегімен жасалды. Танымал веб-ресурста скрипт DDoS шабуылын ұйымдастыра алады.

Түрі бойынша XSS активті және пассивті болып бөлінеді, түсінікті болу үшін пассивтілер пайдаланушының іс-шараларын талап етеді, активті қолданушының қатысуынсыз орындалады.

- 1) XSS-ті енгізудің негізгі арналары:
- 2) Браузердегі қателер.
- 3) HTML арнайы символдарын экрандаудың болмауы.
- 4) Рұқсат етілген тегтерде атрибуттарды сүзудің және олардың мәндерінің болмауы.
- 5) Парақша тақырыпшасында кодалауды алмастырып жіберу.

XSS-тен қорғаудың негізгі тәсілдері:

- 1) беттерді генерациялау кезінде кіріс деректерін валидациялау және оларды өңдеу ("эскейпинг").
- 2) HTML-контекст маңыздылығы (body, attribute, JavaScript, CSS, URL).
- 3) Content Security Policy-ді енгізу.
- 4) HTTPOnly сессиялық куктар, оларды JavaScript-тен оқу мүмкіндігін тудырмас үшін.

2.2.9 SQL кодты енгізу (SQL-injection)

Пайдаланушы жіберген SQL код параметрлеріне енгізуге бағытталған шабуыл жасау әдісі, табысқа жеткен жағдайда қаскүнем сұрау логикасын өзгерте алады, жоюға немесе деректерді базаға қосуға мүмкіндік алады. Бұл шабуылдарды пайдаланудың көптеген түрлері бар, бірақ олардың барлығы өзінің синтаксистік дұрыс сұрауына пайдаланушы сұрауын өзгертуге бағытталған.

SQL-инъекциядан классикалық қорғау түріне байланысты қабылданатын

параметрлерді қатаң типтеу және сүзгіден өткізу, атап айтқанда тырнақшалар мен символдарды сүзу "-" \^*"болып табылады. Қазіргі заманғы көптеген әзірлеу құралдары ORM-ды (деректерді Объектілік ұсыну) пайдалану арқылы осы осалдықты түбірімен жоюға мүмкіндік береді, атап айтқанда Microsoft компаниясы өзінің EntityFramework шешімін ұсынады [16].

2.2.10 Сессияны/сертификатты болжау (Credential/Session Prediction)

Бұл әдісте пайдаланушы сессиясының бірегей мәнін табу, болжау арқылы өзін пайдаланушы етіп көрсетеді (бұл мүмкіндікті қаскүнем авторизациядан кейін иемденеді). Бұл әдіс Қосымша cookie-ді қолданатын сессия механизмін пайдаланғанда тиімді. Бұл шабуылдан қорғану үшін қолданушыларға арналған уникальді идентификаторларды генерациялаудың сенімді алгоритмдерін пайдалану қажет.

2.2.11 Серверді дұрыс орнатпау (Server Misconfiguration)

Серверді дұрыс баптау мәселесі зиянкестер үшін шабуылдардың тағы бір векторын береді, бастапқы бойынша серверді орнату кезінде пайдаланылмайтын көптеген қызметтер енгізілген, бірақ сол арқылы зиянкестерге шабуыл жасауға мүмкіндік береді, мысалы сервер конфигурациясының файлдары қол жетімді, қажетсіз қызметтер (контентті басқару, қашықтан басқару), сондай-ақ баптау функциялары немесе әкімшілік функциялары енгізілген. Осының бәрі аутентификация әдістерін айналып өту және жоғары артықшылықтармен құпия ақпаратқа қол жеткізу үшін қаскүнемнің тиімді құралы болып табылады. Сервер белгілі тіркеу жазбаларын, әдепкі парольдерді қамтуы мүмкін. SSL сертификаттары және шифрлау параметрлері, әдепкі куәліктерді пайдалану және сыртқы жүйелермен тиісті емес аутентификация ақпараттың құпиялылығына қауіп төндіруі мүмкін. Қателер туралы толық және ақпараттық хабарламалар деректердің сыртқа кетуіне себеп болуы мүмкін және шабуылдың келесі қадамын дайындауда қолданылуы мүмкін.

2.2.12 CSRF

Мұның осалдығы мынада, веб-қосымша қарапайым сілтеме бойынша көшкен кезде қандай да бір әрекет орындауға мүмкіндік береді. Қаскүнем арнайы URL дайындайды, ол жүктелген кезде клиенттің қаржысын аударып алады да оны сурет ретінде танымал ресурстардың біріне орналастырады.

CSRF-тен қорғау әдістері:

- арнайы токендермен сұрауларға қол қою.
- токендерге қосымша, барлық әрекеттерді POST-сұраныстарға аудару
- сұраныстар көздерін тексеру.
- белгілі осалдықтары бар компоненттерді пайдалану;
- кең танымал және өндірушілер түзеткен ПҚ-дың осалдықтары қолданылады.

Бұл осалдықтарды жою үшін мынадай шаралар атқарылу керек:

- барлық бөгде компоненттер тізімін жасау;
- дер кезінде жаңарту;

- қажетсіз қызметтерді алып тастау;
- автоматтандырылған тексеруді ендіру.

Ашық қайта бағыттау (Open redirect)

Мұндағы осалдық – қолданушыны параметр ретінде қайта бағыттау үшін сілтемелерді қолдану және осы параметрлерді қосымша деңгейінде тексерудің. Осалдық фишингтік шабуыл үшін жиі қолданылады. Қорғау әдістері:

- сыртқы ресурстарға қайта бағыттаудан бас тарту;
- таныс емес адресстер үшін «Растау құжатын» жүргізу [17].

2.3 Мобильді қосымшалар қауіпсіздігін қамтамасыз ету әдістері мен құралдары

Болашақта ашық платформаның функционалдық мүмкіндіктерін ұсынатын мобильді құрылғылардың үлесі өсе береді деп күтілуде. Бұл платформалардың ашықтығы мобильді экожүйенің барлық бөліктері үшін, пайдаланушының қажеттіліктері мен талаптарына сәйкес орнатылуы, жойылуы немесе жаңартылуы мүмкін бағдарламалар мен қызметтерді – опцияларды икемді ұсыну мүмкіндігінің арқасында айтарлықтай қолайлылықтар тудыру. Алайда, мобильді ресурстарға және API-интерфейстеріне белгісіз немесе сенімсіз шыққан қолданбаларға шексіз қол жеткізу пайда болады, бұл пайдаланушыға, құрылғыға, желіге немесе барлығына түгелдей зиян келтіруі мүмкін, егер тиісті қауіпсіздік сәулет мен желілік сақтық шаралары пайдаланылмаса.

Қолданба қауіпсіздігі ашық ОЖ бар (Symbian OS, Microsoft, BREW және т. б.) ұялы құрылғылардың көпшілігінде қандай да бір нысанда қамтамасыз етіледі. 2017 жылы Google үшінші тұлғалар әзірлеген және Google Play Store арқылы қол жетімді қосымшаларда табылған осалдықтарды қамту үшін табылған осалдықтар үшін өз сыйақы бағдарламасын кеңейтті. Оның ішінде өнеркәсіптік топтар болып саналатын GSM және Open Mobile Terminal Platform (OMTP) қауымдастығы да бар.

Мобильді қосымшалардың қауіпсіздігін арттырудың бірнеше стратегиясы бар:

- қосымшалардың "ақ тізімін" құру;
- транспорттық деңгей қауіпсіздігін қамтамасыз ету;
- қатаң аутентификация және авторизация;
- жадқа жазу кезінде деректерді шифрлау;
- қосымша «Құмсағаты»;
- API деңгейінде қосымшаларға қол жеткізуді ұсыну;
- пайдаланушының идентификаторына процестерді байланыстыру;
- мобильді қосымша мен ОЖ арасындағы өзара іс-қимылды алдын ала анықтау;
- қосымшаға артықшылығы жоғары қатынас ұсыну үшін қолданушыны растаут талаб;
- сеансты дұрыс өңдеу.

Қосымшалар қауіпсіздігін тестілеу

Қауіпсіздікті тестілеу әдістері қосымшалар қауіпсіздігіне осалдықтарды немесе тесіктерді анықтайды. Бұл осалдықтар қосымшаларды эксплуат үшін ашық қалдырады. Ең дұрысы, қауіпсіздікті тестілеу осалдықтарын уақтылы және мұқият жою үшін бағдарламалық қамтаманы әзірлеудің барлық өмірлік циклі бойы жүзеге асырылуы тиіс. Өкінішке орай, тестілеу әзірлеу циклінің соңында жиі өткізіледі. DevOps және Continuous delivery (үздіксіз жеткізу) танымалдылығының өсуімен бағдарламалық жасақтаманы әзірлеу және өрістету модельдері ретінде, үздіксіз қауіпсіздікті қамтамасыз ету модельдері неғұрлым танымал болады.

Осалдықтар сканерлері және нақты, веб-қосымшалардың сканерлері, сондай-ақ еруге тестілеу құралдары ретінде танымал құралдарды (мысалы, этикалық хакердің құралдары) HTTP сұраныс/жауаптарының қауіпсіздігін тестілеуді автоматтандыру үшін қауіпсіздік жөніндегі ұйымдар мен консультанттар жиі қолданады; дегенмен, бұл бастапқы кодты нақты тексеру қажеттілігін алмастырмайды. Бағдарламаның бастапқы кодын тексеру қолмен немесе автоматты түрде орындалуы мүмкін. Жеке бағдарламалардың жалпы көлемін (кодтың 500 000 жолы немесе одан көп) ескере отырып, адам барлық ықтимал осалдықтарды қолмен толық тексеру үшін қажетті деректерді жан-жақты талдауды орындай алмайды. Ол үшін бастапқы кодты талдаудың автоматтандырылған құралдары пайдаланылады, содан кейін сүзу және нәтижелерді талдау жүзеге асырылады.

Қосымшалардағы осалдықтарды анықтау үшін автоматтандырылған құралдардың көптеген түрлері бар. Олардың кейбіреулері қауіпсіздік сараптамасын жүргізудің үлкен тәжірибесін талап етеді, ал басқалары толығымен автоматтандырылған пайдалануға арналған. Нәтижелер талдағышқа ұсынылған ақпарат түрлеріне (бастапқы файлдар, екілік файлдар, HTTP трафигі, конфигурация, кітапхана, қосылыстар), талдау сапасына және Қамтылған осалдықтарға байланысты. Қосымшалардың осалдығын анықтау үшін пайдаланылатын жалпы технологиялар мыналарды қамтиды:

Қосымшалардың қауіпсіздігін статикалық тестілеу (SAST) – бұл бастапқы кодты талдау құралы ретінде жиі қолданылатын технология. Әдіс бастапқы кодты қосымшаны іске қосар алдында осалдықтардың болуын талдайды. Бұл әдіс аз жалған оң нәтиже береді, бірақ көптеген іске асырулар үшін қосымшаның бастапқы кодына кіру талап етіледі және сараптамалық конфигурация және үлкен есептеу қуаттарын қажет етеді.

Қосымшалар қауіпсіздігін динамикалық тестілеу (DAST) – бұл автоматты сканерге URL-адресін беру арқылы көрінетін осалдықтарды таба алатын технология. Бұл әдіс оңай масштабталып, оңай интегралданады және жылдам. DAST кемшіліктері сараптамалық конфигурация және жалған жұмыс істеу ықтималдығы жоғары.

Қосымша қауіпсіздігін интерактивті тестілеу (IAST) – бағдарлама құралдарын пайдалана отырып, қосымшаларды ішінен бағалайтын шешім. Бұл әдіс IAST және DAST артықшылықтарын пайдалануға мүмкіндік береді,

сондай-ақ кодқа, HTTP трафикке, кітапхана туралы ақпаратқа, ішкі қосылымдарға және конфигурация туралы ақпаратқа қол жеткізуге мүмкіндік береді. Кейбір IAST өнімдері Қосымшаның шабуылға ұшырауын талап етеді, ал басқалары әдеттегі сапа тестілеу кезінде пайдаланылуы мүмкін.

Қосымшалар қауіпсіздігін қамтамасыз ету Интернет желісінде өзінің коммерциялық қызметін жүргізетін компаниялар клиенттерінің кибершабуылына бағытталған зиянды бағдарламаларды дамыту 2007 жылдан бастап веб-қосымшаларға қойылатын талаптарды өзгертуге түрткі болды. Интернет пайдаланушыларының айтарлықтай саны зиянды БҚ-мен залалданған, сондықтан залалданған машиналардан жіберілген кез келген деректер зиянды болуы мүмкін. Осыған байланысты, клиенттік Тарапқа немесе веб-серверге қарағанда, бекенде ақпаратты қорғаудың және шабуылдарды блоктаудың озық жүйелері енгізілуде. 2016 жылғы жағдай бойынша БҚ өзін-өзі қорғау технологиялары кеңінен қолданылды. RASP орындау ортасымен бірге енгізіледі немесе хакерлік шабуылдарды анықтауға және болдырмауға мүмкіндік береді.

Осалдықтарды үйлестірілген анықтау

CERT үйлестіру орталығы – CVD (ағылш. Coordinated Vulnerability Disclosure) "ақпараттық қауіпсіздік осалдығын азайту кезінде қарсыластың артықшылығын азайту процесі" ретінде осалдықтардың Үйлестірілген ашылуын сипаттайды. CVD- бұл осалдықтарды жою үшін бірге жұмыс істейтін бірнеше мүдделі тараптар (пайдаланушылар, бағдарламалық қамтамасыз ету жеткізушілері, қауіпсіздік мамандары) қатысатын итеративті көп кезеңді процесс. CVD процестеріне бірнеше мүдделі тараптар қатысатындықтан, коммуникацияны басқару және осалдықтарды жою табысқа жету үшін шешуші мәнге ие.

Пайдалану тұрғысынан көптеген құралдар мен процестер CVD-ға көмектесе алады. Оларға қателерді бақылау жүйелері мен Bug Bounty бағдарламалары жатады.

2.4 Android ОЖ қорғау компоненттері

Android операциялық жүйесі қауіпсіздікпен байланысты қателердің жиілігін және әсерін азайтуға мүмкіндік беретін бірқатар кіріктірілген функцияларға ие. Жүйе стандартты құралдарды пайдалану кезінде қауіпсіздікпен байланысты күрделі шешімдерді болдырмау үшін жобаланған.

Келесі базалық қорғау құралдарын бөліп көрсетуге болады:

- кодты орындауды және басқа қосымшалардан бөлек түрде деректермен жұмыс істеуді қамтамасыз ететін оқшауланған бағдарламалар ортасы (Android Application Sandbox);

- криптография, кіру құқығы, қауіпсіз процессаралық өзара іс-қимыл сияқты негізгі қорғау функционалын сенімді жүзеге асыратын қосымшалар фреймворкы (IPC);

- ASLR, NX, ProPolice, safe_iop, OpenBSD dlmalloc, OpenBSD calloc және операциялық жүйесінен келген Linux mmap_min_addr сияқты технологиялар;

- файлдық жүйені шифрлау;
- телефонның жүйелік функцияларына қатынасты шектеуші, қолданушыларға ұсынылатын мүмкіндіктер (User-granted permissions);
- әрбір қосымшаның негізінде деректерді басқару үшін қосымшада көрсетілген рұқсаттар.

Аталған қорғаныс құралдарын және олардың үйлесімін қолдану арқылы қосымшаны бұзу ықтималдығын айтарлықтай азайтуға болады [18].

2.5 Реверс-инжинирингтен Android қосымшаларын қорғау. Обфускация

Обфускация (лат. obfuscare — адастыру) немесе кодты шатастыру — бастапқы мәтінді немесе орындалатын бағдарлама кодын оның функционалдығын сақтайтын, бірақ талдауды, декомпиляция кезінде жұмыс алгоритмдерін түсінуді және модификацияны қиындататын түрге келтіру.

- кодты "шатастыру" алгоритмі, бастапқы мәтін және/немесе ассемблерлік мәтін деңгейінде жүзеге асырылуы мүмкін. Шатасқан ассемблер мәтінін жасау үшін бағдарламаны орындау ортасының өзгермейтін немесе құжатталмаған мүмкіндіктерін пайдаланатын мамандандырылған компиляторлар пайдаланылуы мүмкін. Сондай-ақ, арнайы бағдарламалар да бар. obfuscator);

- кері әзірлеуді болдырмау немесе DRM айналып өтуді және лицензияларды тексеру жүйелерін болдырмау мақсатында проприетарлық бағдарламаларды декомпиляциялау қиындығы;

- жұмыс кодының мөлшерін азайту және (егер білінбейтін тіл пайдаланылса) жұмысты жеделдету мақсатында бағдарламаны оңтайландыру;

- программист тілінің мүмкін емес мүмкіндіктерін және біліктілігін көрсету (егер аспапты құралдармен емес, қолмен жүргізілсе).

2.5.1 ProGuard

Proguard – Андроид астында әзірлеу кезінде кодты жою үшін ең жиі қолданылатын құрал, ол тегін, ашық бастапқы коды бар. Сонымен қатар DexGuard одан да жетілген программа бар, ол да қосымшаны қорғауға арналған.

Пайдаланылмайтын кодты жою

Қолданылмайтын код — ақпараттың артық байттары, Proguard оны жояды да, программаның ақырғы өлшемін (Apk) үнемдейді. Бұл процедураны абайлап жасау керек, егер год рефлексия арқылы қолданылса, онда обфусцирленген қосымша бұзылады.

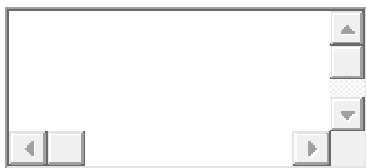
Proguard қалай бапталады?

Нақты нұсқаулықты Андроид ресми құжаттарынан табуға болады, жалпы бұл процесс мынадай тәртіпте өтеді:

build.gradle-ді өзгерту

Java

11 lines



```
android {  
    ...  
  
    buildTypes {  
        release {  
            shrinkResources true  
            minifyEnabled true  
            proguardFiles getDefaultProguardFile('proguard-android.txt'),  
                'proguard-rules.pro'  
        }  
    }  
}
```

Сурет 29 – build.gradle-ді өзгерту

Мұндағы, `getDefaultProguardFile('proguard-android.txt')` — Android SDK-дағы Андроиддың базалық конфигі (Сурет 29). Бастапқы түрде ондағы оңтайландыру ажыратылған, оны қосу үшін

`proguard-rules.pro` — тікелей қолданушы модуліндегі конфигурациямен алмастырылу керек [19].

Қосымша басқа да кітапханаларды қолдануы мүмкін, мұндада Proguard-ты баптаудың қосымша баптаулары талап етілуі мүмкін. Көптеген қажетті конфигтерді қамтитын (кең қолданылатын кітапханалар үшін) снопеттер жинағы бар, ол [GitHub](#) жобасы ретінде танымал. Баптаудың барлық файлдарын қолданушы модуліндегі `proguard` папкасына салса жеткілікті (бастапқы бойынша `app`), ал `build.gradle`-ке қатарды қосу қажет, сонда `proguard` үшін жауап беретін блок мына түрге келеді:

Java

4 lines



1
2
3
4

```
minifyEnabled true  
shrinkResources true  
proguardFiles getDefaultProguardFile('proguard-android.txt')  
proguardFiles(file('./proguard').listFiles())
```

Сурет 30 – build.gradle-ке қатарды қосу

proguardFiles(file('./proguard').listFiles()) фрагменті proguard папкасынан барлық конфиг файлдарды алып (Сурет 30), қолданушы құрып отырған қосымшада обфускация кезінде қолдануға мүмкіндік береді.

Енді қосымшаның жұмысқа қабілеттігін тексеруге болады. Обфускациясыз Debug жиынтықты емес, нақты оңтайландырылған қосымшаны тексереді. Бұл қолданушыда жұмыс істегенімен, тестілеушіде программа жұмыс істемейді.

Осылайша Proguard қолданушы қосымшасында жұмысқа дайын болады.

2.5.2 DexGuard

Жоғарыда айтып кеткендей, егер қолданушыға тек базалық обфускация мен оңтайландыру қажет болса, онда нағыз қажет аспап, ол – ProGuard (Кесте 5). Егер — сіздің қосымшаңыз немесе кітапханаңыз қорғаудың маңыздырақ шарасын талап етсе, онда DexGuard қажет. Осы екі құралдың арасындағы айырмашылықтар:

Кесте 5 – ProGuard және DexGuard сипаттамалары

ProGuard	DexGuard
Java байт кодын оңтайландыру	Жиі қолданылатын кітапханалардың тюнингтелген нұсқаларын қамтитын кешенді қорғау Android қосымшасы (Google play service, Dagger, Realm, SQLCipher және т.б.)
Кодты статикалық талдаудан базалық қорғау	Қолданбаны статикалық және динамикалық талдаудан қорғау

5-кестенің жалғасы

Бағдарлама коды байтындағы Фокус	Манифест файлдарын, нативті кітапханаларды, ресурстар файлдарын және т.б. оңтайландыру, фигуралау және шифрлеу.
Әдіс кластарын және т.б. қайта атау арқылы Инжиниринг реверсін күрделендіру.	Базалықтан басқа, арифметикалық және логикалық операция, әдістерді орындау тәртібін бақылау, жолдар мен кластарды шифрлау, сыни деректерге қол жеткізу үшін рефлексия қосу
Ашық бастапқы коды бар құрал	Лицензияны талап ететін коммерциялық инструмент

3 Мобильді қосымшаны құру және қауіпсіздік шарасын қамту

3.1 Web-қосымша құрылымы

Қосымшалар әдетте "қабаттар" деп аталатын логикалық бөліктерге бөлінеді, бұл ретте әрбір қабатқа өз рөлі тағайындалады. Жергілікті қосымшалар тек бір қабаттан тұруы мүмкін, ол клиенттің компьютеріне орналастырылады, ал web-қосымшалар өзінің табиғаты бойынша N – қабаттық тәсілге сай келеді. Әр түрлі нұсқалар мүмкін болса да, ең көп таралған қосымшалар үш қабатты пайдаланатын: көрініс қабаты; бизнес-логика қабаты; деректерге қол жеткізу қабаты (қойма). Әрбір қабат арнайы функцияларды орындайтын компоненттер жиынтығын (кластар жиынтығын) қамтиды.

Төмендегі суретте функционалдық салалар бойынша топтастырылған ең жиі қолданылатын компонент жиынтығымен web-қосымшаның типтік архитектурасы көрсетілген.

Көрініс қабаты әдетте пайдаланушы интерфейсінің (UI) компоненттерін және ұсыну логикасын қамтиды. Ойын – логика қабаты Функционалдық тапсырмалар мен Ойын компоненттерін қамтиды (Сурет 31). Деректерге қол жеткізу қабаты талап етілген деректер мен web-сервистерге қол жеткізуді іске асыратын компоненттерді қамтиды.



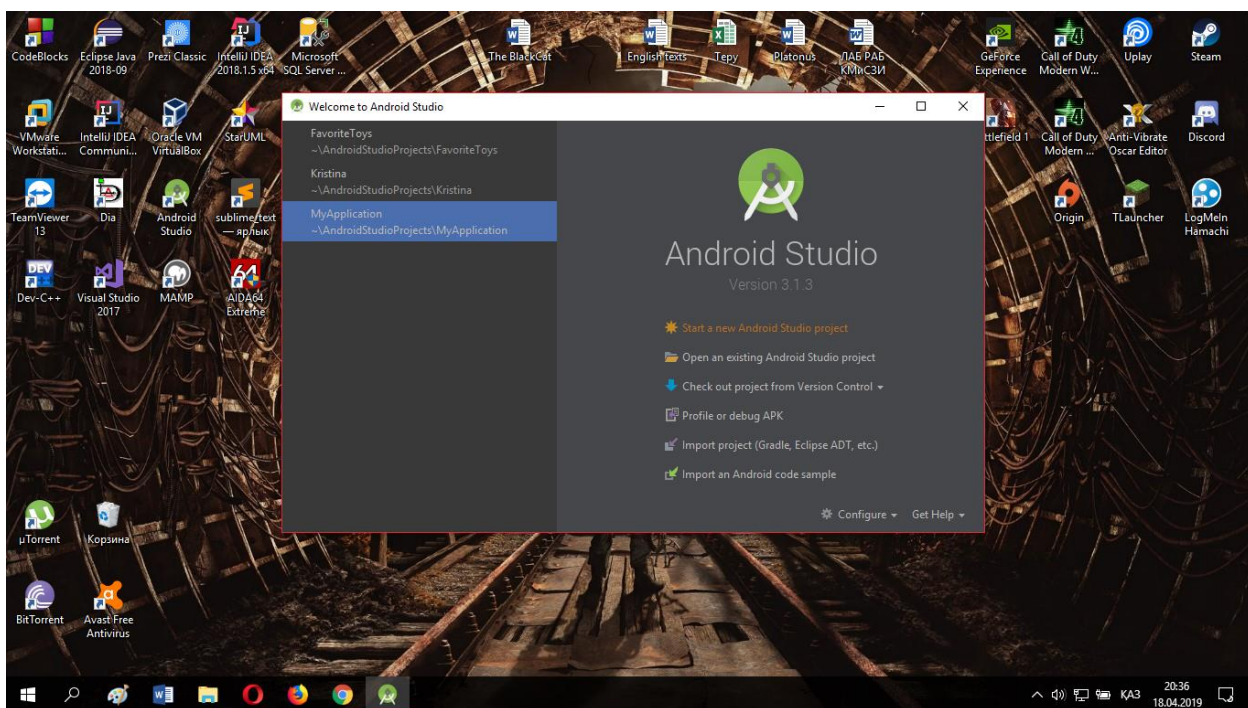
Сурет 31 – Функционалдық салалар бойынша топтастырылған ең жиі қолданылатын компонент жиынтығымен web-қосымшаның типтік құрылымы

Сонымен қатар қауіпсіздікті қамтамасыз ету шарасы қамтылған.

Бағдарламада Қосымшаны рұқсат етілген қолданушылар ғана қолдана алатын шара қамтылған, ол қолданушыны пароль және логин арқылы идентификациялау және Қосымшаның программалық кодын өзгертуден сақтаудың тиімді жолы, Android Studio-да тіркелген ProGuard — бұл кодты қысқарту, оңтайландыру және жою құралы.

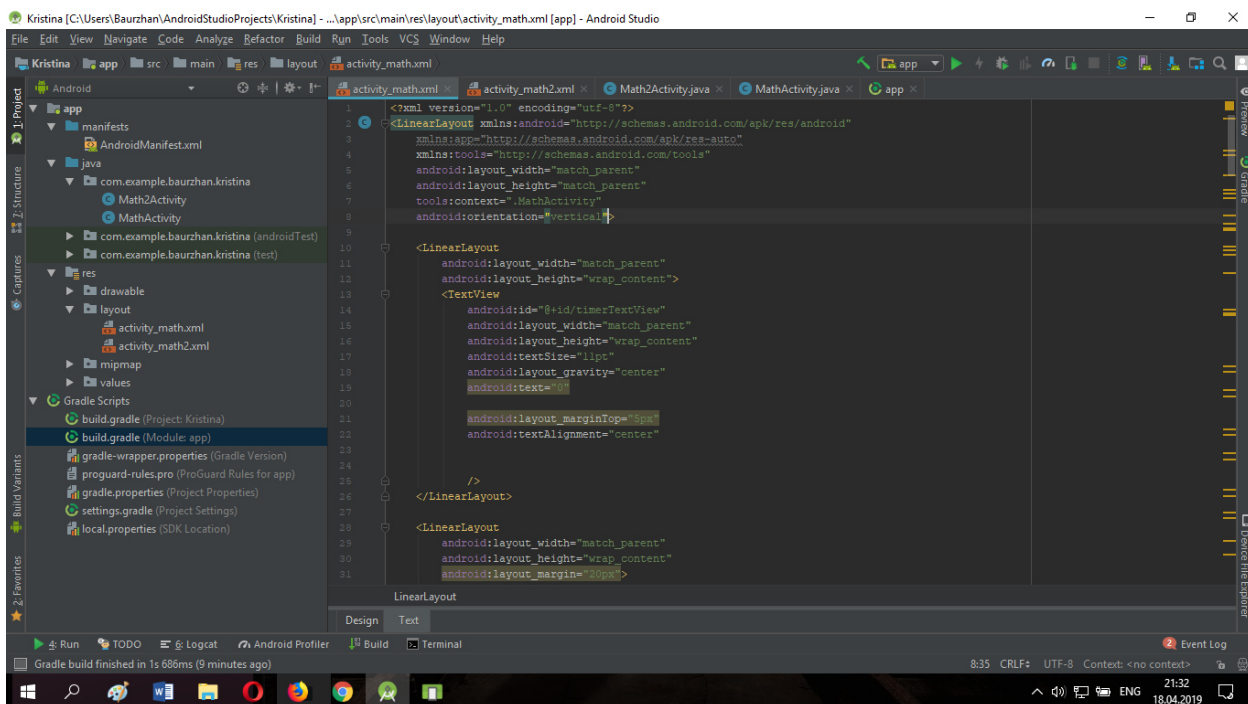
3.2 Android ОЖ үшін қосымша әзірлеу

Android ОЖ үшін қосымша әзірлеуде Android Studio орнатылу керек. Android SDK әзірлеу құралдарын әзірлеушілер сайтынан жүктеуге болады, сонымен қатар SDK элементтерін таңдауға болады. Android қосымшасын әзірлеуде кең таралған программалау тілдерінің бірі - Java қолданылады. Бағдарлама кодын тікелей жазудан басқа, экранның белгілі бір орындарына апарып, қолдар қосып, олардың өлшемдерін өзгертіп, түймелер мен Мәтін өрістері сияқты дайын нысандардан графикалық интерфейсті жинауға мүмкіндік беретін Eclipse және Android Studio даму ортасын пайдалануға болады. Бұл даму ортасы Android қолданбаларын тез және ыңғайлы жасауға, тестілеуге және реттеуге мүмкіндік береді.



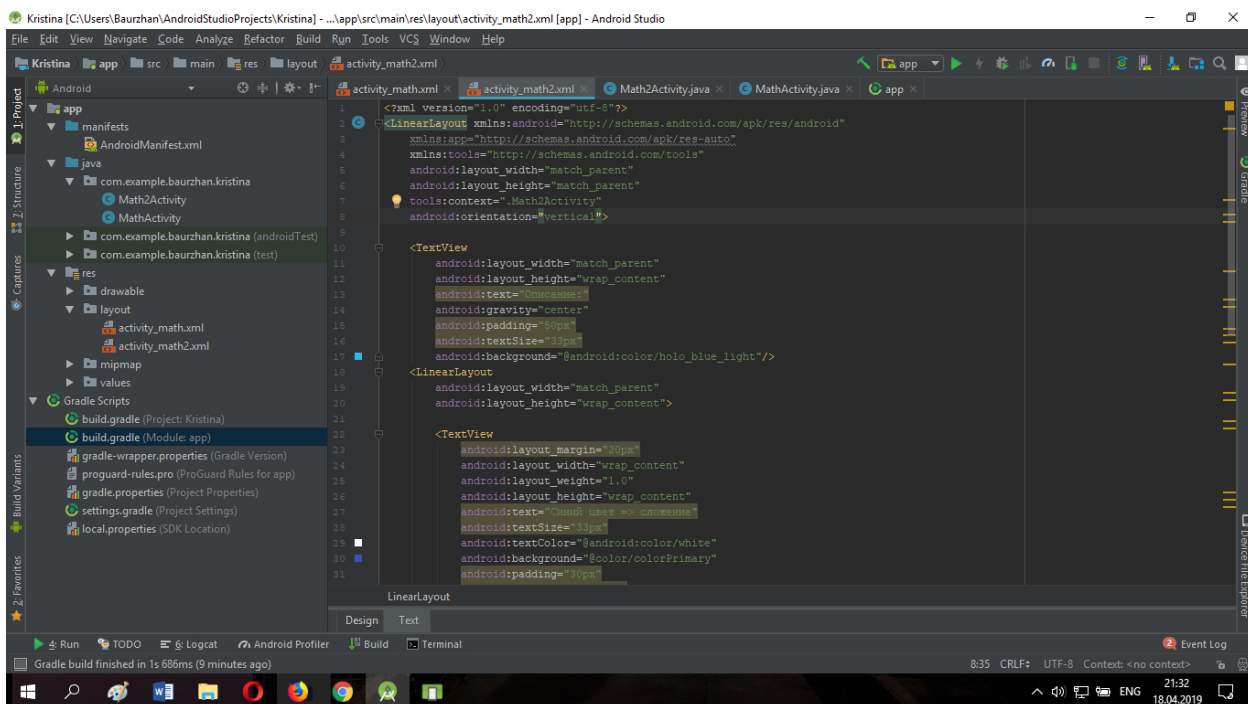
Сурет 32 - Android Studio-ны жүктеу

Әдепкі бойынша жасалатын Android ОЖ астында бағдарлама жобасының құрылымын қарастырамыз. Жоба түрлі модульдерді қамтуы мүмкін (Сурет 32). Барлық модульдер setting.gradle файлымен сипатталады. Егер біз жобаның құрылымына қарайтын болсақ, онда интерфейстің барлық мәнді коды - файлдары, java және т. б. кластары app папкасында болады. build.gradle файлы жоба құруда қажетті ақпаратты қамтиды, ол сол модульге тән жобаның конфигурациясын анықтайты.

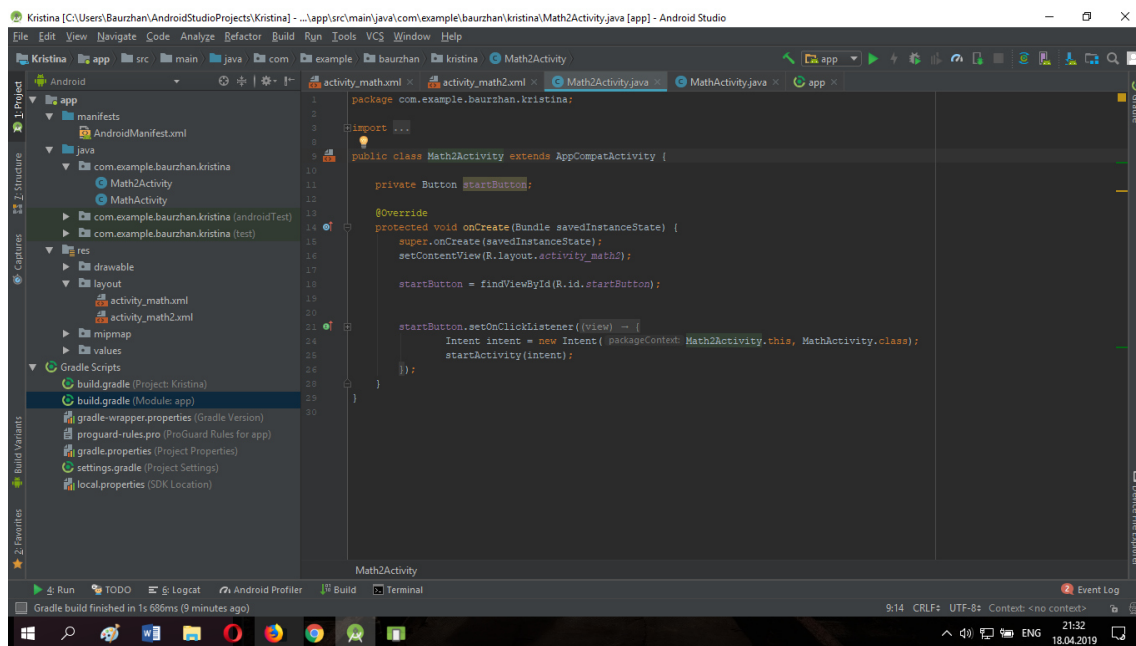


Сурет 33 – Структура Android жоба құрылымы

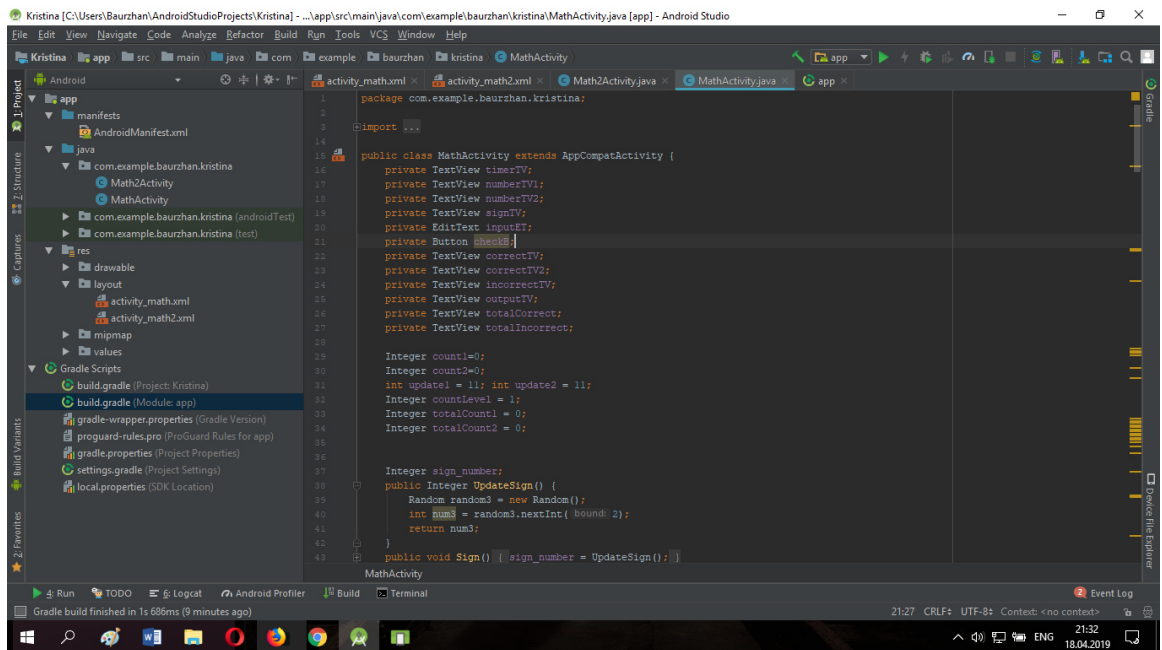
Енді қолданба үшін пайдаланушының графикалық интерфейсін жасаймыз (Сурет 33). Макеттік редактор (Layout Editor) пайдаланушының графикалық интерфейсін Button, TextView, ImageView және т. б. сияқты GUI құрауыштарын қолдану терезесіне апару арқылы жасауға мүмкіндік береді. Әдепкі бойынша Empty App үлгісі үшін макеттің сипаттамасы activity_main.xml атымен res / layout папкасындағы Xml файлда сақталады (Сурет 34, Сурет 35, Сурет 36, Сурет 37). Біз қолданба жасау үшін макеттік редактор және Component Tree терезесін қолданамыз. Activity_main.XML файлында XML белгілеу тек қолданбада қолданылатын TextView және ImageView компоненттерін орналастыру әдісін өзгерту үшін өңделеді. Android құрылғысының өлшемдері, мүмкіндіктері және пиксельдер тығыздықтары (DPI, Dot Per Inch) әртүрлі болғандықтан, әзірлеуші түрлі өлшемде көріністер ұсына алады, ал операциялық жүйе құрылғы пиксельдерінің тығыздығы негізінде графиканы таңдайтын болады. Осы себепті res папкасы drawable префиксінен басталатын бірнеше ішкі папкаларды қамтиды. DP немесе dp тығыздығына тәуелсіз пикселдер өлшемін орнату Android платформасына физикалық құрылғы экранының пикселдерінің тығыздығына байланысты пайдаланушының графикалық интерфейсін автоматты түрде масштабтауға мүмкіндік береді [20].



Сурет 34 – Интерфейс элементтерінің параметрлері мен мүмкіндіктерін қалыптастыру версткасы



Сурет 35 – Код 15. Фрагмент для отображения контента



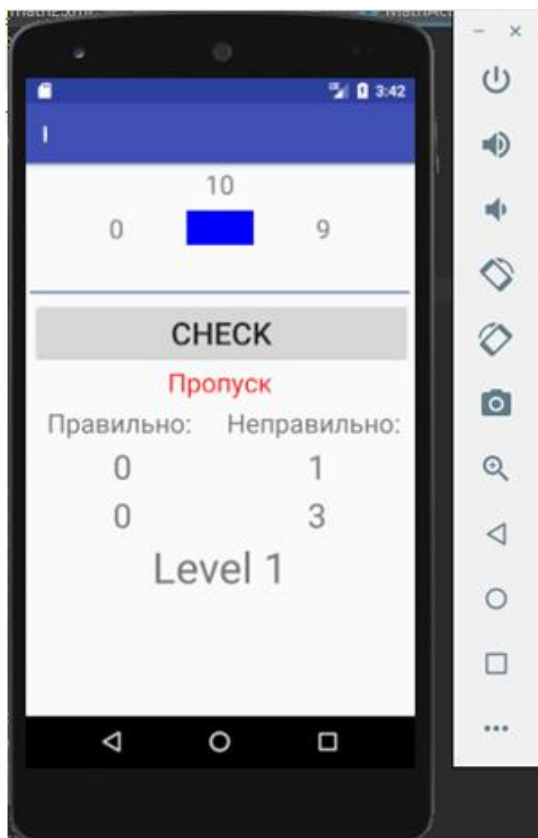
Сурет 36 – Интерфейс базалық класстарын анықтау



Сурет 37 – Қосымша интерфейсiнiң бастапқы қалыптары

Бiз қарапайым графикалық интерфейс кұрдық және қасиеттер терезесiнде компоненттердiң қасиеттерiн баптадық. XML таңбалау файлында әдепкi RelativeLayout компонентi LinearLayout компонентiмен ауыстырылды, содан кейiн көрiнiстердiң тiк орналасуы үшiн бапталған (Сурет 38). Қолданба мәтiндi TextView компонентiнде, ал кескiндердi ImageView компонентiнде шығарады. Мәтiн ортасында, үлкейтiлген қарiппен және стандартты

тақырыптағы түстердің бірінде туралануы үшін TextView графикалық интерфейсінің құрамдас бөлігі өзгертілді.



Сурет 38 – Қосымша интерфейсі

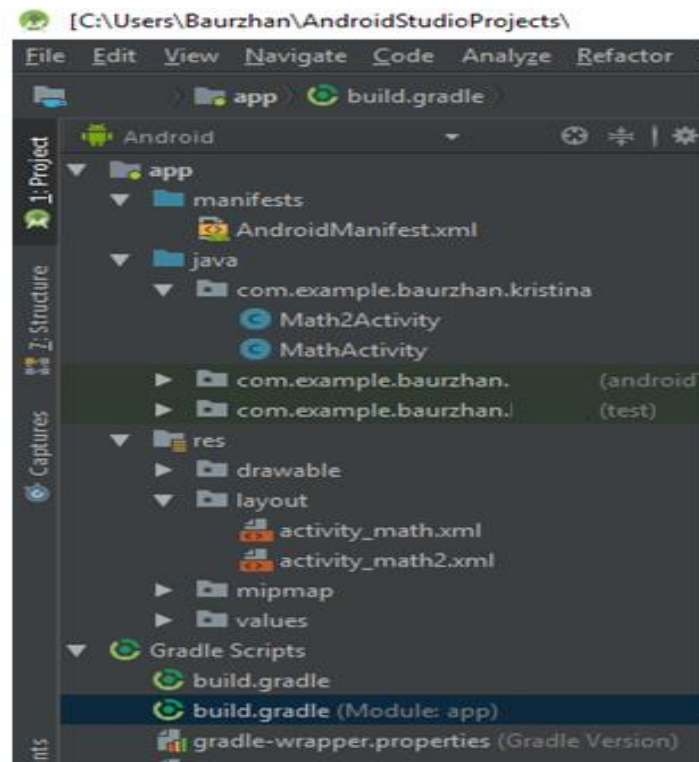
3.3 ProGuard-кодты бұрмалау процедурасы

ProGuard – бұл кодты қысқарту, оңтайландыру және жою құралы. Шығысында өлшемі аз, реинжинирлеу әлдеқайда қиын *.apk алынады.

Программа кодын реверстен қорғаудың үздік тәсілі – бұл обфускация, басқа сөзбен айтқанда – байт-кодты реверсер танымайтындай етіп шатастыру. Осы бағытта бірнеше құралдар бар, ол Android Studio құрамындағы тиімді құрал - ProGuard.

Құралды активтендіру үшін мына процедура орындалу керек (Сурет39):

```
android → buildTypes → release →  
→ build.gradle → minifyEnabled true:
```



Сурет 39 – ProGuard құралдарын активтендіру

```

buildTypes {
    release {
        minifyEnabled true
        proguardFiles getDefaultProguardFile('proguard-android.txt'), 'proguard-
rules.pro'
    }
}
}

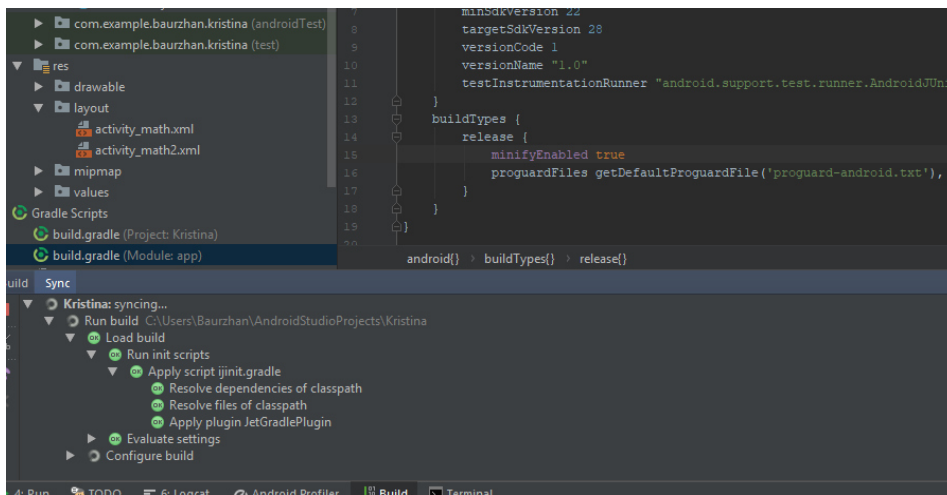
```

```

minSdkVersion 22
targetSdkVersion 28
versionCode 1
versionName "1.0"
testInstrumentationRunner "android.support.test.runner.AndroidJUnitRunner"
}
buildTypes {
    release {
        minifyEnabled false
        proguardFiles getDefaultProguardFile('proguard-android.txt'), 'proguard-rules.pro'
    }
}
}

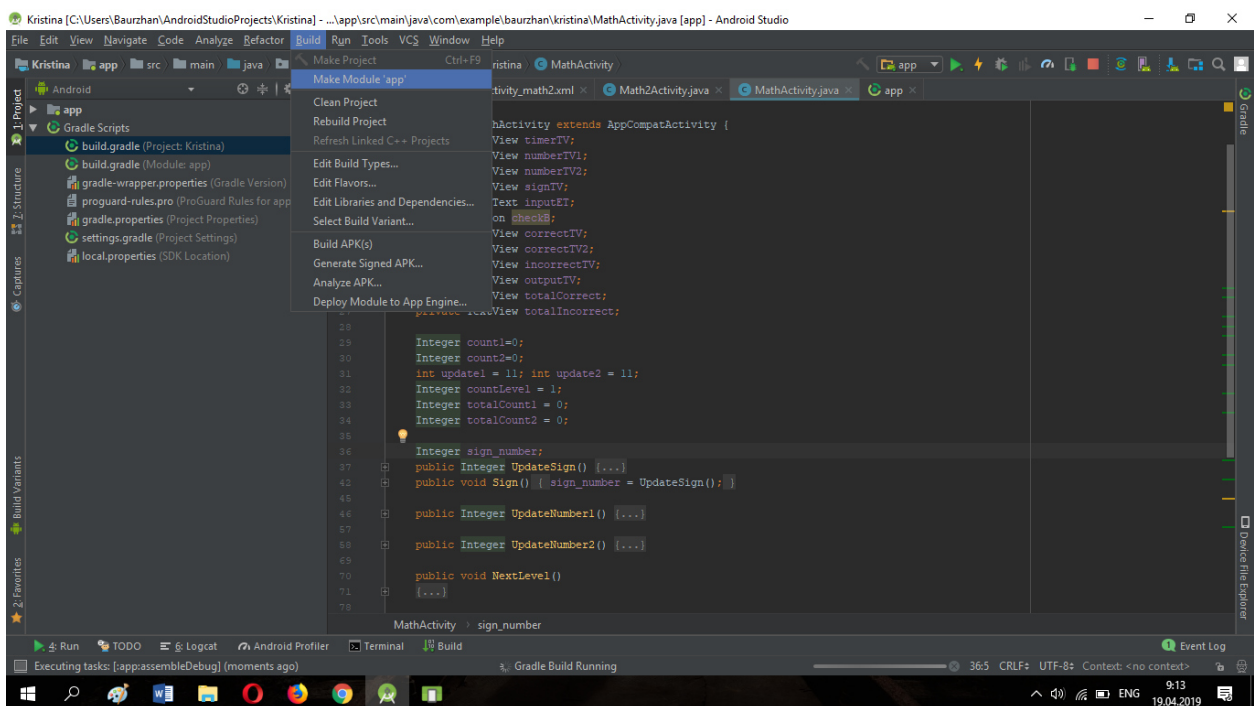
```

Сурет 40 – ProGuard функциясы қосылған программа үзіндісі

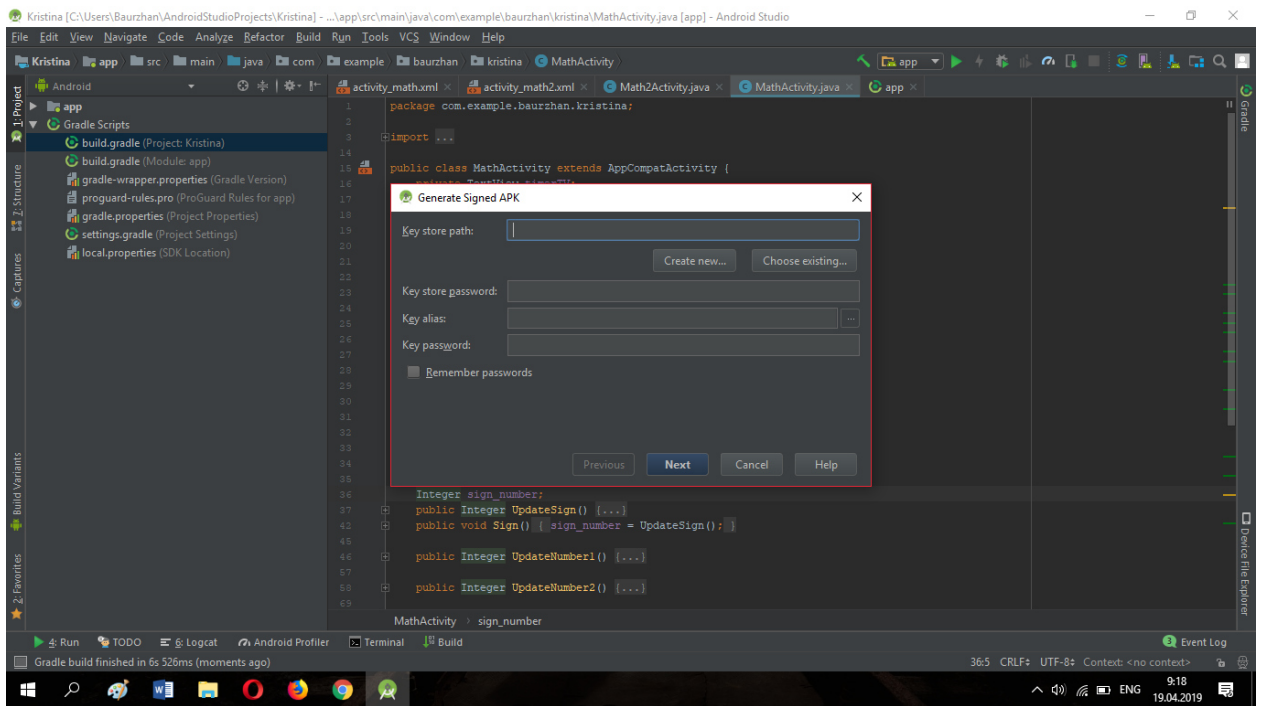


Сурет 41 – ProGuard функциясының ішкі мүмкіндіктері

Осыдан соң Android Studio барлық «релиздік» жинақты ProGuard арқылы өткізе бастайды. Нәтижесінде қосымша жинақы болады (қолданылмайтын кодты жоюдың арқасында), реверстен сонымен қатар қорғаудың кейбір деңгейлерін иемденетін болады (Сурет 42, Сурет 43, Сурет 44, Сурет 45).

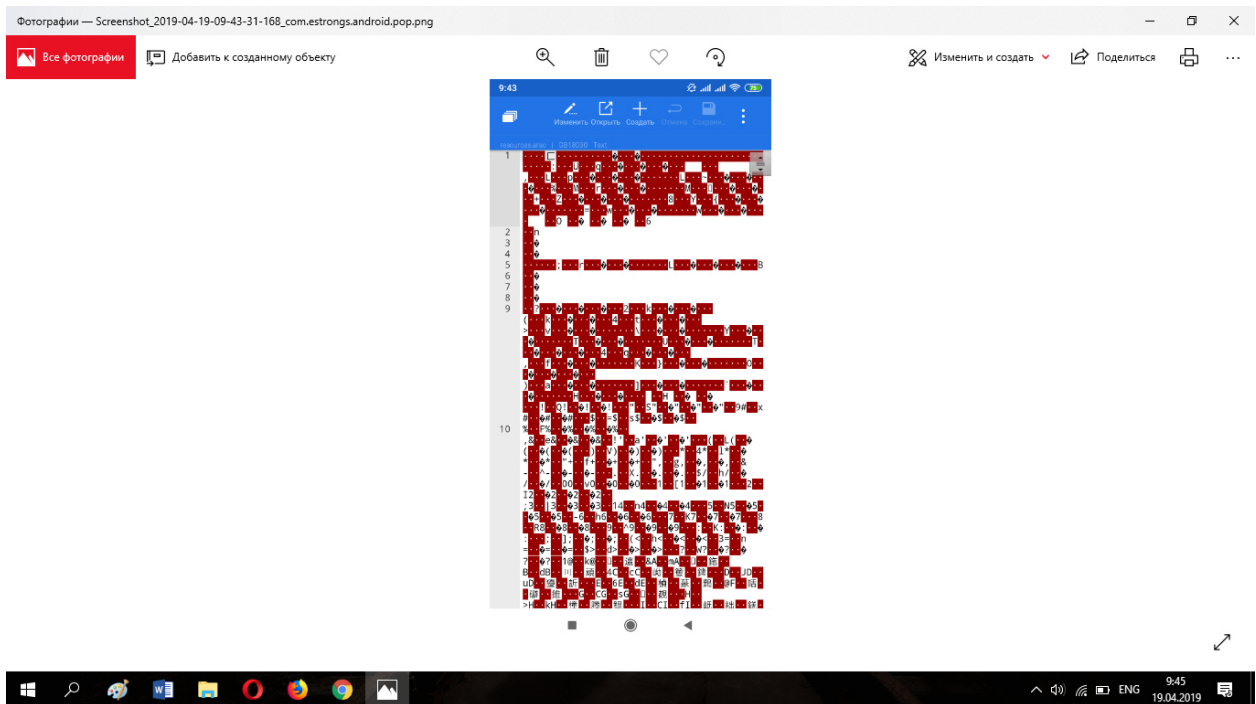


Сурет 42– App модулінің мүмкіндіктері

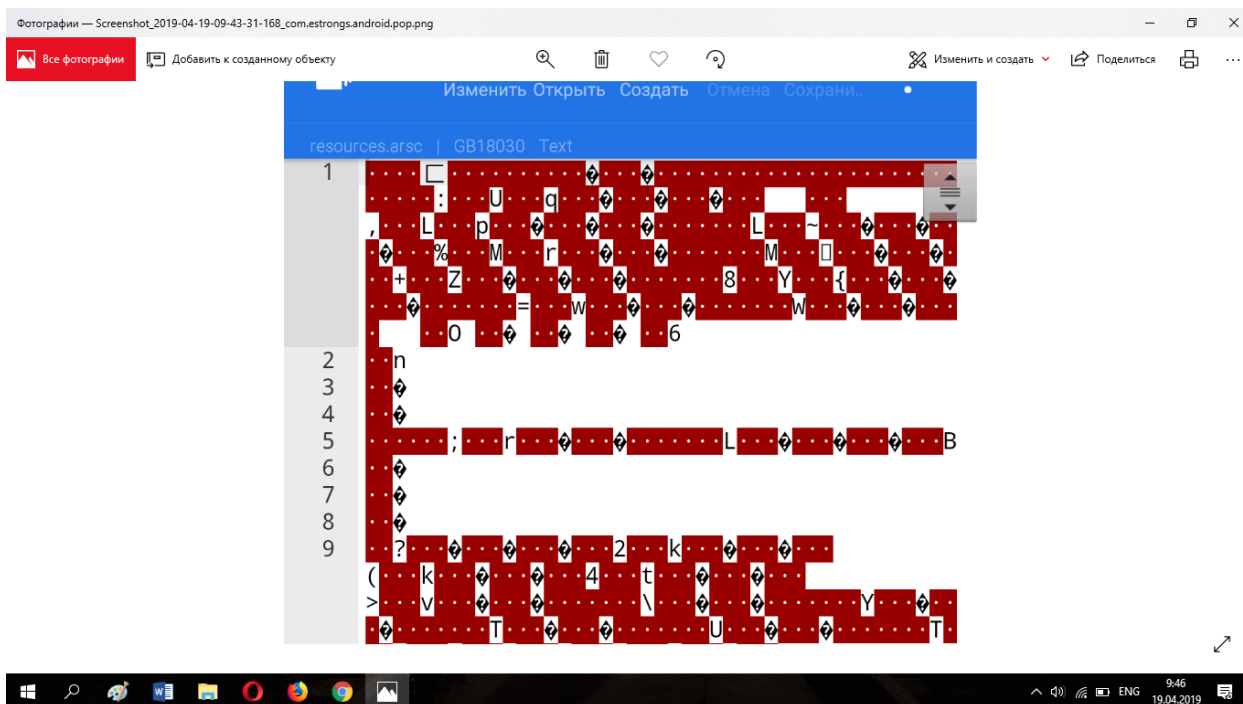


Сурет 43 – Жобаға қолтаңба қою

Осы суретке қарасак, pro-guard өзінің кодын құпияландырды.



Сурет 44 – Бұрмаланған программа коды



Сурет 45 – Бұрмаланған және көлемі ықшамдалған программа коды

3.4 Мобильді қосымшаны іске қосу

Қосымша құрылғаннан кейін және желіде орналастырылғаннан кейін ол туралы потенциалды тұтынушыларды хабардар ету керек. Қолданба басында көптеген қолданушылары бар "Play market" іздеу жүйелері арқылы беттерге түседі. Қолданба қандай да бір іздеу сұраулары бойынша шығуды бастау үшін, іздеу роботтары арқылы индекстеліп, олардың контент дерекқорларына енгізілуі тиіс. Іздеу арқылы бетті көтеру және сайтқа кіруді бірнеше жолмен арттыруға болады, атап айтқанда, тегін және ақылы, олардың әрқайсысының өз артықшылықтары мен кемшіліктері болады.

а) оңтайландыру – бұл қосымшаның оңтайлы атауы және қосымша сипаттамасында кілттік сөздердің болуы. Қосымшаның кең сұранысқа ие болуы оны көшіріп алу санына байланысты және қолданушылар арасындағы оның рейтингіне байланысты. Сонымен қатар қосымшаны заман талабына және қолданушылар талаптарына сәйкес жаңартып отыру, ескі версияларын түпкілікті жойып отыру да маңызды.

ә) басқа қосымшалардағы біріктірілген жарнама.

Ол үшін келесі әрекеттерді жасау қажет.

1) оларды орнатылған қосымшаларда әлеуетті клиенттермен байланыстыру

2) танымал қосымшаларда жарнаманы орналастыру.

3) мақсатты аудиторияны қызығушылық бойынша санаттандыру, олардың сұраныстарын пайдаланатын қосымшаларды таңдау;

4) баннерлерді енгізу. Мұндай мүмкіндіктерді Google AdWords кең ұсынады.

б) контент-маркетинг.

Талдау кейін мақсатты аудитория уақыт өткізетін ресурстар іріктелу керек, қосымшаларды жариялауға онда бірқатар қонақ бекеттерін таңдау қажет. Ол үшін талап етіледі:

- аудио-подкасттар жазу;
- бейнебаяндар құру;
- әлеуметтік желілерде белсенділік таныту.

Контент-маркетингі кешенді, ақылға қонымды және оның барлық механизмдерін: қонақ постинг, SMM, бейне-маркетинг енгізе отырып қолдану керек.

в) пікір көшбасшыларымен жұмыс.

Қосымшаны алға жылжыту кезінде сіздің мақсатты аудитория үшін пікір - бедел көшбасшысының көмегінсіз қиын болады. Миллионға дейін үйрену үшін миллиондаған адамдарды тыңдайтын бірнеше адамды анықтау керек.

Сізге өніміңізді ұнататындай етіп жасау керек.

5. Промо – сайт.

Ұялы қолданба үшін желіде ресми өкілдікті құру қажет. Бұл жеке промо-сайт, сондай-ақ басты сайт аясында отырғызылатын бет болуы мүмкін [21].

3.5 Интернет желісінде мобильді қосымшаны тарату жоспары

Басқару және талдау жүйелерінде тіркеу. Қосымшаларды маркеттерде орналастырғаннан кейін, "Play Market" - дегі қондырғылардың динамикасы 48-72 сағатқа толық жаңартылуын күту қажет. Бірақ қосымшаны жүктеу аз, бағдарламаны алға жылжыту қажет, ол үшін Яндекс және Google сияқты Рунеттегі негізгі іздеушілердің арнайы сервисін пайдалану қажет. AppMetrica қолданбасын индекстеу үшін Яндекс сервис деп аталады. Яндекс – бұл нақты уақытта аудиторияның көздері туралы ақпарат жинақтайтын, оның қосымшадағы сипаттамасын талдайтын және біздің пайдаланушыларымыз тап болатын қателерді тіркейтін тегін құрал.

Google – да бұл сервисің Яндекске ұқсас атауы бар – Google analytics. "Play Market" қосымшасы жүктелгеннен кейін сервис автоматты түрде орнатылады және статистиканы жүргізеді.

4 Техникалық және экономикалық негіздеме

4.1 Жобаның сипаттамасы

Бұл дипломдық жобаның мақсаты Android studio қорғалған мобильді қосымшасын әзірлеу болып табылады.

Әзірленген бағдарламалық модуль смартфон ресурстарын мониторингілеуге арналған мобильді қосымша болып табылады.

Мобильді қосымша:

– смартфон процессорына жүктемені және оның жұмыс жиілігін, смартфонның ОЗУ (барлық ОЗУ/пайдаланылған/еркін) және оның жадына (жалпы көлемі/пайдаланылған/еркін) мониторинг жүргізу);

– батареяны бәсеңдету уақытын болжауды және смартфон батареялары бойынша статистиканы жүргізуді жүзеге асыру (разрядтау жылдамдығы / сағатына разрядтау қарқыны/зарядтау жылдамдығы/толық зарядталғанға дейінгі уақыт / толық разрядталғанға дейінгі уақыт);

– смартфон ресурстарын тұтыну бойынша топ қосымшаларды ұсыну;

– ресурстар жұмысы бойынша файлдардың логын ұсыну;

– смартфонның жалпы температурасын бақылауды қамтамасыз ету.

Бағдарламалық модульді әзірлеу Java бағдарламалау ортасында жүзеге асырылды.

Әзірленген Мобильді қосымша негізінен телефондарды жөндеумен айналысатын ұйымдарға арналған, қосымша арқылы алынған деректер олардың қызметін жүзеге асыру үшін қажет болып табылады.

Бұл мобильді қосымшаны смартфонның ішінде не болып жатқанын, оның жасырын мүмкіндіктері туралы ақпаратқа мүдделі смартфондардың иелері де пайдалана алады.

Өңделетін бағдарламалық модуль қолданыстағы аналогтармен салыстырғанда келесі артықшылықтарға ие:

– ыңғайлы және ақпараттық интерфейс;

– нақты уақытта ақпаратты көрсету;

– файлдардың логын жүргізу және оларды шығару мүмкіндігі;

– виджеттердің болуы;

– қосымшаның өзінде ресурстарды аз тұтынуы;

– төмен баға.

Нарықта бағдарламалық модульді жүзеге асыру Google Play Market арқылы екі нұсқада жоспарланады:

1-нұсқа-бағасы 1000,00 тенге ;

2-нұсқасы, онда ақылы жарнама болады – ТЕГІН.

Менің жұмысымда әзірлеу мен енгізудің техникалық-экономикалық негіздемесі мыналарды қамтиды:

- бағдарламаны әзірлеудің еңбек сыйымдылығын анықтау;

- бағдарламаны әзірлеуге арналған шығындарды есептеу;

- әзірленген бағдарламаның ықтимал бағасын анықтау;

- қызмет етудің әлеуметтік-экономикалық нәтижелерін бағалау.

4.2 Еңбек сыйымдылығы

Кесте 6 – Еңбек сыйымдылығының қорытынды көрсеткіштері

Әзірмелеу кезеңі	Осы кезеңдегі жұмыс түрі	Еңбек сыйымдылығы ,адам сағ.
1	Міндеттер қою	13
2	техникалық тапсырманы әзірлеу және бекіту	12
3	Қолданыстағы әдістермен танысу	14
4	Әдебиетті таңдау және зерттеу	23
5	Кешенді қорғауды әзірлеудің әртүрлі әдістеріне талдау жүргізу	17
6	Тестілеу	15
7	Бағдарламалық жобаның теориялық бөлігін рәсімдеу	19
8	Бағдарламалық жобаның эксперименттік бөлігін әзірлеу	33
9	Әзірлеу ортасын таңдау	12
10	Математикалық есептеулерді әзірлеу және бағдарламалық қамтамасыз етуді жазу	16
11	Жобаны іске асыру	50
12	Қолданбаны баптау	18
13	Есепті рәсімдеу және атқарылған жұмыс туралы қорытынды жасау	14
Қорытынды	жобалық жұмысты орындаудың еңбек сыйымдылығы	256

$\frac{256}{8} = 32$, жұмыс күнінің ұзақтығы 8 сағатқа тең. Нәтижесінде бағдарламалық қамтамасыз етуді іске асыру үшін 32 жұмыс күні қажет, 6 – кестеде көрсетілген.

4.3 Әзірлеуге арналған шығындарды есептеу

Өзіндік құнды есептеу ТҚ әзірлеу кезінде жұмсалған шығыстар бойынша жүргізіледі. Бұл ӨҚ әзірлеушілері орындайтын барлық жұмыстарға арналған бір реттік шығындар.

Шығындар өзіндік құн калькуляциясының баптарын қосу жолымен анықталады:

- материалдар;
- ғылыми және тәжірибелік жұмыстарға арналған арнайы жабдықтар;

- еңбекақы;
- еңбекақы төлеу қорына есептеу;
- басқа да тікелей шығындар;
- үстеме шығыстар.

Материалдық шығындарды есептеу 7-кестеде берілген нысан бойынша жүргізіледі.

Кесте 7 – материалдық ресурстарға шығындар

Материалдың атауы	Өлшем бірлігі	Саны	1 дананың бағасы, тг	Қорытынды бағасы
Парақтарға арналған қағаз	бума	4	1 200	4800,00
Дәптер (80 бет)	Дана	2	150	300,00
Қаламдар	Дана	2	135	270,00
Компьютерлік тышқан	Дана	1	4000	4000,00
Қорытынды:				9370,00

Материалдық құралдарға (Z_m) қажетті жалпы соманы мынадай формула бойынша есептеуге болады:

$$Z_m = \sum P_i * C_i, \quad (4.1)$$

Мұндағы, P_i - материалдық ресурстың i түрінің шығысы, заттай бірліктер;

C_i - материалдық ресурстың i түрінің бірлігінің бағасы, тг;

i - материалдық ресурстың түрі;

n - материалдық ресурстар түрлерінің саны.

Бағдарламалық жасақтаманы әзірлеу үшін ASUS – BV381T Gray ноутбугі қолданылады. Бағдарламалық өнімді тестілеу үшін орнатылған операциялық жүйесі бар ДК қажет болады. Windows 7/8/10 нұсқалары. Ноутбукке сым арқылы қосылу үшін смартфон қажет.

Қажетті жабдықтар мен бағдарламалық қамтамасыз ету шығындарын есептеу 8 – кестеде келтірілген нысан бойынша жүргізіледі.

Кесте 8 – жоба үшін қажетті жабдық пен БЖ шығындарын есептеу.

Материалдық ресурстың атауы	Өлшем бірлігі	Саны	1 дананың бағасы, тг	Қорытынды бағасы, тг
Жеке компьютер Операциялық жүйе MS Windows 7	Дана	1	130 000	130 000,00
Ноутбук ASUS -BV381T Gray	Дана	1	340 000	340 000,00
Процессор PH-5543, A(M)/microB(M)	Дана	2	50 000	100 000,00
Смартфон (HUAWEI P smart 20)	Дана	1	160 000	160 000,00
Қорытынды				730 000,00

$$З_m = 730\ 000 + 9370 = 739\ 370,00$$

Осы кестеге сәйкес жобаға материалдық шығындар 739 370,00 теңгені құрайды.

Электр энергиясын тұтынбай-ақ, бағдарламалық қамтамасыз етуді әзірлеу кезінде электр энергиясына жұмсалатын шығындарды есептеу мәні бар.

Жұмыс уақыты әр түрлі, сондықтан әрбір қызметкердің сағаттық ставкасын және жалпы жалақы көлемін белгілеу мағынасы бар.

8-кестеге сәйкес программист үшін бағдарламалық қамтамасыз етуді әзірлеу үшін 256 сағат, ал басшыға 120 сағат қажет. Енді 256 сағат ішінде жұмсалатын электр энергиясының құнын есептеу қажет.

$$\mathcal{E} = \mathcal{I}_{\text{электр энергиясына жабдықтар}} + \mathcal{I}_{\text{қосымша қажеттілік}} \quad (4.2)$$

Мұндағы, $\mathcal{I}_{\text{электр энергиясы жабдықтар}}$ – жабдықтың электр энергиясына арналған шығындары;

$\mathcal{I}_{\text{қосымша қажеттілік}}$ – қосымша қажеттіліктерге арналған электр энергиясының шығындары.

Жабдық үшін қажетті электр энергиясын есептеу мынадай формула бойынша анықталады:

$$\text{Ш}_{\text{электр энергиясына жабдықтар}} = \sum W * K_1 * S * T, \quad (4.3)$$

Мұндағы, W – тұтынылатын қуат, Вт;

K_1 – пайдалану коэффициенті ($K_1 = 0,7..0,9$);

Кесте 9 – электр энергиясына шығындар

Аспаптардың атауы	Қуаты, кВт	Қуат коэффициенті	Жабдықтың жұмыс уақыты, сағ.	ЭЭ бағасы, тг/кВ	Сомасы, тг
Ноутбук	0,5	0,7	256	23,85	2136,96
Жұмыс станциясы	0,4	0,9	256	23,85	2198,02
Смартфон	0,5	0,9	15	23,85	160,99
Жеке компьютер	0,9	0,9	140	23,85	2704,59
Жарықтандыру	0,35	0,7	256	23,85	1495,87
Қорытынды:					8696,00

$$\text{Ш}_{\text{электр энергиясына жабдықтар}} = 8696,00(\text{тенге})$$

Қосымша қажеттіліктерге шығыстар электр энергиясына арналған шығыстардың 5% көлемінде жоғары көрсеткіш негізінде есептеледі:

$$\text{Ш}_{\text{қосымша қажеттілік}} = 5\% * \text{Ш}_{\text{электр энергиясына жабдықтар}}, \quad (4.4)$$

(4.4) формулаға сәйкес қосымша қажеттіліктерге жұмсалатын шығындарды анықтаймыз:

$$\text{Ш}_{\text{қосымша қажеттілік}} = 0.05 * 8696 = 434,80(\text{тенге})$$

Барлық есептеулерге сүйене отырып, электр энергиясына толық шығындар құрайды:

$$\text{Э} = 434,8 + 8696 = 9130,80 (\text{тенге})$$

4.4 Еңбекақы төлеу шығындарын есептеу

Бағдарламалық қамтамасыз етуді әзірлеу үшін бұрын көрсетілгендей, екі қызметкер қажет.:

– жоба жетекшісі-жұмыс уақытын басқару, жұмыс процестерін түзету, үйлестіру, пәндік облысты зерттеу;

– программист-әзірлеуші-БҚ әзірлеу, тестілеу және сүйемелдеу.

Еңбекақы төлеу шығындарының сомасын келесі формула бойынша

есептеуге болады:

$$\text{Ш}_{\text{еңбекақы}} = \sum \text{ЧС}_i * T_i \quad (4.5)$$

Мұндағы, ЧС_i - i -ші қызметкердің сағаттық мөлшерлемесі, тг;
 T_i - модельді әзірлеудің еңбек сыйымдылығы, адам×сағ; i - қызметкердің санаты;

n – ПҚ әзірлеумен айналысатын қызметкерлердің саны.

Қызметкерінің сағаттық мөлшерлемесін есептеуге болады мынадай формула бойынша:

$$\text{ЧС}_i = \frac{3\Pi_i}{\text{ФРВ}_i} \quad (4.6)$$

мұнда, $3\Pi_i$ - i -ші қызметкердің 1 айдағы еңбекақысы, тг;

ФРВ_i - i -ші қызметкердің жұмыс уақытының айлық қоры, сағ.

Басшының айлық жалақысы 190 000 теңгеге тең және әзірлеушінің айлық жалақысы 140 000 теңгеге тең. Әр қызметкердің сағаттық мөлшерлемесін формулаға сәйкес есептейміз (4.6):

$$\text{ЧС}_{\text{басшы}} = \frac{190\,000}{22 * 8} = 1\,079,54 \text{ тг/ч}$$

$$\text{ЧС}_{\text{әзірлеуші}} = \frac{140\,000}{22 * 8} = 795,45 \text{ тг/ч}$$

Басшының сағаттық мөлшерлемесі 1 079,54 (тг/сағ) құрайды, еңбек сыйымдылығы 120 сағатқа тең. Әзірлеушінің сағаттық мөлшерлемесі 795,45 (тг/сағ), әзірлеудің еңбек сыйымдылығы 256 сағатқа тең. (4.5) формулаға сәйкес қызметкерлердің еңбекақысына арналған шығындар сомасын есептеуге болады:

$$\text{Ш}_{\text{еңбекақы}} = 1\,079,54 * 120 + 795,45 * 256 = 333\,635,00$$

Еңбек ақы төлеу бойынша шығындарды есептеу 10-кестеде көрсетілген.

Кесте 10 – Жалақыны есептеу

Қызметкердің санаты	Квалификациясы	Еңбек сыйымдылығы, сағ.	Сағ.мөлшерлемесі, тг/сағ.	Бағасы, тг.
Басшы	Инженер – жобалаушы	120	1 079,54	130 000,00
Әзірлеуші	Программист	256	795,45	203 635,00
Қорытынды:				333 635,00

4.5 Әлеуметтік салық бойынша шығындарды есептеу

Қазақстан Республикасының Салық кодексіне сәйкес әлеуметтік салық еңбекақы төлеу қорының 9,5% - ын құрайды. Әлеуметтік салықты келесі формула бойынша есептеуге болады:

Еңбекақы төлеу қоры – ЕТҚ;
Зейнетақы аударымдары – ЗА.

$$C_H = (ЕТҚ - ЗА) * 0,095 \quad (4.7)$$

бұл жерде зейнетақы қорына аударымдар ЕТҚ-дан 10% құрайды.

$$ЗА = 333\ 635 * 0,1 = 33\ 363,50 \text{ тенге}$$
$$C_H = (333\ 635 - 33\ 363,5) * 0,095 = 28\ 525,80 \text{ тенге}$$

Есептеу нәтижелері 11-кестеде берілген:

Кесте 11 – әлеуметтік салықты есептеу

Қызметкердің санаты	Адам саны	Еңбекақы, тг	Пенсиондық аударымдар, тг	Әлеуметтік салық, тг
Басшы	1	130 000	13 000	11 115,00
Әзірлеуші	1	203 635	20 363,5	17 410,80
Қорытынды:				28 525,80

4.6 Негізгі қорлардың амортизациясы және өзге де шығындар

Амортизация нормалары ҚҚ анықтау қажет салық кодексіне сәйкес. ОФ амортизациясын келесі формула бойынша анықтауға болады:

$$A_r = \frac{K_{\text{жкк}} * H_a}{100} \quad (4.8)$$

мұндағы, $K_{\text{жкк}}$ – жабдықтың құны;

H_a – амортизация нормасы (амортизация нормасы = 25);

Формула (4.8) ноутбук үшін бір жыл ішінде амортизациялық аударымдар үшін қажетті соманы есептеуге мүмкіндік береді:

$$A_r = \frac{340\ 000 * 25}{100} = 85\ 000 \text{ тенге}$$

Енді әзірлеу кезеңі үшін амортизация нормасын есептеу қажет:

$$A_r = \frac{85\ 000 * 32}{365} = 7452,05 \text{ тенге}$$

Осылайша, барлық жабдық үшін амортизация нормасын есептеу қажет. Есептеу нәтижелері 12-кестеде келтірілген.

Кесте 12 – ОФ амортизациясы

Жабдық және БЖ атауы	Жабдықта р мен БЖ құны, тг	Жылдық амортизация нормасы, %	Жыл ішіндегі амортизация сомасы, тг	Әзірлеу кезіндегі амортизация сомасы, тг
Ноутбук	340 000	25	85 000	7452,05
Смартфон	160 000	15	24 000	2104,11
Жеке компьютер	130 000	20	26 000	2279,45
Қорытынды:			135 000	11835,61

БЖ әзірлеуге арналған шығыстар сметасы.

Барлық берілген есеп – қисаптардың негізінде 13-кестеде келтірілген нысан бойынша әзірлеуге арналған шығыстар сметасын ресімдеу қажет.

Кесте 13 – шығындар Сметасы әзірлеу бойынша

Шығындар	Құны, тг
Жабдыққа арналған шығындар	730 000,00
Электр энергиясына арналған шығындар	8 696 ,00
Еңбекақы төлеу шығындары	333 635,00
Әлеуметтік салықтар	28 525,80
Негізгі қорлардың амортизациясы	11835,61
Материалдық ресурс шығындары	9370,00
Смета бойынша қорытындысы:	1 122 062

4.7 Ықтимал (шарттық) бағасын анықтау

Бағдарламалық қамтамасыз етудің құны әзірленген өнімнің сапасы, оны әзірлеу мерзімі және өнімнің өнімділігі негізінде анықталады. Бағдарламалық қамтамасыз ету үшін Ц_д құнын мына формула бойынша есептеуге болады:

$$Ц_d = Z_{\text{Бағ}} (1+P/100), \quad (4.9)$$

мұнда, $Z_{\text{Бағд}}$ – бағдарламалық қамтамасыз етуді әзірлеуге арналған шығындар, тг;

P – БЖ рентабельділігінің орташа деңгейі, (%). Бұл параметр 25% тең.

$$Ц_d = 1\,122\,062 + 1\,122\,062 * 0,25 = 1\,122\,062 + 280516 = 1\,402\,578 \text{ тенге.}$$

Бұдан әрі қосылған құн салығын (НДС) есепке ала отырып, өткізу құнын

анықтау қажет, НДС ставкасы ҚР заңнамалық Салық кодексімен белгіленеді. 2019 жылға НДС ставкасы 12% мөлшерінде белгіленген.

Іске асыру құны НДС -ты ескере отырып есептеуге болады мынадай формула бойынша:

$$C_p = C_d + C_d * \text{НДС}, \quad (4.10)$$

$$C_p = 1\,402\,578 + 1\,402\,578 * 0,12 = 1\,683\,094 \text{ тенге}$$

Бұл бағаны 1 684 000 теңгеге дейін дөңгелектеуге болады.

4.8 ПҚ жұмыс істеуінің әлеуметтік-экономикалық нәтижелерін бағалау

Бұл жобаның экономикалық мақсаттылығы сандық және сапалы құрамдастардан құралатын болады. Әзірлеушілер үшін экономикалық тиімділік жеке әзірлеушілер мен жобаны іске асырумен айналысатын кәсіпорындардың қаржылық жағдайын жақсартудан тұрады. Осы жобаны сәтті іске асыру кезінде: әзірлеушілер тікелей еңбекақы алады, ол 203 635 теңгені құрайды. Әзірлеушілер үшін сапалы тиімділік-бұл жобаны нарыққа шығарудың алғашқы тәжірибесі, онда әзірлеуші одан әрі жобалау мәселелерін шешеді, жобаның тиімділігі, одан әрі жұмыс негіздерін жобалау. Сондай-ақ жобаны іске асыру барысында Маркетинг, жарнама, бағдарламалық қамтамасыз ету нарығын игеру мәселелері шешілетін болады. Осы Жобаның өзіндік құны 1 122 062,00 теңгені құрады, пайдалы баға 280516,00 құрайды. Осы жобаның ықтимал бағасы 1 684 000,00.

5 Өмір тіршілік қауіпсіздігі

5.1 Мобильді телефонның зиянды факторлары

Ұялы телефонның зиянын өте маңызды ұйымдар зерттейді. Мәселен, АҚШ Ұлттық онкология институтының анықтаған үш негізгі себебі бар, олар ұялы телефоннан қауіптену керек екенін айтады.

1) әрбір жұмыс істеп тұрған құрылғыдан радио жиілік сәулесі шығады, ол өзінің табиғаты бойынша кез келген тірі ағзаға зиянды әсер етеді;

2) пайдаланушылар саны өсіп, үлкен электромагниттік фонды көбейтіп және әрбір адамға әсер етеді;

3) байланыстың қолжетімділігі артуда, соның салдарынан қоңыраулардың саны мен ұзақтығы артуда.

Смартфондарды жетілдіру адамдарды көбінесе оларды пайдалануға ынталандырады, бұл ағзаға көп жүктеме береді. Дегенмен, ғалымдардың көпшілігі ұялы телефонды жиі пайдалану Обыр әкеледі деп күмәнді деп санайды. Шынында да, сөйлесу барысында, құрылғы құлаққа қысылған кезде, сәулелену телефонға жақын маталар қызып кетеді.

Бірақ осындай температура мен обыр арасында тікелей тәуелділік табылған жоқ. Егер адам гарнитураны пайдаланса немесе қатты сөйлессе, онда сәулелену оған әсер етпейді.

Дегенмен, телефондар ғана емес, басқа да факторлар бар:

1) Микробтар

"Ұялы телефонды" әрбір қолданар алдында және одан кейін қолдарын жуатын адамдар жоқ. Осыған байланысты телефондарда көптеген микробтар мен тіпті ішек таяқшалары болады. Сондықтан қолды таза матамен немесе майлықпен сүртіп, телефонды таза ұстау керек.

2) Жазатайым оқиғалар

Статистикаға сәйкес, АҚШ-тағы жолдарда ғана күн сайын 10-ға жуық адам көз жұмып, 1000-нан астам түрлі ауыр жарақат алады. Телефон арқылы хат алмасу және сөйлесу – бұл қайғының басты себебі. Телефонға көңіл бөле отырып, жүргізушілер рульде шоғырлануын жоғалтады, бұл ауыр зардаптарға әкеп соғады.

3) Көздің шаршауы

Ұялы телефонның әрбір белсенді пайдаланушысы көзге жүктемені сезінеді. Ұйықыны құрбан етуге дайын балалар мен жасөспірімдер туралы не айтуға болады?

Жарқын жарық тез көзді сындырады. Экрандағы бейнелерді көруге бейімдеу үшін, көз бұлшық еттерін іске қосамыз. Бұл жағдайда көз шаршайды және белгілі бір ауруға әкеліп соғады. Сонымен қатар, смартфон ұйқының сапасына өте нашар әсер етеді, бұл денсаулыққа қатысты бірқатар басқа да мәселелерді тудырады. Ал төсектің жанында телефонды зарядтау ақымақ әдет, ол тек жалпы зиянды күшейтеді. Ұзақ уақыт аралығында сәулелену аймағында болған адамдарда келесідей белгілер байқалады:

1) Әлсіздік;

- 2) Ашуланғыштық;
- 3) Тез шаршау;
- 4) Есте сақтау қабілетінің төмендеуі;
- 5) Ұйқының бұзылуы;
- 6) Жүйке жүйесінің вегетативті қызметінің бұзылуы;
- 7) Гипотония;
- 8) Жүректің ауруы;
- 9) Тамыр соғысының бұзылуы;
- 10) Мазасыздану;
- 11) Есте сақтауы және зейін қоюы бұзылады.



Сурет 46 – Мидың белгілі бір градусқа дейін жылуы

Радиожилік сигналдарының тұрақты әрекеті адам денсаулығына теріс әсер етуі мүмкін. Көптеген адамдар ұялы байланыстан түрлі кемшіліктерге шағымданады: тұрақты бас ауруы, жадымен проблемалар, құлақтың ауыруы және шаршау [22].

Ұялы телефонды ұзақ пайдалану адамның миын белгілі бір градусқа дейін жылытуы мүмкін (Сурет 46). Wi Fi деректер беру технологиялары ми қыртысына теріс әсер етуі мүмкін, яғни Конституцияда бұл мәселе бойынша ешқандай заң жоқ, салдары белгісіз. Әрбір пәтерде микротолқынды пеш бар, бірақ ол қалай жұмыс істейтінін біледі. Электромагниттік сәуле шағын бөліктерді қозғайды - атомдар және өнімдер қызады. Ыдыс суық болып қалғанына карамастан. Электромагниттік сәуле біздің маталарды жылытады. Адамның жасушалары бұл процеске ауыр. Бірақ бұл қаншалықты зиянды екенін ешкім түсінбейді. Енді телефондар 1800 МГц және 1905 МГц жиіліктерінде жұмыс істей алады.

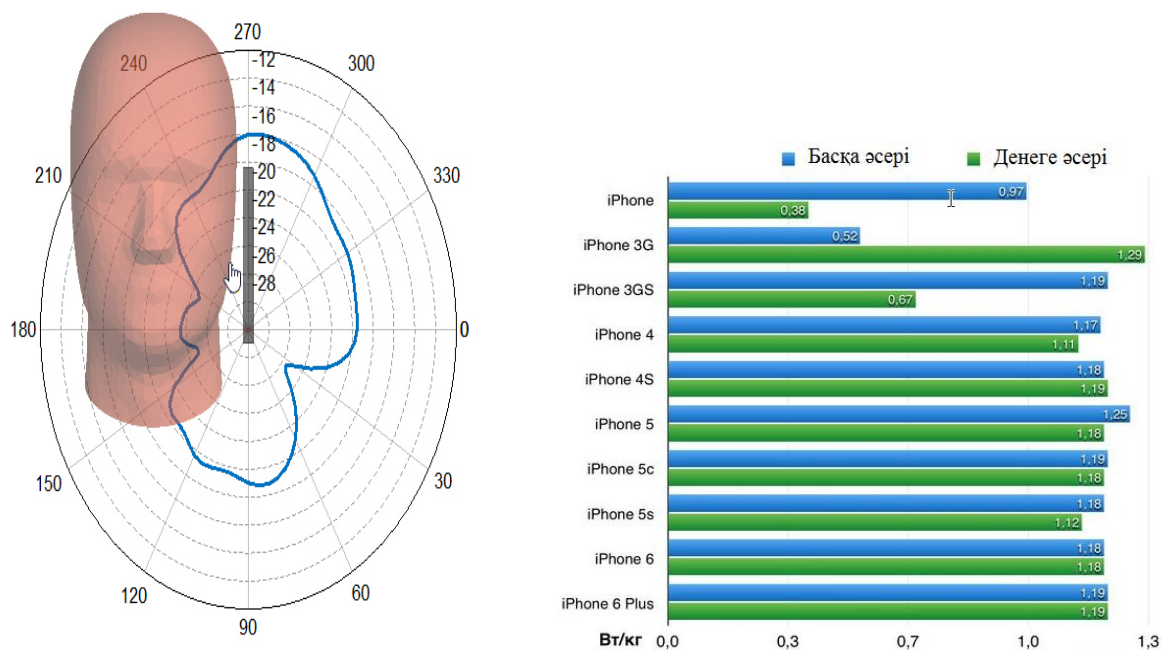
Бұл жерде телефондарға салынған антенналардың сәуле шығарғыштарының зияны туралы сөз болып отыр. Онда ештеңе зиян келтірмейді, материалдар да (пластик, шыны және т.б.) және басқа да бөліктер.

Ғалымдар жүргізген зерттеулерден адамдардың 3%-ы "гиперэлектроқұрылымдылықтан" зардап шегетіні анық болды, яғни, бұл адамдардың ағзасы электромагниттік өрістерге өте сезімтал. Ұялы телефондардан түрлі ауруларды ғалымдар байқап, жүрек-қан тамырлары ауруларын, балалар лейкемиясын жүйке жүйесінің бұзылуы деп айтты. Қазіргі уақытта әлемде екі миллиардтан астам адам мобильді пайдаланушылар болып табылады, олардың бес жүз миллионнан астамы GSM телефондарын пайдаланады. Ғалымдар аналогтық телефондар сандық телефондарға қарағанда адамға әлдеқайда зиянды деп санайды. Қазіргі ұялы байланыс жұмыс істейтін өрістердің радиожілік диапазоны 450 МГц-ден 1,9 ГГц-ке дейінгі шектерде орналасқан.

Адам ағзасына теріс әсер ететін электромагниттік сәулеленуден басқа, телефоннан тағы бір қауіп бар – оның корпусында аллергиялық типтегі реакциялар мен қауіпті ауруларды тудыруы, қауіпті микроорганизмдердің таралуы. Әрине, бактериялар мен вирустардан аппаратты тазалауға болады, бірақ бәрі мұны қалай дұрыс жасауды білмейді. Бұл жағдайда бензин, спирт немесе дымқыл майлықтар. Ультракүлгін жарық-жалғыз нәрсе көмектесе алады. Қоңырау шалу кезінде телефон мен бас терісінің арасындағы қашықтық кемінде 3 сантиметр болуы тиіс, ал осы қашықтық барынша сәулеленуі тиіс. Құлаққапты пайдаланса, сәулеленудің өсуіне жол бермеу үшін Bluetooth әсері аз болады, GPRS технологиясы бойынша деректерді тасымалдау құралы ретінде мобильді телефонды пайдаланбауға тырысу керек.

Жұтудың меншікті коэффициенті (ағылш. Specific Absorption Rate-SAR) электромагнитті энергия – бір секунд ішінде адам денесінің тіндерінде сіңетін электромагнитті өрістің энергиясын анықтайтын көрсеткіш. Еуропада сәулеленудің рұқсат етілген мәні 10 грамм мата үшін 2 Вт/кг құрайды. АҚШ-та басқа өлшеу жүйесі қолданылады-Федералдық байланыс агенттігі 1 грамм мата үшін мск 1,6 Вт/кг аспайтын ұялы аппараттарды ғана сертификаттайды. Ресейде сәулеленетін қуатты өлшеу жүйесі – шаршы сантиметрге ваттпен.

iPhone 6 (a 1586) және iPhone 6 Plus (A1524) ішінде SAR деңгейі 1,18 және 1,19 Вт/кг деңгейінде, тиісінше, бас пен дене үшін бірдей, 47-суретте көрсетілген. Осылайша, Apple компаниясы стандартты шектеулердің жоғарғы планкасына сәулеленуді келтіріп, байланыс өнімділігі мен сапасына назар аударады деп айтуға болады. Мысалы, 2003 жылы шығарылған Motorola MPx200, SAR мәні тек 0,120 Вт/кг, ал Samsung Galaxy note 4-0,23. Бірақ, тіпті соңғы жылдары iPhone сияқты жоғары көрсеткіштерде, сәулелену ағзаға әсер етпейді.



Сурет 47 - Айфондағы SAR деңгейі

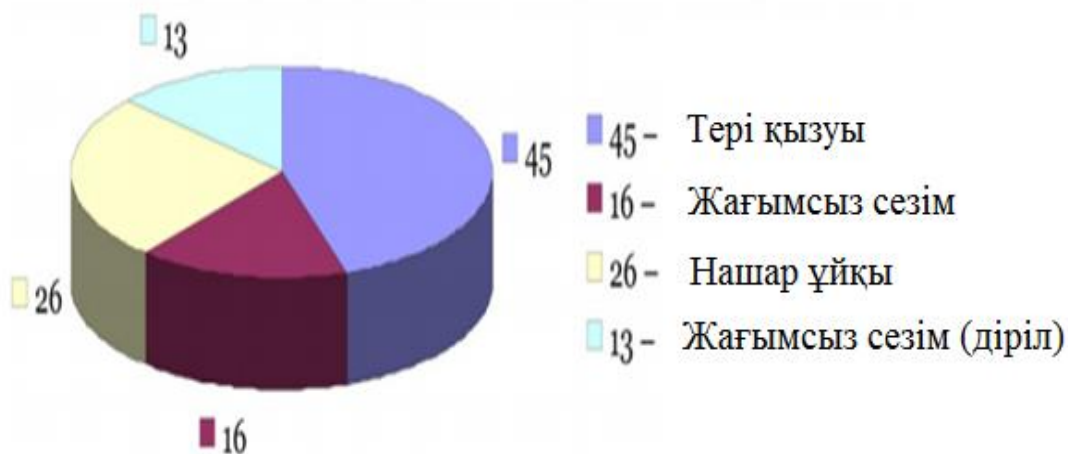
5.2 Ұялы телефондардың адам ағзасына әсері

1996 жылы Дүниежүзілік денсаулық сақтау ұйымы халықаралық жоба құрды. Электромагниттік өрістер бойынша ұялы телефондармен және олардың базалық станцияларымен шығарылатын радиожиилік өрістерін қоса алғанда, электромагниттік өрістердің адам денсаулығына әсер етуінің бар ғылыми фактілерін бағалау үшін, сондай-ақ ғылыми зерттеулер жүргізу бойынша ұсыныстар беру үшін жобаны құрды.

Норвегия мен Швецияда жүргізілген зерттеулер бойынша жастардың сәулелену әсеріне ұшырауы туралы зерттеуі, тіпті күніне екі минуттан аз телефонды пайдаланған адамдар ыңғайсыздық пен бөгде әсерлерге шағымданды. Телефонды ұзақ пайдаланса, денсаулық проблемалары туындайды. Күн сайын 30 минутқа жуық пайдаланатындар, жадының жоғалу ықтималдығы екі есе дерлік шектеледі. Ең үлкен тәуекел 30 жасқа дейінгі адамдар ұшырайды, олар бөгде әсерлерге 3-4 есе жиі ұшырайды.

Бірақ бүгінгі күні қоршаған ортада адамға теріс әсер ететін электромагниттік сәулелену көздерінің саны тым үлкен болғандықтан ұялы телефонның әсерін азайту өте қиын.

Сарапшылар телефонды жиі қолданатын 100 студентпен сұхбат жүргізді. Сарапшылар алған нәтижелері 48-суретте көрсетілген. Телефонды қолдану аймағына жақын тері аудандарында 45 адамда қызу, 26 адам нашар ұйқы, 16 студентте жағымсыз сезім, жағымсыз сезім діріл 13 студентте байқалды.



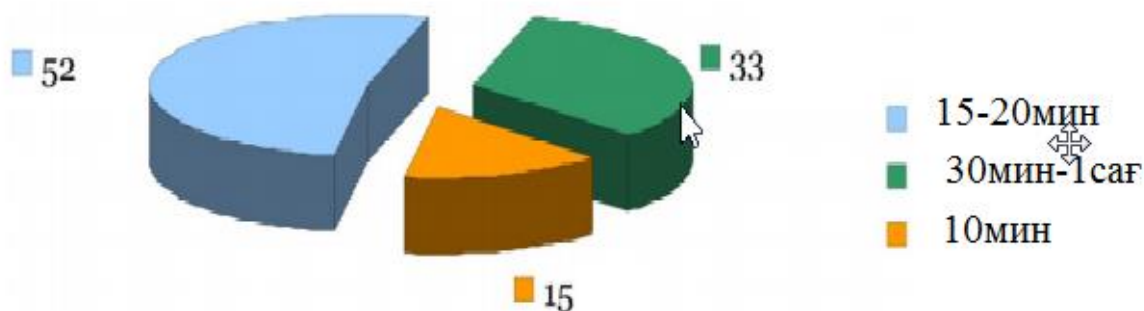
Сурет 48 - Ұялы телефонды пайдалану кезіндегі сезім

Экспериментке қатысушыларды сарапшы-медбикелер зерттей отыра, олардың ішінен ұялы телефоннан шығатын электромагниттік толқынның әсерінен ағза жүйесіне теріс әсерін тигендерді анықтады.

Бұл жағдайда ұялы телефондардың орталық жүйке жүйесі зиянды әсер ететінін ескере келе: Есте сақтау, ерік-жігердің нашарлауы, ұйқының бұзылуы байқалды.

Зерттеулер адамдардың денсаулығы мен ұзақтығына әртүрлі әсер ететінін көрсетті. Бірнеше жыл бойы телефонды ұзақ және тұрақты пайдаланған кезде ұйқының бұзылуы, иммунитеттің тежелуі, анемия байқалуы мүмкін.

Студенттердің тәулігіне ұялы телефон арқылы сөйлесу уақытын мониторингілеу, 49-суретте көрсетілгендей нәтиже берді.



Сурет 49 - Телефон арқылы сөйлесу уақыты

Диаграммада сұралған 100 адамның 52 – сі сөйлесу уақыты 15 – тен 20 минутқа дейін; 33 адам 30 мин-1 сағатқа дейін; 15 адам-10 минутқа дейін сөйлесетінін көруге болады.

Телефон бастың жанында орналасқандықтан, ми ісігінің даму қаупі, ұйқының қалыпты режимінің бұзылуы және күн фазасының өзгеруі

айтарлықтай артады.

Ұялы телефонды жиі және ұзақ пайдалану нәтижесінде иммунитеттің төмендеуі, бұл ағзаның әртүрлі инфекцияларға қарсы тұруының нашарлауына әкеледі. Ұялы телефондарды пайдалану демікпе мен экземаның дамуына ықпал етеді. Электромагниттік толқындардың эндокриндік жүйеге әсері нәтижесінде қандағы адреналин мөлшері артады [23].

Өйткені барлық жастар мектеп жастан бастап ұялы телефонмен пайдаланады, онда электромагниттік толқындардың әсерінен олардың жыныстық жүйесіне назар аудару қажет. Бұл мәселе өте маңызды, өйткені ұрпақты болу жасындағы жастар әсіресе ұялы байланыс көздерін жиі пайдаланады.

Швед ғалымдары ұялы телефонның сәулелері бірте-бірте мидың маңызды жасушаларын бұзады деп дәлелдеді. Ұялы телефон желісі жоғалған жағдайда, ол зиянды болады, өйткені оны іздеу үшін электромагниттік импульстердің күшті бағытталған ағындарын шығарады. Бұл ретте іздеу сигналының қуаты мен жиілігі әдеттегі режимде жұмыс істеген кезде қарағанда айтарлықтай жоғары.

2000-2003 жылдары ұялы телефонның денсаулыққа зиян келтіретіні туралы ешқандай сенімді деректер болған жоқ. 2000 жылы Дүниежүзілік Денсаулық сақтау ұйымы алдағы Еуропа Парламенті конференциясына байланысты ұялы телефондардың қауіпсіздігі мәселесі бойынша өз ұсыныстарын жариялады. Ұсынымдарда сол кезде ұялы телефондарды пайдалану Обыр немесе басқа да ауыр аурулардың дамуымен байланысы туралы сенімді дәлелдердің болмағандығын айтты. Жағымсыз әсерлері реакция немесе ұйқының бұзылуының баяулауы сияқты, сондай-ақ ғылыми расталмаған деп танылды. Осылайша, ұсыныстарында көрсетілгендей, бұл ұялы телефондарға ешқандай қауіпсіздік шаралары қолданбауы тиіс. Ұялы телефондардың иелерін зерттей отырып, мұндай тұжырымды психологтар жасайды. Аппаратқа психологиялық тәуелділік келесі түрлерде көрінуі мүмкін.

Біріншіден, бұл телефонның болмауы туралы алаңдаушылық. Австралиялық психолог Диана Джеймс өзінің ұялы телефонына тәуелділігі темекіге қарағанда күшті деген пікір айтады. Егер өзіңізбен бірге жарық түтік болмаса, жалғыздық пен депрессивті жағдай туындайды, адам қатты алаңдаушылық сезінеді, кейбір жағдайларда үрейге ұласуы мүмкін. Бұл ретте гипертониялық құбылыстар – артериялық қысымның секіруі байқалады. Немесе мысал: жақын адам ұялы телефонын үйде қалдырды - және мұнда алаңдаушылық себебі бар, не болып қалды, қайда екен, неге кідіреді? телефон тәуелділікті тудырады-мұндай қорытынды психологтар ұялы телефон иелерін зерттейді. Аппаратқа психологиялық тәуелділік келесі түрлерде көрінуі мүмкін.

Екіншіден, бұл SMS-жазушылар. Адам күніне ондаған SMS жазады және жібереді, тіпті оған қоңырау шалу оңайырақ болса да тоқтай алмайды. Италияда, мысалы, сұралғандардың 25% күніне 15 SMS алады және жібереді.

Олардың арасында өз денсаулығына қауіп төндіретін рекордшылар да бар. Осылайша, он төрт жасар итальяндық қыз ауруханаға түсті, себебі күн сайын достарына жүздеген SMS жіберді.

Келесі тәуелділік түрі-ақпараттықшылар десекте болады. Телефон иесі үнемі қоңырау немесе SMS күтеді, ұялы телефонды алады, маңызды ақпаратты жіберіп алмауын тексереді, электрондық пошта мен SMS-хабарламаларды оқиды. Нәтижесінде, адам оған қандай ақпарат маңызды екенін есте сақтай алмайды және өз ұялы телефоныңызға қайта-қайта хабарласады.

5.3 Пайдалы кеңестер мен сақтық шаралары.

- 1) микротолқынды сәулелену қуаты аз телефондар сатып алу.
- 2) ұялы телефонды шалбардың қалтасында емес, сөмкеде алып жүру керек, оны ұялы антеннасы адамнан әрі қарай және дисплейден алыстататындай етіп орналастырған жөн.
- 3) ұялы телефонды қажетсіз пайдаланбау керек, себебі, егер ұялы телефон күту режимінде ештеңе түсірмесе де, телефон желі қамту аймағында болмаса, бұл жағдайда желіні анықтау үшін таратқышты мезгіл-мезгіл қосады және онымен байланыс қалпына келтірілгенге дейін жалғасады.
- 4) дыбыс деңгейін арттыру кезінде қуат, сәуле шығару автоматты түрде артады.
- 5) кем дегенде 15 минут үзілісімен мүмкіндігінше қысқа сөйлескен дұрыс. Сөйлесуді СМС – хабарламаларға немесе жеке кездесуге болады. Ұялы телефон бойынша ұзақ сөйлесуге болмайды.
- 6) әңгіме кезінде бас терісінен кемінде 3 сантиметр қашықтықта ұстау керек, себебі бұл аралықта сәулеленудің ең жоғары ошағы болады. Құлаққапты пайдаланғанда, Bluetooth (құлаққап пен ұялы телефон арасындағы сымсыз байланыс) аз әсер береді. Сондай-ақ, GPRS, EDGE технологиясы бойынша деректерді жіберу режимінде сәулелендіру қарқындылығы өсе түсетінін ескеру керек.
- 7) ұялы байланыс 16 жасқа дейінгі балалар мен жасөспірімдерге, жүкті әйелдерге, неврологиялық ауруларға бейім адамдарға, жүрек ырғағының кардиологиялық құрылғылары имплантацияланған адамдарға мүлдем ұсынылмайды.
- 8) ұялы телефонды метрода, трамвайда, троллейбустарда және жоғары вольтты электр беру желілерінің жанында пайдаланбау керек. Яғни табиғи электромагниттік өріс әлсіреген жерде.
- 9) қоңырау кезінде телефонды құлаққа жақындатпаған жөн, себебі бұл уақытта телефон таратқышының ең үлкен қуаты болады.
- 10) телефонды түнде өшіруген дұрыс. Тіпті күту режимінде жұмыс істейтін ұялы телефон ұйқының жылдам және баяу фазасын бұза отырып, ұйқы кезінде әсер етеді. Оятарда телефон өшірулі кезінде де жұмыс жасайды.

Меншікті жұту қуатын есептеу

Анықтау бойынша, меншікті жұтылатын қуат (SAR - Specific AbsorptionRate) кеңістікте :

$$SAR = \frac{\sigma|E|^2}{\rho} \quad (4.11)$$

мұндағы σ - материалдың осы көлемдегі өткізгіштігі, См/м; E -өріс кернеулігі, В/м; ρ - заттың меншікті тығыздығы, кг/м³.

Формулада (4.11) егер бас моделінің қызықты нүктелерінде E мәндері белгілі болса, пайдалануға болады. Талдау өріс шектеуге болады нүктелер неғұрлым жақын орналасқан – антенна жүйесі, немесе ең тән бағыттар. Мұндай бағыттармен анализде телефонның корпусына перпендикуляр және антенна биіктігіне жақын биіктікте жүретін желілерді таңдаймыз, 0,9 және 1,9 жиіліктері үшін адам басының үш қабатты моделінің параметрлері (жақшада көрсетілген) ГГц.Жұмыста адам басының үш қабатты моделі қолданылады 14-кестеде көрсетілген.

Кесте 14 –Адам басының үш қабатты моделі

Адамның басының үш қабаты	Қалыңдығы, мм	Радиус сферасы, мм	Салыстырмалы диэлектрлік өткізгіштігі, ϵ	Қабаттың өткізгіштігі, См/м	$\text{tg } \delta$ [6]	Қабаттың тығыздығы кг / м ³
Мый		48	53 (46)	1,1 (1,7)	0,415 (0,369)	1030
Сүйек	3		9 (8)	0,06 (0,1)	0,133 (0,125)	1800
Тері	1		59 (46)	1,3 (1,9)	0,44 (0,41)	1100

Қорытындылай келе, ұялы байланыс халық үшін зиянды болып табылады. Алайда, ұялы байланыстың адам денсаулығына зиянды екеніне қарамастан, қазіргі уақытта одан бас тарту өте қиын, демек, оны мүмкіндігінше аз пайдалану керек .

Ұялы телефон – жоғары жиілікті электромагниттік сәулелену көзі. Ұялы телефондардан екі бағыт бойынша адам денсаулығына әсер ететіні белгілі. Біріншіден, мидағы электр процестеріне әсер етеді, бұл нейроциркуляторлық дистонияға әкелуі мүмкін. Екіншісі-жылу, әсіресе нашар қан айналымы бар тіндерге қауіпті.

Қорытынды

Осы дипломдық жұмыстың мақсаты-жаңа клиенттерді неғұрлым тиімді тарту үшін дамытушы білім беру орталығы үшін мобильді қосымша жасау, ойын арқылы балалардың ойлау, жылдам шешім қабылдау мүмкіндіктерін дамыту. Сондай-ақ Android Studio әзірлеу ортасында Android ОЖ үшін бағдарламалаудың практикалық дағдыларын бекіту. Қойылған мақсатқа жету үшін келесі міндеттер құрылды:

Ресей және Қазақстан мобильді қосымшалар нарығының бүгінгі таңдағы жағдайына талдау жасау, сол арқылы мобильді қосымшаның қаншалықты сұранысқа және қолданысқа ие екендігін анықтау мақсатында талдау жасалды. Қолданушы интерфейс жобаланып, мобильді қосымша әзірленді. Қосымшаның қауіпсіздігін қамтамасыз етуде парольдік қорғау механизмі және pro-guard кодты бұрмалау процедурасы қолданылды. Мобильді қосымша ойынға арналған. Сол арқылы қолданушының ойлау қабілеті, жылдам шешім қабылдау мүмкіндігі, жылдам жұмыс істеу машығы қалыптасады деп болжанады.

Мобильді қосымшаға қойылған талаптар анықталып,, пайдаланушы интерфейсіннің прототипі жасалған интерфейске функционалды талаптар талданды. Бұдан әрі мобильдік технологиялар саласындағы жаңа технологияларды қолдана отырып, Android ОЖ үшін мобильді қосымшаның ең қарапайым нұсқасын әзірлеу жүргізілген. Тапсырманы шешу кезінде бағдарламалық қамтамаға, пайдаланушы интерфейсінә қойылатын талаптарды ұсыну және талдаудың теориялық әдістері зерделенді. Дипломдық жұмысқа қойылатын талаптарға сәйкес келетін қосымша әзірленді және сипатталған талаптарға сәйкес жұмыс істейді. Сондай-ақ, Android Studio әзірлеу ортасында жаңа жұмыс дағдылары бекітіліп, алынды. Осылайша, міндеттер толық көлемде шешілді, мақсатқа қол жеткізілді.

Әдебиеттер тізімі

- 1 Дронов В.А. Разработка современных Web-сайтов. - СПб.: БХВПетербург, 2013. – 414 с. 5.
- 2 Зольников Д.С. PHP: Как самостоятельно создать сайт любой сложности. 2 изд. - М.: ИТ Пресс, 2014. - 272 с.
- 3 Прохоренок Н. М. HTML, JavaScript, PHP и MySQL. Джентельменский набор Web-мастера, 2013. – 912 с.
- 4 Печников В.Н. Создание Web-страниц и Web-сайтов. Самоучитель. - М.: Триумф, 2013. - 470 с.
- 5 Джеймс Гослинг, Билл Джой, Гай Л. Стил, Гилад Брача, Алекс Бакли - Язык программирования Java SE 8.
- 6 Голощанов А. Google Android: программирование для мобильных устройств. — СПб.: БХВ-Петербург, 2010. — 448 с. — ISBN 978-5-9775-0562-8.
- 7 Коматинэни С., Маклин Д., Хэшими С. Google Android: программирование для мобильных устройств = Pro Android 2. — 1-е изд. — СПб.: Питер, 2011. — 736 с. — ISBN 978-5-459-00530-1.
- 8 Сатия Коматинени, Дэйв Маклин. Android 4 для профессионалов. Создание приложений для планшетных компьютеров и смартфонов = Pro Android 4. — М.: Вильямс. — 880 с. — ISBN 978-5-8459-1801-7.
- 9 Роджерс Р., Ломбардо Д. Android. Разработка приложений. — М.: ЭКОМ Паблишерз, 2010. — 400 с. — ISBN 978-5-9790-0113-5.
- 10 Донн Фелкер. Android: разработка приложений для чайников = Android Application Development For Dummies. — М.: Диалектика, 2011. — 336 с. — ISBN 978-5-8459-1748-5. – URL: <http://habrahabr.ru/post/185096/> (кіру уақыты 25.03.2019)
- 11 Дейтел П., Дейтел Х., Дейтел Э., Моргано М. - Android для разработчиков. URL: <http://developer.android.com/index.html> (кіру уақыты 18.02.2019)
- 12 RecyclerView и CardView. Новые виджеты в Android L. URL: <http://habrahabr.ru/post/237101/> (кіру уақыты 27.03.2019)
- 13 Основы JavaScript. URL: <https://learn.javascript.ru/first-steps> (кіру уақыты 27.03.2019)
- 14 JavaScript and HTML DOM Reference URL: <https://www.w3schools.com/jsref/default.asp> (кіру уақыты 02.04.2019)
- 15 Знакомство с JavaScript. URL: <http://www.wisdomweb.ru/JS/javascript-first.php> (кіру уақыты 01.05.2019)
- 16 Stetho — Вслушиваемся в работу приложения. URL: <http://developer.alexanderklimov.ru/android/debug/stetho.php> (кіру уақыты 17.05.2019)
- 17 Руководство по языку Kotlin. URL: <http://kotlinlang.ru/> (кіру уақыты 28.04.2019)

- 18 Используем Kotlin в своем Android-проекте. URL: <http://java-help.ru/kotlin-introduction/> (кіру уақыты 24.05.2019)
- 19 Вихарев, А. П. Влияние сотовой связи на здоровье пользователя / А. П. Вихарев // Наука – производство – технологии – экология : сб. материалов конф. – Киров, 2004. – Т. 4. – С. 181–182.
- 20 Редковская, В. Ю. Влияние мобильных сотовых телефонов на здоровье человека / В. Ю. Редковская, В. В. Аччасов // Научная сессия ТУСУР–2006. : материалы докл. Всерос. науч.-техн. конф. студентов, аспирантов и мол. ученых. – Томск, 2006. – Ч. 5. – С. 92–94.
- 21 Заде, Л. Основы нового подхода к анализу сложных систем и процессов принятия решений / Л. Заде // Математика сегодня : пер. с англ. – М. : Знание, 1974. – С. 5–49.
- 22 Авдонина, Л. А. Процессный подход к созданию информационных систем поддержки прогнозных решений по оценке уровня безопасности технических объектов : моногр. / Л. А. Авдонина, В. И. Волчихин, А. К. Тарасов, Е. В. Тихомирова. – Пенза : Изд-во ПГУ, 2012. – 220 с.
- 23 Вершинин, Н. Н. Методы оценки управленческих решений по повышению безопасности специальных технических систем / Н. Н. Вершинин // Известия высших учебных заведений. Поволжский регион. Технические науки. – 2005. – № 5 (20). – С. 115–123.