МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

Кафедра протидії кіберзлочинності факультету № 4

МЕТОДИЧНІ МАТЕРІАЛИ
ДО СЕМІНАРСЬКИХ ЗАНЯТЬ

навчальної дисципліни
«Розробка захищених мобільних застосувань»
обов'язкових компонент освітньої програми
другого (магістерського) рівня вищої освіти

125 Кібербезпека та захист інформації
(безпека інформаційних та комунікаційних систем)

Харків 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 30.08.2023 № 7

СХВАЛЕНО
Вченою радою факультету № 6
Протокол від 16.08.2023 № 8

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 29.08.2023 № 7

Розглянуто на засіданні кафедри протидії кіберзлочинності факультету № 4 (протокол від 15.08.2023 № 19)

Розробники:
1. Доцент кафедри протидії кіберзлочинності факультету № 4, кандидат технічних наук, доцент Клімушин П.С.

Рецензенти:

1. Завідувач кафедри інформаційних управляючих систем ХНУРЕ, д.т.н., професор Петров К. Е.

2. Провідний науковий співробітник Науково-дослідної лабораторії з проблем розвитку інформаційних технологій ХНУВС, к.т.н., доцент Мордвинцев М.В.

ЗМІСТ

Загальні методичні вказівки

Навчання з дисципліни «Розробка захищених мобільних застосувань» проходить у формі: лекцій(20 год.), практичних (10 год.) та семінарських занять (10 год.), а також самостійної роботи (90 год.). Метою лекційного курсу є розкриття основних категорій, особливостей тематики та проблемних аспектів відповідних тем.

Аудиторні заняття проводяться у формі практичних занять, на яких студенти під керівництвом викладача засвоюють навички розв'язання практичних задач шляхом побудови алгоритмів і подальшої їх реалізації шляхом розробки програми або розв'язання задачі за допомогою інструментальних засобів. Самостійна робота за кожною темою включає вивчення рекомендованих джерел, навчальної та науково-монографічної літератури, а також розв'язання практичних завдань, що сформульовані в методичних вказівках, та підготовку звіту про виконання лабораторної роботи.

1. Розподіл часу навчальної дисципліни за темами (денна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни					Вид контролю
	Всього	з них:				
		лекції	Семінарські заняття	Практичні заняття	Самостійна робота	
Тема № 1. Бездротові локальні мережі	9	2	2		5	
Тема № 2. Сучасні мобільні операційні системи та мові програмування додатків	9	2	2		5	
Тема № 3. Інструменти і середовища розробки мобільних додатків	9	2	2		5	
Тема № 4. Середовище розробки платформи Android	9	2	2		5	
Тема № 5. Побудова інтерактивних програм	9	2		2	5	
Тема № 6. Множинні активності та інтенти	9	2		2	5	
Тема № 7. Користувацький інтерфейс	9	2		2	5	
Тема № 8. Робота з базами даних	9	2		2	5	
Тема № 9. Безпека мобільних застосувань	9	2		2	5	
Тема № 10. Месенджери миттєвого обміну повідомленнями та захист мобільних і хмарних обчислювальних середовищах	9	2	2		5	
Всього за семестр № 2:	**90**	**20**	**10**	**10**	**50**	**екзамен**
Всього по дисципліні	**90**	**20**	**10**	**10**	**50**	

(заочна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни					Вид контролю
	Всього	з них:				
		лекції	Семінарські заняття	Практичні заняття	Самостійна робота	
Тема № 1. Бездротові локальні мережі	9	1		0,5	7	
Тема № 2. Сучасні мобільні операційні системи та мові програмування додатків	9	1		0,5	7	
Тема № 3. Інструменти і середовища розробки мобільних додатків	9	1		1	7	
Тема № 4. Середовище розробки платформи Android	9	1		1	7	
Тема № 5. Побудова інтерактивних програм	9	1		1	8	
Тема № 6. Множинні активності та інтенти	9	1		1	8	
Тема № 7. Користувацький інтерфейс	9	1		1	8	
Тема № 8. Робота з базами даних	9	1		1	8	
Тема № 9. Безпека мобільних застосувань	9	0,5		1	7	
Тема № 10. Месенджери миттєвого обміну повідомленнями та захист мобільних і хмарних обчислювальних середовищах	9	0,5		1	7	
Всього за семестр № 2:	**90**	**8**		**8**	**74**	**екзамен**
Всього по дисципліні	**90**	**8**		**8**	**74**	

2. Методичні вказівки до практичних занять

Семінарське заняття № 1. Бездротові локальні мережі

Кількість годин: 2 год.

Навчальна мета заняття:

1. Придбання теоретичних знань з теми «Середовище розробки платформи Android», розвиток здібностей до творчого мислення, формування навичок самостійної роботи з аналізу і узагальнення інформації, вміння проектувати компонентну архітектуру мобільного додатку.

Рекомендована література:

1. Dawn Griffiths, David Griffiths. Head First. Android Development. A Brain-Friendly Guide. O'REILLY. Beijing. Cambridge. Köln. Sebastopol. Tokyo.2015. 704 p.

2. Казимир В., Карпачев І., Усік А. Моделі системи безпеки ос android. URL: https://www.researchgate.net/publication/328775065_MODELI_SISTEMI_BEZPEKI_OS_ANDROID.
3. Конспект лекцій з дисципліни «Програмування для мобільних пристроїв». Укладачі: Готович В. А., Михайлович Т. В. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2020. 216 с.
4. Розробка застосувань для мобільних пристроїв. Конспект лекцій. Міністерство освіти і науки України ЗНТУ. Кафедра програмних засобів. Запоріжжя 2016. 62с.
5. Сайко В.Г., Казіміренко В.Я., Літвінов Ю.М. Мережі бездротового широкосмугового доступу. Навчальний посібник. Кив: ДУТ, 2015. 216 с.
6. Опорний конспект лекцій з курсу «Мобільні інформаційні системи». Тернопільський національний економічний університет. Факультет комп'ютерних інформаційних технологій. Тернопіль. 2016. 60с.
7. Соколов В. Ю., Бурячок В. Л., Тадждіні М. М. Безпека безпроводових і мобільних мереж. Київ, КУБГ, 2019. 130 с.
8. Шматко О. В., Поляков А. О., Федорченко В. М. Аналіз методів і технологій розробки мобільних додатків для платформи Android: навч. посіб. Харків : НТУ «ХПІ», 2018. 284 с.

Матеріально-технічне забезпечення: комп'ютерний клас.

Навчальні питання:

1. Загальна характеристика бездротових комп'ютерних мереж (КМ)
2. Класифікація бездротових КМ
3. Технології Wi-Fi, Bluetooth, NFC. Wireless Application Protocol
4. Покоління мереж мобільного зв'язку
5. Безпека бездротових КМ

1. ПОРЯДОК ПРОВЕДЕННЯ ЗАНЯТТЯ:

1.1. Проведення експрес-контролю готовності до заняття.

1.2. Ввести текст підготовленої програми і виконати її відлагодження.

1.3. Підібрати тести і виконати відпрацювання розробленого алгоритму на цих тестах.

1.4. Скласти звіт про виконану роботу і здати роботу викладачу.

1. **Загальна характеристика бездротових комп'ютерних мереж**

Бездротові комп'ютерні мережі – це технологія, що дозволяє створювати комп'ютерні мережі, які повністю відповідають стандартам дротових мереж, наприклад, Ethernet (езернет) без використання кабельної проводки. Бездротові технології передбачають передачу інформації між пристроями за допомогою електромагнітних хвиль.

Існують середовища передавання даних в комп'ютерної мережі: дротові або бездротові. Дротові системи передачі засновані на використанні витої порі, коаксіального кабелю, оптоволоконного кабелю. Бездротовий зв'язок переважно здійснюється в інфрачервоному або радіочастотному діапазонах електромагнітних хвиль.

Інфрачервоне випромінювання відрізняється відносно слабким

енергетичним рівнем і не може проникати через стіни чи інші перешкоди.

Бездротова оптична мережа на основі світлодіодів забезпечує передавання даних на відстань в одному напрямі в межах приміщенням і обмежена швидкістю 1-10 Мбіт/с.

Заміною інфрачервоним мережам є технологія BlueTooth. Працює в смузі частот 2,4 ГГц. Швидкість передачі даних і радіус дії цієї технології обмежений, але її перевага полягає в тому, що вона дозволяє обмінюватися даними між кількома пристроями одночасно.

Wi-Fi - позначає високочастотну бездротову локальну мережу (WLAN). Wi-Fi пропонує своїм користувачам свободу переміщення. Wi-Fi може використовуватися для поширення сигналу на відстань у кілька кілометрів. Як правило, одна точка доступу може забезпечити радіус дії до 100-200 метрів.

Напрями застосування:

1. Створення мережі між комп'ютерами офісу, виставкового комплексу, на виробництві, коли будувати кабельну проводку не доцільно або не можливо.
2. Надання доступу до мережі Інтернет мобільним користувачам у кафе, аеропортах, бібліотеках, готелях тощо.
3. З'єднання сегментів дротових мереж (функція мосту).
4. Створення домашніх мереж.
5. Мережі провайдерів Інтернет: підключення клієнтів там, де немає можливості протягнути кабель.

Компоненти: Бездротові локальні мережі на базі стандарту 802.11 будуються за допомогою двох основних типів пристроїв: *бездротових станцій*, якими звичайно є персональні комп'ютери, обладнані бездротовими *мережними картами*, і пристроями доступу, або "*точками доступу*".

Антени класифікуються за способом випромінювання сигналу. Спрямовані антени концентрують потужність сигналу в одному напрямку. Всенаправлені антени випромінюють сигнал у всіх напрямках з однаковою інтенсивністю. Концентруючи сигнал в одному напрямку, спрямовані антени можуть передавати сигнали на великі відстані. Спрямовані антени зазвичай використовуються для об'єднання систем, а всенаправлені антени використовуються в точках доступу.

Режими роботи:

1. Ад Хок - для спеціальної мети - децентралізований режим бездротової мережі, коли клієнтські станції взаємодіють безпосередньо один з одним без точки доступу або Wi-Fi роутера. Для режиму Ад Хок потрібно мінімум обладнання - досить, щоб кожна станція була оснащена бездротовим адаптером Wi-Fi. При такій конфігурації не потрібно створення будь-якої мережевої інфраструктури. У цьому режимі кожен вузол бере участь в маршрутизації шляхом пересилання даних для інших вузлів, тому визначення того, які вузли пересилають дані, проводиться динамічно на основі мережевого з'єднання і алгоритму маршрутизації. Режим Ad-Hoc застосовується в основному для створення тимчасових мереж, наприклад коли потрібно швидко з'єднати два комп'ютери для передачі даних. Бездротові мобільні мережі ad hoc є самонастроювальні динамічні мережі, в яких вузли можуть вільно

переміщатися. Бездротовим мережам не вистачає складнощів в налаштуванні і адмініструванні інфраструктури, що дозволяє пристроям створювати і приєднуватися до мереж «на льоту» - в будь-якому місці і в будь-який час.

2. Режим інфраструктури. Точку доступу можна розглядати як бездротовий концентратор. Режим інфраструктури є бездротовим мережевим середовищем, в центрі якої знаходиться точка доступу до бездротової мережі / маршрутизатор. У режимі інфраструктури бездротові пристрої з'єднуються один з одним через точку доступу до бездротової мережі/маршрутизатор. Точка доступу до бездротової мережі/маршрутизатор також може виступати в ролі моста або шлюзу дротової мережі, таким чином бездротові пристрої можуть підключатися не тільки один до одного, а й до дротової мережі.

Додаткові режими:

Режим повторювача для збільшення радіусу дії бездротової мережі. Точка доступу дозволяє розширити діапазон дії бездротової мережі за допомогою повторення сигналу від віддаленої точки доступу.

Точка доступу в режимі "Клієнт". Режим можна застосовувати при підключенні до бездротової мережі пристроїв з портом Ethernet, але без можливості установки бездротового адаптера.

Технологія WDS (Wireless Distribution System). Режим можна застосовувати при підключенні до бездротової мережі пристроїв з портом Ethernet, але без можливості установки бездротового адаптера.

Термін WDS (Wireless Distribution System) розшифровується як «розподілена бездротова система». Дана технологія дозволяє точкам доступу встановлювати бездротове з'єднання не тільки з бездротовими клієнтами, але і між собою. Технологія WDS може використовуватися для реалізації двох режимів бездротових з'єднань між точками доступу: режиму бездротового моста (радіомоста) і режиму бездротового повторювача. Режим бездротового моста (WDS) дозволяє точкам доступу працювати тільки з іншими точками доступу, але не з клієнтськими адаптерами. Режим бездротового повторітеля дозволяє точкам доступу працювати як з іншими точками доступу, так і з клієнтськими адаптерами.

Роумінг в бездротових мережах. Як тільки користувач переміщається від однієї точки доступу до іншої, бездротової адаптер автоматично встановлює заново з'єднання і підключається до найближчої точки для забезпечення кращої якості сигналу і продуктивності.

Роумінг – використання одних і тих же каналів для збільшення зони охвату. Точки доступу, зони охвату яких перетинаються, повинні бути налаштовані на різні канали. Але можна використовувати однакові канали на точках доступу з зонами охвату, що не перетинаються. Таким чином, можна збільшувати загальне покриття мережі практично без обмежень.

Термін, *прихований вузол* в бездротової мережі відноситься до вузлів, які находяться за межами видимості інших вузлів. Проблема виникає тоді, коли ці вузли починають посилати пакети на точку доступу одночасно, тому що вузли не бачать один одного.

Бездротові мережі дозволяють швидко організувати обмін даними в

умовах, які перешкоджають розгортанню кабельної інфраструктури або коли створення кабельної мережі є просто недоцільним, скажемо, при створенні тимчасових робочих груп, для проведення конференцій, виставок тощо. Особливо зручні бездротові мережі для тих користувачів, які за родом своєї діяльності повинні бути мобільними. Вони дозволяють їм вільно переміщатися, залишаючись при цьому постійно підключеними до мережі і маючи можливість оперативного доступу до будь-якої інформації.

Бездротові мережі не тільки забезпечують мобільний доступ, але і самі мобільні: можна легко перемістити мережу в інше місце.

Переваги:

1. Низька вартість розгортання, яка постійно зніжується.
2. Висока швидкість розгортання.
3. Висока заявлена швидкість передачі даних, але фактична – значно менше.
4. Мобільність: користувач може рухатися і постійно мати доступ до даних.
5. Масштабуємость – можливість простого і швидкого розширення зони покриття і збільшення кількості користувачів.
6. Гнучкість: підключення можливе де завгодно і коли завгодно.

Недоліки:

1. Швидкість передавання даних залежить від впливу перешкод і відстані між передавачем й приймачем сигналу.
2. Низька захищеність у порівнянні з дротовими мережами від атак зловмисників.

2. **Класифікація бездротових мереж**

Залежно від технологій та передавальних середовищ:

- мережі на радіомодемах;
- мережі на стільникових модемах;
- інфрачервоні системи;
- системи VSAT (супутникові станції з антенами менше 2,5 метрів);
- системи з використанням низькоорбітальних супутників;
- системи з технологією SST (використано розподіл сигналу за спектром частот);
- радіорелейні системи;
- системи лазерного зв'язку.

Стільниковий зв'язок - один із видів мобільного радіозв'язку, в основі якого лежить стільникова мережа. Особливість стільникового зв'язку полягає в тому, що зона покриття ділиться на «чарунки стільника», що визначається зонами покриття окремих базових станцій. Чарунки частково перекриваються й разом утворюють мережу. На ідеальній (рівній і без забудови) поверхні зона покриття однієї базової станції являє собою коло, тому складена з них мережа має вигляд шестикутних зон (бджолиного стільника).

Мережу становлять рознесені в просторі прийомопередавачі, що працюють у тому самому частотному діапазоні, і комутувальне устаткування,

що дозволяє визначати поточне місце розташування рухливих абонентів і забезпечувати безперервність зв'язку при переміщенні абонента із зони дії одного прийомопередавача в зону дії іншого.

За дальністю дії

– Бездротові персональні мережі (WPAN — Wireless Personal Area Networks). Приклади технологій - Bluetooth.

– Бездротові локальні мережі (WLAN — Wireless Local Area Networks). Приклади технологій -Wi-Fi.

– Бездротові мережі масштабу міста (WMAN - бездротовий Metropolitan Area Networks). Приклади технологій - WiMAX.

– Бездротові глобальні мережі (WWAN - бездротова глобальна мережа). Приклади технологій - CSD, GPRS, EDGE, EV-DO, HSPA, LTE.

Залежно від використовуваної технології бездротові мережі можна розділити на три типи:

– локальні обчислювальні мережі;

– розширені локальні обчислювальні мережі;

– мобільні мережі (переносні комп'ютери).

Основні відмінності між цими типами мереж - параметри передачі. Локальні і розширені локальні обчислювальні мережі використовують передавачі і приймачі, що належать тій організації, в якій функціонує мережа. Для переносних комп'ютерів середовищем передачі служать загальнодоступні мережі, наприклад телефонна мережа або Інтернет.

3. Технології Wi-Fi, WIMAX Bluetooth, NFC. Wireless Application Protocol.

Wi-Fi - це набір глобальних стандартів. На відміну від стільникових телефонів, Wi-Fi обладнання може працювати в різних країнах по всьому світу.

Стандарт IEEE 802.11 є базовим стандартом для побудови бездротових локальних мереж (Wireless Local Network — WLAN). Стандарт IEEE 802.11 постійно вдосконалювався, а тому зараз існує сімейство, до якого відносять специфікації IEEE 802.11 з різними буквеними індексами від a до w. Однак тільки п’ять з них (a, b, g, і та n) є основними й користуються найбільшою популярністю у виробників устаткування, інші ж являють собою доповнення, удосконалення або виправлення прийнятих специфікацій.

Для просування на ринку пристроїв для бездротових локальних мереж (WLAN) була створена група, що одержала назву Альянс Wi-Fi. Цей альянс здійснює керівництво роботами по сертифікації устаткування різних виробників і видачі дозволу на використання членами Альянсу Wi-Fi логотипа торговельної марки Wi-Fi. Наявність на устаткуванні логотипа Wi-Fi гарантує надійну роботу й сумісність устаткування при побудові бездротової локальної мережі (WLAN) навіть при використанні пристроїв різних виробників. На сьогоднішній день Wi-Fi сумісним є устаткування, побудоване по стандарту IEEE 802.11a, b і g (для забезпечення захищеного з'єднання також може використовуватися стандарт IEEE 802.11i). Крім того, наявність на устаткуванні логотипа Wi-Fi означає, що робота устаткування здійснюється в

діапазоні 2,4 Ггц або 5 Ггц. Отже, під Wi-Fi варто розуміти сумісність устаткування різних виробників, призначеного для побудови бездротових локальних мереж, з урахуванням викладених вище обмежень.

Технологія WIMAX це стандарт IEEE 802.16 — стандарт безпровідного зв'язку, що забезпечує широкосмуговий зв'язок на значні відстані зі швидкістю, порівняною з кабельними з'єднаннями. Між сусідніми базовими станціями встановлюється постійне з'єднання з використанням надвисокої частоти 10-66 ГГц радіозв'язку прямої видимості. Дане з'єднання в ідеальних умовах дозволяє передавати дані зі швидкістю до 120 Мбіт / с. Обмеження по умові прямої видимості, зрозуміло, не є перевагою, проте воно накладається тільки на базові станції, що беруть участь в цілісному покритті району, що цілком можливо реалізувати при розміщенні обладнання. Як мінімум одна з базових станцій може бути постійно пов'язана з мережею провайдера через широкосмугове швидкісне з'єднання. Фактично, чим більше станцій мають доступ до мережі провайдера, тим вища швидкість і надійність передачі даних. Однак навіть при невеликій кількості точок система здатна коректно розподілити навантаження за рахунок стільникової топології. На базі стільникового принципу розробляються також шляхи побудови оптимальної мережі, що обгинає великі об'єкти (наприклад, гірські масиви), коли серія послідовних станцій передає дані по естафетному принципу.

1	№ стандарту	IEEE 802.16
2	Радіус дії	6 - 8 км
3	Діапазон	1,5-11 Ггц; 10-66 ГГц
4	Швидкість	70 Мбіт/с; 120 Мбіт/с
5	Основна функція	Розширення *Wi-Fi*. Об'єднує точки *Wi-Fi*
6	Перевага	Вихід у національні мережі, Інтернет

Bluetooth або блютуф (Wireless Personal Area Network, WPAN). Bluetooth забезпечує обмін інформацією між такими пристроями як персональні комп'ютери (настільні, кишенькові, ноутбуки), мобільні телефони, принтери, цифрові фотоапарати, мишки, клавіатури, джойстики, навушники, гарнітури на надійній, безкоштовній, повсюдно доступну радіочастоту для ближнього зв'язку. Bluetooth дозволяє цим пристрої повідомляти, коли вони знаходяться в радіусі до 100 метрів друг від друга (дальність сильно залежить від перешкод та перешкод), навіть у різних приміщеннях.

Зв'язок Bluetooth застосовується передусім для передачі інформації між різними портативними пристроями. Виробники стільникових телефонів, ПЕОМ, кишенькових комп'ютерів почали вбудовувати радіостанції Bluetooth у свої вироби.

Технологія Bluetooth забезпечує швидкість передачі інформації до 723

кбіт/с (версія 1.2) або до 2,1 Мбіт/с (версія 2.0) у радіусі від 10 до 100 м.

Технологія NFC – це технологія бездротової передачі на малій відстані: радіус зв'язку не перевищує 10 см. Інформація з об'єктів зчитується за допомогою радіосигналу.

В основі роботи NFC-модуля лежить електромагнітна індукція: на частоті 13,56 МГц передавач зчитувача за допомогою антени постійно випромінює сигнал у формі синусоїди. У датчику також є антена, і коли датчик і зчитувач опиняються на відстані, достатній для роботи NFC модуля, магнітне поле породжується змінним струмом у котушці зчитувача. Після цього струм створюється в другій котушці.

Цієї енергії достатньо для роботи останнього, тому NFC-модуль здатний працювати з пасивними пристроями.

Достоїнствами NFC є:

– Безпека. Тому що радіус дії NFC-модуля обмежений малою відстанню (10 см), дані перебувають у безпеці, адже ніхто за межами цієї відстані не зможе отримати доступ до платіжних даних або файлів.

– Швидкість з'єднання. Дана технологія забезпечує передачу даних менше, ніж за секунду. У старих смартфонах процедура могла зайняти до 15 секунд.

– Енергоефективність. NFC-модуль є дуже енергоекономічним. В наших реаліях це особливо актуально, тому що мале кількість пристроїв може відрізнятися високою автономність.

– Зручність. За допомогою даної технології вдається автоматизувати безліч завдань та спростити собі життя, скоротивши час виконання рутинних операцій

– Малі розміри. NFC-модуль має невеликі розміри, що дозволяє вбудовувати його у безліч пристроїв, як браслетів, каблучок, планшетів і т.д.

Таким чином, переваги даної технології роблять її дуже популярною тільки в безконтактній оплаті, а й в інших сферах життя, таких як: медицина, наука, туризм і т.д.

Протокол безпровідної передачі даних, (WAP, Wireless Application Protocol) - технологія, що використовується для запуску інтернет-додатків на мобільних терміналах. Інтернет-додатки, призначені для такого використання повинні бути підготовлені в спеціальному форматі і придатні для відпрацювання на мобільних терміналах з використанням низькошвидкісних каналів передачі даних існуючих мереж стільникового зв'язку.

WAP 2.0 - поліпшена версія WAP, що використовує скорочений варіант XHTML та CSS, тобто це означає, що сайт WAP 2.0 може бути відкритий за допомогою звичайного браузера на комп'ютері без установки будь-яких додаткових плагінів та ін.

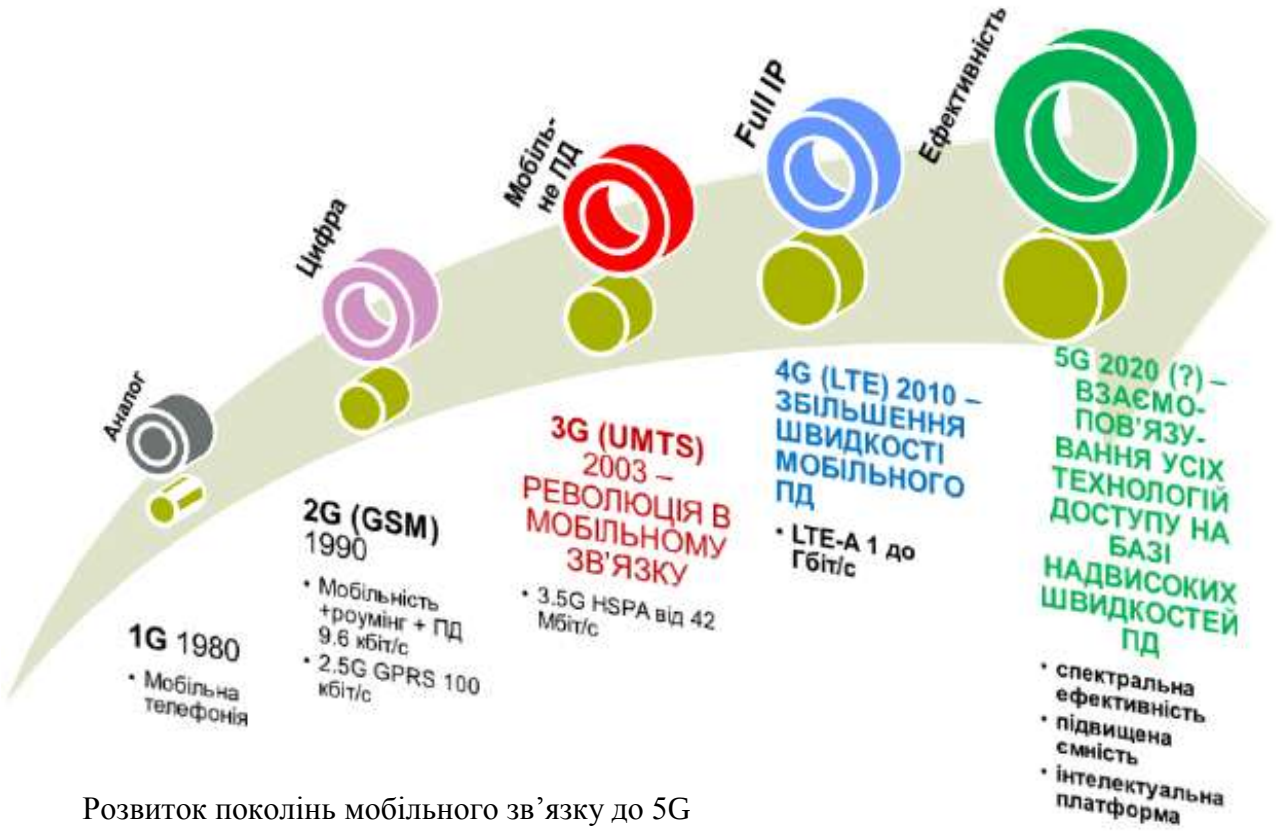
4. Покоління мереж мобільного зв’язку

Зараз для мобільного зв'язку, обслуговування соціальних мереж і веб-сайтів використовують технологію бездротового зв'язку четвертого покоління (4G), призначену для забезпечення високих швидкостей передачі даних і

великої пропускної здатності мережі. До розгляду можливостей технології 5G зупинимося на історичному розвитку, перевагах та недоліках

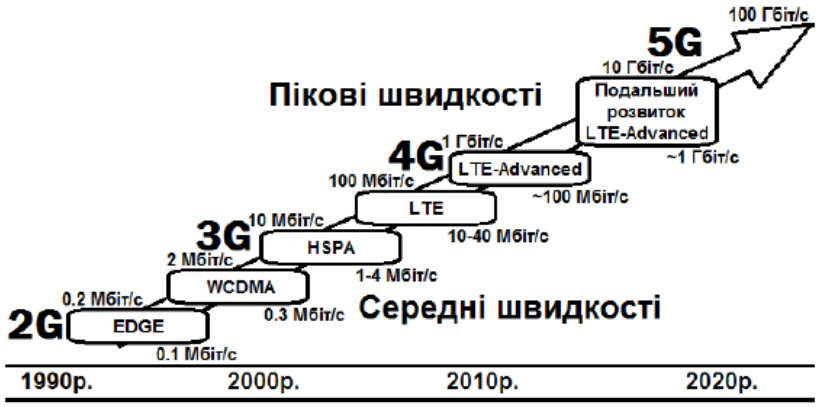
Таблиця 1. **Порівняння характеристик поколінь технологій бездротового зв'язку**

Технологія	1G	2G	3G	4G	5G
Розгортання	1970 –1980	1990-2001	2001-2010	2011-2020	2021
Пропускна здатність	2 Кбіт/с	1,6 Мбіт/с	2 Мбіт/с	1 Гбіт/с	вище 1 Гбіт/с
Смуга частот	-	1,25 МГц	5 МГц	20 МГц	вище 20 МГц
Технологія	Аналоговий стільнико-вий, техно-логія FM-радіо	Цифровий стільнико-вий, технологія GSM	CDMA 2000 (1xRTT, EVDO) UMTS, EDGE	Wi-Max LTE Wi-Fi	WWWW (скоро)



Розвиток поколінь мобільного зв’язку до 5G

Еволюція сучасних мереж мобільного зв'язку



Для забезпечення переходу на новий рівень продуктивності систему стільникового зв'язку LTE (Long-Term Evolution, - «Довготривалий розвиток», часто позначається як 4G LTE) - стандарт бездротової високошвидкісної передачі даних для мобільних телефонів та інших терміналів, що працюють з даними було вдосконалено від рівня 3GPP (3G) до B4G (вище 4G) з версіями стандарту LTE Release.

Системи 4G були спочатку запропоновані двома технологіями конкурентами, а саме: технологією глобальної сумісності для мікрохвильового доступу (WiMAX) та технологією довгострокового розвитку (LTE), основаної на 3GPP, який став найпоширенішим стандартом для мобільних послуг 4G на сьогодні. Це дає можливість користувачам безперешкодно перемикатися між провайдерами бездротового зв'язку, використовуючи тепер дійсно глобальний стандарт LTE-A (IMT-Advanced 4G), прийнятий у 2010 році.

Зараз найпоширенішим засобом зв'язку для інтелектуальних мобільних пристроїв є стандарт IEEE 802.11, більш відомий за маркетинговим терміном як WiFi. Набір стандартів, що лежить в основі технології та визначений для бездротової локальної мережі (WLAN), дає змогу розділити протокол доступу до середовища і до специфікації фізичного рівня. Залежно від фактичної реалізації, фізичний рівень ґрунтується на базових швидкостях в 1–2 Мбіт/с, смугах 2,4 ГГц та інфрачервоному LOS (поширення радіоліній прямої видимості). Завдяки розподілу на два рівня, визначення базових каналів може виконуватися окремо від реальних механізмів, що уможливлює вільне застосовування різних промислових, наукових і медичних діапазонів (ISM) у всьому світі.

Згодом з'явилися просунутіші версії від 802.11a до 802.11n і 802.11ac, які збільшують пропускну здатність за рахунок об'єднання каналів та робочих змін у смугах частот понад 300 і 400 Мбіт/с.

Термінали користувача у мережі 4G повинні мати можливість вибирати цільові бездротові системи. Базові станції періодично транслюють сигнальні повідомлення у наявні системи GSM для передплати на послуги мобільного зв'язку. Однак цей процес є складним у гетерогенних системах 4G через відмінності в бездротових технологіях та протоколах доступу.

Для надання бездротових послуг у будь-який час і в будь-якому місці мобільність терміналу є обов'язковою умовою в інфраструктурі 4G. Мобільність дає змогу клієнтам переміщатися по географічних регіонах через кордони бездротових мереж. Існує дві основні проблеми мобільності терміналу: керування місцем розташування та керування передачею. За керування місцем розташування система відстежує та знаходить мобільний термінал для можливого підключення. Керування розташуванням включає в себе оброблення всієї інформації про роумінг терміналу, такої як оригінальні і поточні осередки, інформація про автентифікацію тощо. З іншого боку, керування передачею обслуговування підтримує постійний зв'язок, коли термінал переміщається. Мобільний IPv6 (MIPv6) - це стандартизований IP-протокол мобільності для бездротових систем IPv6. У цій схемі кожний термінал має домашню адресу IPv6. Кожний раз, коли термінал виходить за межі локальної мережі, домашня адреса стає недійсною і термінал отримує у поточній мережі нову службову IPv6-адресу. Крім схеми з широким доступом, вдосконалені методи передачі каналу з багатьма входами та виходами (MIMO) і значну координацію між декількома стільниковими вузлами, що має назву скоординованої багато точкової передачі/прийому (CoMP), було прийнято в якості ключових методів для LTE.

Платформа мережі 5G надає для операторів значні переваги, що виражаються перш за все, в розширенні функціональних можливостей та пропускної здатності мережі (performance) і підвищенні задоволеності користувачів (User Experience).

На рисунку 2 показані основні параметри мережі IMT2020 (5G), в порівнянні з показниками IMT-Advanced (4G), які дозволяють цього досягти.

Рисунок 3 - Основні параметри мереж IMT2020 (5G) та IMT-Advanced (4G)

Пікова швидкість: мережа 5G забезпечує в 20 разів бòльшую швидкість в порівнянні з 4G, тобто, близько 20 Гбіт/с. Швидкість на користувача (середня) при цьому може досягати 100 Мбіт/с і більше. Ефективність використання спектру, кількість інформації, яку можна передати на одиницю частотного діапазону, в мережі 5G буде принаймні в 3 рази вище, ніж в 4G. Мобільність користувача, швидкість, з якою може переміщатися користувач з терміналом 5G по площі покриття мережі без втрати зв’язку між базовими станціями, в мережі 5G досягає 500 км/год, що дає можливість користуватися послугами 5G в швидкісних поїздах.

Затримка в мережі 5G знижується до 1 мс і менше, в той час як в мережі 4G можна досягти мінімум 10-мілісекунди затримки. Це дозволяє використовувати технологію 5G для критичних комунікацій і відеоспостереження, послуг тактильного інтернету, AR/VR тощо.

Щільність терміналів в мережі 5G підвищується на порядок і може досягати декількох мільйонів пристроїв на 1 квадратний кілометр, тобто, на 1 квадратному метрі поверхні можуть розташовуватися кілька десятків або навіть сотень мініатюрних пристроїв (наприклад, сенсорів IoT).

Енергоефективність мережі 5G на порядок краще, ніж в мережі попереднього покоління. Ємність трафіку на одиницю площі, тобто швидкість передачі даних квадратний метр площі покриття мережі, в 5G на два порядки вище, ніж в мережі 4G.

5. Безпека бездротових мереж

Безпека мережі - заходи, які захищають інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів. Безпека інформаційної мережі включає захист обладнання, програмного забезпечення, даних і персоналу. Мережева безпека складається з положень і політики, прийнятої адміністратором мережі, щоб запобігти і контролювати несанкціонований доступ, неправильне використання, зміни або відмови в комп'ютерній мережі та мережі доступних ресурсів.

Концепції мережевої безпеки. Мережева безпека починається з автентифікації, що зазвичай включає в себе ім'я користувача і пароль. Зв'язок між двома комп'ютерами з використанням мережі може бути зашифрований, щоб зберегти конфіденційність.

Система безпеки мережі: захищає від внутрішніх та зовнішніх мережних атак. Ефективна система безпеки стежить за активністю в мережі, сигналізує про аномалії та реагує відповідним чином.

Захист в wi-fi мережах. Існує два основних варіанти пристрою бездротової мережі:

-Ad-hoc - передача безпосередньо між пристроями;

-Hot-spot - передача здійснюється через точку доступу.

Hot-spot представляє найбільший інтерес з точки зору захисту інформації.

Специфічні механізми безпеки.

Причина 70% успішних атак на бездротову мережу – неправильна

конфігурація точки доступу.

Реалізувати сервіси безпеки можна, впровадивши механізми:

шифрування	автентифікаційний обмін
цифровий підпис	заповнення трафіку
керування доступом	керування маршрутом
контроль цілісності даних	нотаризація

Загальні рекомендації щодо захисту мережі:

Використовуйте антивірусне ПЗ.

Використовувати ПЗ тільки з джерел яким ВИ ДІЙСНО довіряєте.

Використовуйте відкрите програмне забезпечення.

Не використовуйте додатки, які визначають Ваше місце положення.

Не переходіть на веб-ресурси, що здаються Вам підозрілими.

Намагайтеся охороняти свою приватність.

Фільтрація MAC-адрес дозволяє задати перелік пристроїв, що мають дозвіл на з'єднання з бездротовою мережею, за допомогою їх MAC-адрес.

Автентифікація - це надання дозволу на вхід в мережу за результатами перевірки автентичності набору облікових даних. Мета - з'ясувати, чи є пристрій, що намагається встановити з'єднання, довіреним пристроєм.

При використанні режиму PSK точка доступу і клієнт повинні використовувати загальний ключ або кодове слово. Точка доступу відправляє клієнту випадковий рядок байтів. Клієнт приймає цей рядок, шифрує використовуючи ключ, і відправляє назад в точку доступу. Точка доступу для розшифровки використовує свій ключ. Якщо розшифрований рядок, прийнятий від клієнта, збігається з вихідним рядком, то клієнту дається дозвіл встановити з'єднання.

PSK виконує односторонню автентифікацію - тільки точка доступу перевіряє справжність вузла. Вузол не перевіряє автентичності точки доступу. Також не перевіряється достовірність користувача, що підключається до вузла.

Шифрування даних використовується для захисту даних, що передаються. Протокол WPA - захист доступу до Wi-Fi, був розроблений на заміну протоколу WEP. Забезпечує контроль доступу на рівне портів: розблокування мережевого порту і забезпечення доступу клієнта до мережі здійснюється тільки після успішної автентифікації. Протокол TKIP, як компонент WPA – тимчасовий протокол цілісності ключів, забезпечує більш надійний механізм шифрування.

Висновки.

Переваги Wi-Fi:

– Дозволяє розгорнути мережу без прокладки кабелю, що може зменшити вартість розгортання і / або розширення мережі.

– Дозволяє мати доступ до мережі мобільних пристроїв.

– Wi-Fi - це набір глобальних стандартів. На відміну від стільникових телефонів, Wi-Fi обладнання може працювати в різних країнах по всьому світу.

Недоліки Wi-Fi:

– Частотний діапазон і експлуатаційні обмеження в різних країнах неоднакові.

– Висока порівняно з іншими стандартами споживання енергії, що зменшує час життя батарей і підвищує температуру пристрою.

– Wi-Fi мають обмежений радіус дії.

– Неповна сумісність між пристроями різних виробників або неповна відповідність стандарту може призвести до обмеження можливостей з'єднання або зменшення швидкості.

– Зменшення продуктивності мережі під час дощу.

– Перевантаження обладнання при передачі невеликих пакетів даних через приєднання великої кількості службової інформації.

– Мала придатність для роботи додатків, що використовують медіапотоки в реальному часі.

– Низка захищеність у порівнянні з дротовими мережами від атак зловмисників, як нової технології через загрози безпеці та конфіденційності інформації.

Семінарське заняття № 2. Сучасні мобільні операційні системи та платформи

Кількість годин: 2 год**.**

Навчальна мета заняття:

1. Придбання теоретичних знань з теми «Середовище розробки платформи Android», розвиток здібностей до творчого мислення, формування навичок самостійної роботи з аналізу і узагальнення інформації, вміння проектувати компонентну архітектуру мобільного додатку.

Рекомендована література:

1. Dawn Griffiths, David Griffiths. Head First. Android Development. A Brain-Friendly Guide. O'REILLY. Beijing. Cambridge. Köln. Sebastopol. Tokyo.2015. 704 p.
2. Казимир В., Карпачев І., Усік А. Моделі системи безпеки ос android. URL: https://www.researchgate.net/publication/328775065_MODELI_SISTEMI_BEZPEKI_OS_ANDROID.
3. Конспект лекцій з дисципліни «Програмування для мобільних пристроїв». Укладачі: Готович В. А., Михайлович Т. В. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2020. 216 с.
4. Розробка застосувань для мобільних пристроїв. Конспект лекцій. Міністерство освіти і науки України ЗНТУ. Кафедра програмних засобів. Запоріжжя 2016. 62с.
5. Сайко В.Г., Казіміренко В.Я., Літвінов Ю.М. Мережі бездротового широкосмугового доступу. Навчальний посібник. Кив: ДУТ, 2015. 216 с.
6. Опорний конспект лекцій з курсу «Мобільні інформаційні системи». Тернопільський національний економічний університет. Факультет комп'ютерних інформаційних технологій. Тернопіль. 2016. 60с.
7. Соколов В. Ю., Бурячок В. Л., Тадждіні М. М. Безпека безпроводових і мобільних мереж. Київ, КУБГ, 2019. 130 с.

8. Шматко О. В., Поляков А. О., Федорченко В. М. Аналіз методів і технологій розробки мобільних додатків для платформи Android: навч. посіб. Харків : НТУ «ХПІ», 2018. 284 с.

Матеріально-технічне забезпечення: комп’ютерний клас.

Навчальні питання:

1. Операційна система iOS
2. Операційна система Android
3. Операційна система Windows Mobile
4. Операційна система Symbian
5. Операційна система BlackBerry
6. Мови програмування мобільних додатків

Вступ. Життя сучасної людини практично немислиме без мобільних пристроїв. Їх якість більшою мірою залежить від апаратних характеристик, а ось зручність користування більшою мірою залежить від мобільної операційної системи. Тому дуже важливо підібрати не тільки хороші апаратні характеристики, потрібно ще вибрати операційну систему, з якою зручно буде працювати. І тільки підсумувавши ці параметри, можна вибрати для себе оптимальний мобільний пристрій.

Мобільна операційна система - операційна система для смартфонів, планшетів, КПК або інших мобільних пристроїв. Мобільні ОС поєднують в собі функціональність ОС для ПК з функціями для мобільних і кишенькових пристроїв: сенсорний екран, стільниковий зв'язок, Bluetooth, Wi-Fi, GPS-навігація, камера, відеокамера, розпізнавання мови, диктофон, музичний плеєр, NFC і інфрачервоне дистанційне управління. Сучасні мобільні телефони стає все більш «розумними», недарма ж їх називають смартфонами (в перекладі з англійської smart phone - розумний телефон).

Смартфон - це мобільний телефон, оснащений потужною операційною системою, яка в свою чергу дозволяє працювати з безліччю додатків одночасно. Іншими словами, смартфон - це аналог комп'ютера. Він може виконувати майже всі ті дії, які ми виконуємо, працюючи за комп'ютером, але в набагато менших масштабах. Саме операційна система є візитною карткою всіх пристроїв.

У даній лекції будуть розглянуті найпоширеніші операційні системи для мобільних пристроїв: Android, IOS, Windows Phone, Symbian OS, Blackberry OS.

1. Операційна система iOS

Мобільна операційна система від компанії Apple. Дана система набула поширення тільки на продуктах компанії Apple. Застосовується в iPhone, iPod, iPad, а також для телевізійної приставки AppleTV. Для завантаження програм під iOS існує магазин додатків App Store.

Переваги:

– Захищеність - гаджет на платформі iOS складно заразити вірусом або вивести з ладу через незнання;

– Хмарне зберігання даних, автоматичне збереження резервних копій - перший варіант допускає спільне використання файлів на всіх пристроях Apple,

другий убезпечить від втрати всіх призначених для користувача даних в разі поломки або крадіжки гаджета;

– Економність - Apple гарантує тривалий час автономної роботи навіть при високому рівні завантаженості апарату;

– Відсутність програмних збоїв - немає зависань і дивацтв у поведінці; висока швидкість роботи;

– Висока якість софта і продуманість. До того ж, компанія Apple займається оновленням заліза в своїх пристроях з періодичністю в 1-1.5 року;

– Якісна робота в бездротових мережах - апарат автоматично перемикається з мобільної передачі даних на Wi-Fi, і навпаки; відсутність налаштувань;

Недоліки:

– Неможливість заміни або видалення стандартних додатків;

– Закритість файлової системи - неможливість прямої перекидання файлів в Apple iPhone, iPod і iPad, відсутність можливостей для повного оглядача вмісту;

– Обмеженість використання софта - формула «один поштовий клієнт - один браузер - один магазин додатків» подобається далеко не всім користувачам;

– Ціни -то, що всі додатки для iOS є платними, ні для кого не новина, просто платити за якість готові не всі.

У iOS є активна функція «антизлодій», що дозволяє надійним чином захистити і зробити ваш iPhone значно менш привабливими для злодіїв. За допомогою Activation Lock в зв'язці з сервісом Find My iPhone можна легко встановити місцезнаходження зниклого гаджета і віддалено заблокувати доступ до нього. Причому, це блокування неможливо зняти при перепрошивки, поки не введёшь Apple ID і пароль. Віруси для iOS існують в невеликій кількості, пояснюється декількома факторами:

– незацікавленістю хакерів в користувачів Apple-пристроїв в силу їх відносно невеликої кількості в порівнянні з власниками гаджетів на Android;

– невеликою кількістю вразливостей в самій операційній системі;

– жорсткої професійної політикою компанії щодо дозволеного до публікації в App Store мобільного контенту.

– захистити iPad або смартфон від вірусів досить просто. Для цього необхідно всього лише слідувати декільком нескладним правилам: регулярно оновлювати антивірус, завантажувати програми тільки з офіційного магазину, не переходити за посиланнями, розташованих у прибуваючих на пошту від невідомих відправників листах.

2. Операційна система Android

Сьогодні найбільш поширеною операційною системою мобільних пристроїв є Android. Перша версія операційної системи вийшла в 2008 році, після чого сталося кілька оновлень системи, яку використовують більшість виробників смартфонів і планшетів. Крім смартфонів і планшетів під управлінням ОС Android працюють і інші пристрої: електронні книги, нетбуки,

наручний годинник і навіть телевізори і окуляри (Google glass).

Android заснована на базі операційної системи Linux і розробляється Open Handset Alliance за підтримки Google. Вихідний код знаходиться у відкритому доступі, завдяки чому будь-який розробник може створити свою версію цієї мобільної ОС. Розробникам додатків висунуто невелику кількість обмежень, завдяки чому існує безліч як платних, так і безкоштовних додатків, які можна зручно завантажити з Android Market.

Переваги:

– Завдяки відкритому вихідному коду будь-хто може створити свій додаток, тому якщо ви вирішите вибрати для свого планшета спеціальні програми або закачати ігри для Android, то знайти їх не складе ніяких труднощів. Для цього існують спеціальні сайти, а для реєстрації досить мати аккаунт Google;

– Особливістю даної системи є абсолютне рівноправність всіх додатків - і вбудованих, і встановлених користувачем. А вибір програми за замовчуванням здійснюється простим натисканням кнопки настройки. Така гнучкість практично недоступна іншим ОС;

– ОС багатозадачна, відрізняється високою швидкодією і зручною інтеграцією з сервісами Google;

– Можливість встановлювати додатки без інтернет-підключення; є голосове управління Google Now;

– Особливу увагу приділено безпеці особистої інформації. Для цього всі додатки запускаються в окремій області пам'яті і на своїй віртуальній машині.

– Є хмарне додаток Google Drive, місця хмарі надається 15 Гбайт.

– Недоліки:

– Безліч актуальних версій - для багатьох пристроїв нова версія входить занадто пізно або не виникає зовсім, тому розробникам доводиться розробляти програми, орієнтуючись на більш старі версії;

– Висока схильність до хакерських атак через відкритості коду; висока витрата батареї;

– У більшості випадків вимагає доопрацювань.

3. Операційна система Windows Mobile

Windows Mobile (WM) - це сімейство мобільних операційних систем, розроблених Microsoft, та орієнтованих на мобільні пристрої. Windows Phone була випущена 2010 року і є наступником WindowsMobile, хоч і несумісна з нею, з повністю новим інтерфейсом.

На відміну від попередньої системи, Windows Phone більшою мірою орієнтований ринку споживачів, ніж корпоративну сферу. Нова операційна система Windows 10 для мобільних пристроїв отримала назву Windows 10 Mobile, замість Windows Phone.

Переваги:

– Швидкість і плавність роботи інтерфейсу. Система не гальмує, вона вкрай чуйна і дуже приємна в роботі;

– Зручність і простота використання;

– Вбудовані і зручні у використанні пакет офісних додатків;
– Немає проблеми нестачі оперативної пам'яті. Навіть при невеликому обсязі оперативної пам'яті, системою можна комфортно користуватися. Якщо, звичайно, не ставити «важких» ігор і додатків;
– Через закритості системи - мала кількість вірусів;
– Список доступних форматів вельми обмежений;
– Багатий вибір додатків;
– Абсолютно закрита ОС, додатки тільки з MS Marketplace;
– Повільний розвиток платформи;
– Недоліки:
– Немає справжньої багатозадачності, додатки «заморожені» в тлі;
– Не у всіх версіях ОС можлива передача файлів через Bluetooth;
– Немає підтримки micro-SD;
– Ні файл-менеджера. Файлова система абсолютно непрозора;
– Контактні дані автоматично передаються в хмару, хочете ви цього чи ні;
– Неможливо встановити статичний IP в підключенні, і, отже, підключитися до ad-hoc мережі;
– Неможливо змінити розмір шрифту.
– Сильно обмежена можливість настройки.

Платформа може бути цікава в першу чергу таким категоріям користувачів: тим, хто потребує постійного використання офісних і корпоративних продуктів Microsoft; тим, хто хоче купити смартфон недорогий або середньої цінової категорії і отримати хорошу функціональність і автономність, нехай і на шкоду вибору програм.

Microsoft Office Mobile мобільний офісний пакет програм від Microsoft для Symbian OS, Windows Mobile, Windows Phone та Windows 10 Mobile. Він складається з Word Mobile, Excel Mobile, PowerPoint Mobile та OneNote Mobile. Office Mobile призначений для використання офісного пакету в дорозі або поза будинком.

Word Mobile (спочатку називалася Pocket Word) це текстовий процесор-програма з аналогічними функціями, що його настільний аналог, Microsoft Word. Програма має можливість базового форматування документів, а також зберігати документи в декількох форматах, включаючи формат ".rtf", ".doc", формат для читання на робочому столі версії Word. Дозволяє також вставляти картинки, списки та таблиці в документи. Крім того, Word Mobile включає перевірку орфографії, інструмент «Знайти» і команду «Замінити». Виноски, кінцеві виноски, заголовки, колонтитули, розриви сторінок, певне поглиблення списків, і деякі шрифти, в той час як шрифти, що не відображаються, не могли бути вставлені під час роботи над документом у Word Mobile, такі можливості зберігаються, якщо вихідний документ має їх.

Excel Mobile була однією з перших програм, включених до Office Mobile. Це таблиця-програма, яка сумісна з Microsoft Excel, і може створювати, відкривати, редагувати та зберігати у форматі .xlsx, і може читати документи,

збережені у форматі .xls. Excel Mobile дозволяє форматування осередків, основних розрахунків формул і створення діаграм та графіків. Крім того, воно підтримує фільтрацію даних. Параметри захисту, налаштування масштабування, налаштування автофільтра, форматування діаграми, приховані аркуші, а також інші функції не підтримуються в Excel Mobile, і будуть змінюватися під час відкриття та збереження.

PowerPoint Mobile є новою програмою у складі пакета. Вона призначена лише для перегляду презентацій, редагувати їх не можна. Працює практично без серйозних недоліків, відображаючи картинки та основну графіку. Великі файли завантажуються досить швидко.

OneNote Mobile дозволяє проводити базове форматування тексту, вставку новин, таких як фотографії або аудіозаписи, створення списків, а також використовувати гіперпосилання в документах. Фото- та аудіозаписи можуть бути взяті безпосередньо з програми за допомогою вбудованої камери та мікрофона відповідно.

Office Mobile інтегрується з OneDrive для «хмарних» послуг. Усі документи, відредаговані з програм Office Mobile, автоматично зберігаються в обліковий запис OneDrive, і список останніх документів, збережених у OneDrive, з'являється на головному екрані Office Hub. Office Mobile також включає файловий менеджер, який може використовуватися для перегляду файлів Word, PowerPoint або Excel, збережених на OneDrive. Крім того, у Office Mobile можна також відкривати та редагувати документи, збережені на обліковому записі Office 365.

4. Операційна система Symbian

Операційна система, яка використовується в смартфонах і комунікаторах. Symbian OS (Сімбіан) розробляється і просувається консорціумом Symbian. Консорціум Symbian був заснований в червні 1998 року такими компаніями як: Nokia (47,9%), Psion, Ericsson (15.6%), Motorola. Трохи пізніше до цього консорціуму приєдналися такі компанії виробників смартфонів як: Sony Ericsson (13.1%), Siemens, Panasonic, Fujitsu, Samsung, Sony, Sanyo. OS написаний практично цілком на C ++, але є підтримка Java. Переваги даної системи:

– Головне достоїнство: вона призначалася саме для мобільних пристроїв і їх не сильно високих технічних потужностей;
– Система не сильно завантажує пам'ять і центральний процесор;
– Зручне управління файлами;
– Реалізована така корисна функція, як звільнення пам'яті, якщо програма вже не використовується;
– Висока стабільність операційної системи.
– Недоліки:
– Для зв'язку з ПК необхідно встановлювати драйвера;
– Дуже часто після виходу нової версії Symbian OS, смартфон не завжди поєднується зі старими програмами;

– Телефон з такою операційною системою часто гальмує через установки великої кількості програм.

5. Операційна система BlackBerry

Операційна система працює виключно на пристроях, що випускаються компанією Research In Motion Limited (RIM). Орієнтована на корпоративних користувачів. Смартфони з цією операційною системою набули поширення в корпоративному середовищі, завдяки складності перехоплення повідомлень.

Переваги:

– Гнучкість меню налаштувань;

– При першому включенні будь-якого пристрою запропонують переглянути невеликі підказки, які навчать управляти смартфоном;

– Зручне управління додатками, в тому числі і неактивними;

– Крім стандартних способів блокування, пристрій можна убезпечити за допомогою "Picture Password". Це унікальний, безпечний і в той же час геніальний спосіб;

– Можливість і простота підключення до різних сховищ даних;

– Підтримка великої кількості кодеків і форматів (практично всіх);

– При вхідному дзвінку, крім основної інформації, можна налаштувати додаткову про абонента;

– Можливість синхронізації з принтером для друку;

– Вбудований пакет офісних додатків;

– Окремо варто сказати про Менеджері паролів. Раніше була вбудована в прошивку всіх Blackberry, що давало можливість після перепрошивки відновитися з резервної копії без зайвих проблем. Зараз це окремий додаток з тим же функціоналом: зберігання паролів під паролем;

– Зручний магазин додатків;

– Підтримує роботу з Android-додатками;

– Є функція Blend для роботи з телефонами з ПК або планшета;

– Відмінна реалізація пошти;

– У версії BlackBerry 10 систем аналізує стиль набору тексту у користувача і адаптується до нього, це відбувається дуже швидко.

Недоліки:

– Немає зв'язків з популярними мессенджерами, а значить, відправити повідомлення з меню контакту можна, потрібно запускати окремий додаток;

– Відсутність синхронізації з настільним браузером;

– Відсутність автоматичних оновлень додатків.

6. Мови програмування мобільних додатків

Найпопулярніші мови програмування у 2022 році:

PHP.

JavaScript / JS.

Java / Ява

Python.

C++

C # або CI Шарп
Visual Basic.
SQL.

На сьогоднішній день існує близько 10000 мов програмування. Так, їх дуже багато. Деякі з них використовуються в обмеженому колі людей, наприклад серед розшукуваних хакерів. Деякими мовами дуже зручно писати ігри. Щось підходить для створення ПЗ у медичних закладах. Деякі мови на кшталт Pascal викладаються у ВНЗ України просто тому, що так прийнято і неважливо – будете ви його використовувати потім чи ні. Мови програмування можна порівняти зі звичайними мовами, яких теж налічується чимало – близько 7000. Парадокс, але мов програмування більше, ніж звичайних.

1. PHP. Мова програмування, за допомогою якої створюються веб-ресурси – сайти, CMS. Взяти наприклад WordPress – це система управління контентом (CMS), яку використовують ⅓ всіх сайтів в інтернеті. WordPress написано на PHP. Facebook до речі теж… і таких масштабних прикладів дуже багато.

Рівень затребуваності більший, ніж високий. PHP дуже простий для освоєння. Можна сказати, цю мову програмування можна вчити першою – вона просто ідеально створена для знайомства з цією сферою. Але… давайте тепер поговоримо про недоліки. Ми з Вами знаходимося в 2022 році і те, що Facebook був написаний на PHP, говорить звичайно про авторитетність мови, але коли це було. Все змінюється і деякі речі старіють. PHP не є винятком. Взяти, наприклад, індекс TIOBE. Як можна бачити на січень 2022 рік, PHP вже на 11 місці, хоча в 2021 був у ТОП 8. Це джерело досить достовірно описує світову ситуацію щодо затребуваності.

Суть у тому, що створення чогось нового на PHP практично ніхто не практикує. У даній мові є деякі проблемні моменти, зокрема, неоднорідний синтаксис (PHP розробник може тупо не зрозуміти, що написав інший PHP розробник). Так як ця мова легка для освоєння і вона вже не модна або застаріла, то і заробітки тут не дуже, в середньому – $1000. Якщо говорити про західні ринки, то цифра звичайно більша, але вона все одно не співставна з програмістами іншого класу.

2. JavaScript / JS. Це модно, це круто, це тренд. За останні 5 років ДжаваСкрипт має таку динаміку розвитку популярності, як жодна інша мова. На ньому можна написати – веб-сайти, мобільні програми, серверну частину та ще купу всього іншого. Освоївши JS ви можете стати Фронтенд розробником, Бекенд розробником, Фулстек спеціалістом – це найпопулярніші на сьогоднішній день спеціальності в IT. Докладніше про те, що таке фронтенд, фулстек та інші незрозумілі слова можете почитати в нашій статті про – план вивчення JS.

Для новачка мова ДжаваСкрипт буде такою ж легкою, як і PHP. Заробітки тут у середньому – $3000. Знаючи тенденцію старіння всіх мов, можна з упевненістю сказати, що JS буде ще в тренді щонайменше 5 років, а далі вангувати не станемо. Як таких недоліків у JS немає. Не дарма ж наша IT-школа Lemon School у Києві запустили курси з ДжаваСкрипту. Після них легко

можна стати програмістом, влаштуватися в будь-яку ІТ компанію і добре заробляти навіть на старті.

3. Java / Ява. Не потрібно плутати цю мову із JavaScript. Загальних коренів у них немає, а така назва вийшла в результаті угоди Netscape та Sun Java. Загалом це суто рекламні проблеми, а не те, що мова Java був прабатьком JS.

Java це мова загального призначення. Що таке мова програмування загального призначення? Якщо по простому, то за допомогою неї можна написати ПЗ під будь-що – наприклад, обслуговувальну систему в банках. Якщо говорити про веб-ресурси, то яскравими прикладами може бути бізнес мережа – Linkedin або пошуковик Yahoo.

Чи підійде Java для новачків? Ні… Це не те, з чого треба починати, але якщо говорити про потрібність цієї мови, то вона впевнено поки що тримається в ТОП-3.

4. Python. Пітон чи Пайтон – високорівнева мова програмування. За допомогою цієї мови можна написати навіть інші мови програмування – ось така ось міць! Хтось вважає Python легким для освоєння, хтось ні. У школах вже до нього привчають дітей. Так, якщо з дитинства вивчати базу, то потім вивчення цієї мови здасться легким, але якщо ви тільки вчора вирішили зайнятися програмуванням і вибираєте першою мовою Пайтон, то … готуйтеся до складнощів.

За популярністю Пітон вже довгий час у ТОП 3 по світу. Це дуже і дуже потрібна мова програмування. Google розробники кодують саме на Python. ІІ розробки ведуться на Python. Саме програмісти Python отримують просто приголомшливу зарплатню, в середньому – $7000. Перспектива тут приголомшлива і протягом найближчих 10 років ця мова не застаріє точно!

5. C++. Якщо ви любите комп’ютерні ігри, то знайте, що вона розроблена саме на C++. Ця мова – дітище вже застарілої мови C, тому якщо ви її вчили, то C++ буде легко освоїти. Навчати з 0 буде складно, тому що синтаксис тут, ууу… голова лопається.

Крім ігор ця мова здатна створювати операційні системи та різні прикладні програми. Затребуваність величезна.

6. C # або СІ Шарп. Так само як і попередня мова, СІ Шарп бере своє коріння з мови C. Мова також універсальна. Зо допогою неї розробляються ігри та різне ПЗ для бізнесу. Microsoft працює здебільшого з ним, тому якщо захотіли працювати в цій компанії, то вчіть C#.

7. Visual Basic. Це спадкоємець такої фундаментальної мови як Basic. Саме Visual Basic заточений для програмування різноманітних додатків Windows. Не будемо тут довго зупинятись, оскільки затребуваність цієї мови потихеньку падає та її еволюція зупиняється.

Зараз Візул Бейсік звичайно входить у ТОП 10, але це не та мова, яку необхідно вивчати на самому початку шляху і навіть у його продовженні.

8. SQL. Ця мова програмування все ще вважається найкращою у питанні взаємодії з базами даних. Як працює ця мова? Грубо кажучи є масив даних всіх учнів школи, і ми хочемо знайти по цій базі даних усіх Пупкіних. Робимо запит

та вуаля – бачимо результат. Щоб це все коректно працювало застосовується SQL. Як ви розумієте, баз даних є багато де і їх потрібно постійно оновлювати, модернізувати, тому роботи тут вистачає.

Мова SQL нескладна для освоєння і може підійти для новачка, але… ця мова специфічна і затребуваність у неї специфічна – тут попит значно менший за пропозиції.

9. Golang або GO. З'явилася мова в 2009 і представлена вона звичайно ж компанією Google. Вони зуміли її просунути до дуже авторитетного рівня. Хтось вважає Go краще, ніж Python. Десь він швидше і простіше, ніж Java. Загалом перспективи цієї мови величезні. Можливо через років 5 вона очолить ТОП 1, тому вчити її можна на перспективу, але для новачків мона буде важкуватою.

10. Assembler або мова Асемблера. Це мова низького рівня – це не означає, що вона крива чи нею не можна нічого написати. Просто синтаксис мови є максимально наближеним до розуміння самого комп'ютера. Це означає, що тут доведеться багато вчити, треба буде стати машиною.

Здавалося б навіщо взагалі потрібна ця складна мова? Потрібна ще й як! Код асемблера безпосередньо йде до процесора і пам'яті, а це означає, що швидкість виконання будь-якої операції дуже велика. Ця мова однозначно складна не те що для новачка, а навіть для досвідченого програміста. Є сфери, де Assembler на вагу золота, наприклад, коли ви хочете зламати чийсь сервер.

Яку мову програмування вибрати для вивчення новачкові?

Всі вищезазначені мови гідні вивчення в 2022 році і в наступних роках, в межах до 5 років. Якщо Ви новачок і збираєтеся вивчати програмування з нуля, рекомендуємо вибрати наступний шлях:

Почніть із Фронтенду – HTML/CSS + JS. Курси Front End є у нашій школі Lemon School. Тут ви вивчите верстку та базу мови програмування JS.

Для тих, хто не хоче вчити верстку, а відразу кинутися в чисте програмування, то рекомендуємо JavaScript та PHP.

Потім звичайно ж Java чи Python.

C++ чи C#.

Можна зупинитися на чомусь одному, а можна поетапно вчити все, бажано в тій послідовності, яку ми описали.

Такі мови програмування як – GO, Assembler, SQL, Visual Basic потрібно розуміти навіщо вчити. У вас має бути мета влаштуватись у якусь компанію, чи на якусь посаду. Просто так починати вчити ці мови – не найкраща ідея.

Топ-5 мов програмування для розробників мобільних додатків.

Java. З моменту появи Java стала основною мовою для розробки мобільних додатків на Android. Він забезпечує крос-платформену підтримку. Крім того, додатки на Java легко перенести на різні операційні системи. Програми Java працюють за принципом «Написано один раз, запускається всюди» (WORA – Write Once Run Anywhere) – вони будуть працювати однаково на будь-якому сумісному з Java пристрої без необхідності зміни коду. І хоча Java – відносно стара мову програмування, вона зберігає популярність.

Kotlin – це новітня мова програмування, повністю сумісна з Java. Ці дві

мови взаємозамінні. Минулого року Google назвав Kotlin «основною мовою для розробки додатків на Android». Серед переваг в порівнянні з Java варто відзначити масштабованість Kotlin.

Swift – мова програмування, розроблена Apple як сучасна заміна Objective-C, яка раніше використовувалася для створення додатків на iOS. Спочатку Swift призначалась для розробки на iOS, але тепер її можна використовувати для розробки додатків для macOS, Windows і Linux. Також доступні й неофіційні інструменти для додавання підтримки Android.

Rust – відносно нова мова, який вже стала відома своїми можливостями управління пам'яттю і безпекою. Як і Java, Rust має крос-платформену підтримку і може використовуватися для розробки мобільних додатків на Android, iOS, Windows, macOS, Linux і для ряду різновидів Unix. Rust підходить для розробки нативних і веб додатків, а також операційних систем, компонентів браузера та ігрових движків.

HTML5 також знаходиться в цьому списку, хоча і не є мовою для розробки мобільних додатків – він використовується для створення веб додатків, які запускаються на будь-якому пристрої через браузер. Програми, написані на HTML5, можна об'єднувати з фреймворками, які надають можливість використовувати API-інтерфейси та, зберігати при цьому всі функції веб додатку.

Висновки. Порівняння мобільних операційних систем за наступними параметрами.

Доступність пристрою. Найбільш доступним варіантом є пристрій під управлінням ОС Android. Найдорожчі пристрої компанія Apple. Над цією проблемою працює вже і Nokia, основним продуктом якої є смартфони Windows Phone.

Інтерфейс і дизайн. Взагалі дизайн Android і Windows Phone мало чим відрізняється один від одного. Але у Android краще якість призначеного для користувача інтерфейсу.

Додатки. Платформи iOS і Android мають в своєму розпорядженні приблизно однакову кількість додатків (більше мільйона). А платформа Window Phone в магазинах має тільки близько чверті мільйона додатків.

Магазини додатків. Всі платформи мають свої власні магазини, в яких і поширюються додатки на платній і безкоштовній основі.

Акумулятори. Час автономної роботи частенько стає тим фактором, на який звертають увагу користувачі в першу чергу. Більшість типів пристроїв забезпечуються досить ємними акумуляторами, але за рахунок недоопрацьованих операційних систем вони витрачають і пропорційну кількість енергії.

Системні оновлення. Оновлення з'являються регулярно як для Android, так і для Windows Phone. Це і локальні патчі, і великі поновлення, які виправляють досить кількість системних помилок. Але контроль над програмним забезпеченням в Microsoft ведеться набагато жорсткіше, ніж в Google. Для Window Phone поновлення, як і для інших операційних систем, виходять майже через кожні 2-3 місяці. Windows Phone в області оновлення

програмного забезпечення і перевершує Android.

Семінарське заняття № 3. Інструменти і середовища розробки мобільних додатків

Кількість годин: 2 год.

Навчальна мета заняття:

1. Придбання теоретичних знань з теми «Структура та компоненти мобільного додатку», розвиток здібностей до творчого мислення, формування навичок самостійної роботи з аналізу і узагальнення інформації, вміння проектувати компонентну архітектуру мобільного додатку.

Рекомендована література:

1. Dawn Griffiths, David Griffiths. Head First. Android Development. A Brain-Friendly Guide. O'REILLY. Beijing. Cambridge. Köln. Sebastopol. Tokyo.2015. 704 p.
2. Казимир В., Карпачев І., Усік А. Моделі системи безпеки ос android. URL: https://www.researchgate.net/publication/328775065_MODELI_SISTEMI_BEZPEKI_OS_ANDROID.
3. Конспект лекцій з дисципліни «Програмування для мобільних пристроїв». Укладачі: Готович В. А., Михайлович Т. В. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2020. 216 с.
4. Розробка застосувань для мобільних пристроїв. Конспект лекцій. Міністерство освіти і науки України ЗНТУ. Кафедра програмних засобів. Запоріжжя 2016. 62с.
5. Сайко В.Г., Казіміренко В.Я., Літвінов Ю.М. Мережі бездротового широкосмугового доступу. Навчальний посібник. Кив: ДУТ, 2015. 216 с.
6. Опорний конспект лекцій з курсу «Мобільні інформаційні системи». Тернопільський національний економічний університет. Факультет комп'ютерних інформаційних технологій. Тернопіль. 2016. 60с.
7. Соколов В. Ю., Бурячок В. Л., Тадждіні М. М. Безпека безпроводових і мобільних мереж. Київ, КУБГ, 2019. 130 с.
8. Шматко О. В., Поляков А. О., Федорченко В. М. Аналіз методів і технологій розробки мобільних додатків для платформи Android: навч. посіб. Харків : НТУ «ХПІ», 2018. 284 с.

Матеріально-технічне забезпечення: комп'ютерний клас.

Навчальні питання:

1. Призначення і типи інтегрованих середовищ розробки мобільних додатків.

2. Характеристика та порівняння типів додатків.

3. Інструменті розробки мобільних додатків.

1. ПОРЯДОК ПРОВЕДЕННЯ ЗАНЯТТЯ:

1.1. Проведення експрес-контролю готовності до заняття.

1.2. Ввести текст підготовленої програми і виконати її відлагодження.

1.3. Підібрати тести і виконати відпрацювання розробленого алгоритму на цих тестах.

1.4. Скласти звіт про виконану роботу і здати роботу викладачу.

1. Призначення і типи інтегрованих середовищ розробки мобільних додатків.

Важливою складовою в процесі розробки програмного забезпечення вважається вибір вірною IDE, що залежить не лише тільки від платформи, але і значення особистої підготовки. Інтегроване середовище розробки (ICP) (Integrated development environment-IDE) – це комплекс програмних засобів, який використовується програмістами для розробки програмного забезпечення.

Інтегровані середовища розробки були створені для того, щоб максимізувати продуктивність програміста завдяки тісно пов'язаних компонентів з простими користувацькими інтерфейсами.

Це дозволяє розробнику зробити менше дій для перемикання різних режимів, на відміну від дискретних програм розробки. Однак так як ICP є складним програмним комплексом, то середовище розробки зможе якісно прискорити процес розробки ПЗ лише після спеціального навчання.

ICP зазвичай являє собою єдину програму, в якій проводиться вся розробка. Вона, як правило, містить багато функцій для створення, зміни, компілювання, розгортання і налагодження програмного забезпечення. Мета інтегрованого середовища полягає в тому, щоб об'єднати різні утиліти в одному модулі, який дозволить абстрагуватися від виконання допоміжних завдань, тим самим дозволяючи програмісту зосередитися на вирішенні власне алгоритмічної задачі і уникнути втрат часу при виконанні типових технічних дій (наприклад, виклику компілятора). Таким чином, підвищується продуктивність праці розробника. Також вважається, що тісна інтеграція завдань розробки може далі підвищити продуктивність за рахунок можливості введення додаткових функцій на проміжних етапах роботи. Наприклад, ICP дозволяє проаналізувати код і тим самим забезпечити миттєвий зворотний зв'язок і повідомити про синтаксичні помилки.

Більшість сучасних ICP є графічними. Але перші ICP використовувалися ще до того, як стали широко застосовуватися операційні системи з графічним інтерфейсом – вони були засновані на текстовому інтерфейсі з використанням функціональних і гарячих клавіш для виклику різних функцій.

Середовище розробки включає в себе:

– текстовий редактор;

– транслятор (компілятор та/або інтерпретатор);

– засоби автоматизації складання;

– відладчик.

IDE – це не просто текстовий редактор. У той час як текстові редактори коду, такі як Sublime або Atom, пропонують безліч зручних функцій, таких як підсвічування синтаксису, настроюваний інтерфейс і розширені засоби навігації, вони дозволяють тільки писати код. Для створення функціонуючих додатків як мінімум потрібен компілятор і відладчик.

IDE включає в себе ці компоненти, як і ряд інших. Деякі з них поставляються з додатковими інструментами для автоматизації, тестування та візуалізації процесу розробки. Термін "інтегроване середовище розробки" означає, що надається все необхідне для перетворення коду в функціонуючі

програми.

С початку розробки програми необхідно визначитися: хто буде користувачем (цільова аудиторія); для яких пристроїв призначене це додаток;платформа, на якій додаток буде функціонувати. Розділяють наступні типи додатків: натівний додаток, веб-додаток, гібридний додаток.

2. **Характеристика та порівняння типів додатків**

Натівний додаток – це додаток, який розроблений на своїй (рідній) мові програмування для вибраної платформи (наприклад: objective-c для ios, java для android, c# для windows phone).

Причини використання:

- працюють швидше і стабільніше, ніж додатки іншого типу;
- дозволяють зняти функціональні обмеження браузерів з доступу до ресурсів пристрою.

Мобільна платформа (SDK - software development kit) надає інструментарій для розробників, який дозволяє отримати доступ практично до всіх сервісів пристрої, а також призначений для спрощення процесу створення додатків.

Веб-додаток - це додаток, розроблене на HTML, JavaScript, CSS (Cascading Style Sheets - каскадні таблиці стилів) і вимагає для свого виконання встановленого і налаштованого браузера мобільного пристрою з виходом в Інтернет. HTML застосовується для розмітки елементів інтерфейсу. CSS описує візуальну складову і взаємне розташування віджетів і елементів управління. Мова програмування JavaScript реалізує логіку програми.

Причини використання:

- можливість повного або хоча б часткового повторного використання коду на різних платформах;
- не пред'являють особливих вимог до графіку і використання апаратних засобів пристрою;
- є величезний вибір інструментів, фреймворків, які прискорюють і спрощують процес розробки;
- існування версії веб-сайту для настільного комп'ютера і є необхідність отримання доступу до через мобільний пристрій.

Гібридний додаток - це додаток, в якому частково використовується нативна функціональність, а частково - можливості веб-додатків. Від нативних додатків - можливість часткового доступу до ресурсів пристрою; від веб-додатків -підтримка HTML і робота в браузері.

Причини використання:

- можна поширити його відразу на безліч платформ;
- загальна продуктивністю і відгук інтерфейсу не є вирішальними;
- можливість поширення (публікації) як готового продукту або тимчасового замінника до виходу нативного додатки (запустити процес маркетингу).

На наступному слайді надана таблиця порівняння типів додатків за критеріями: доступ до ресурсів, доступ до Інтернет, установка, розповсюдження (Публікація), обновлення, платформи. Як видно більш додатків розробляється на крос-платформенної основі.

Природно, вибір засобів розробки залежить від призначення і складності додатку. Діаграма знизу показує, які середовища використовують розробники для роботи.

Середовища розробки дозволяють отримати повний доступ до можливостей операційної системи і компонентів телефону. Для створення програмного забезпечення вони використовують високопродуктивні мови програмування, саме тому вони дозволяють домогтися найвищої продуктивності, що критично для таких додатків, як ігри. Для різних платформ використовуються різні мови програмування:

– Для платформи Android використовується мова Java, проте можливо використовувати мови C / C ++, що дозволяє підвищити продуктивність на критичних ділянках коду;

– Для платформи iOS використовується мова ObjectiveC і Swift. Swift - нова мова програмування, представлений компанією Apple в 2014 році. Вона успадкувала більшість рис від ObjectiveC.

3. **Інструменті розробки мобільних додатків**

Як правило, розробка Android-додатків здійснюється на мові Java. Тому, в першу чергу, необхідно встановити Java Development Kit (JDK).

Java – це об'єктно-орієнтована мова програмування. Програми на Java транслюються в байт-код, що виконується віртуальною машиною Java, яка обробляє байт-код і передає інструкції обладнанню як інтерпретатор. Перевага подібного способу виконання програм полягає в повній незалежності байт-коду від операційної системи і устаткування, що дозволяє виконувати Java-додатки на будь-якому пристрої, для якого існує відповідна віртуальна машина. Іншою важливою особливістю Java є гнучка система безпеки завдяки тому, що виконання програми повністю контролюється віртуальною машиною. Будь-які операції, які перевищують встановлені повноваження програми (наприклад, спроба несанкціонованого доступу до даних або з'єднання з іншим комп'ютером) викликають негайне їх переривання. Слід зауважити, що фактично, більшість архітектурних рішень, прийнятих при створенні Java, було продиктовано бажанням надати синтаксис, схожий з C/C++. В Java використовується практично ідентичний синтаксис для оголошення змінних, передачі параметрів і операторів. Тому ті, хто вже має досвід програмування на C/C++, зможуть швидко освоїтися і почати писати Java-додатки.

JDK (Java Development Kit) – це безкоштовно розповсюджуваний комплект розробки додатків на мові Java, що включає в себе компілятор Java, стандартні бібліотеки класів Java, зразки коду, документацію, різні утиліти і систему Java Runtime Environment (JRE). До складу JDK не входить інтегроване середовище розробки IDE (Integrated Development Environment). Тому після того, як буде встановлено JDK, слід встановити IDE.

Android Software Development Kit (SDK) містить багато інструментів і

утиліт для створення і тестування додатків. Наприклад, за допомогою SDK Manager можна встановити Android API будь-якої версії (рис. 2), а також перевірити репозиторій на наявність доступних, але ще не встановлених пакетів і архівів.

Android Studio – комерційне середовище розробки під Android надає інтегровані інструменти для розробки і налагодження. Підтримувані мови: Ajax, ASP.NET, DHTML, JavaScript, JScript, Visual Basic, Visual C#, Visual C++, Visual F#, XAML та інші. Особливості :

- величезна бібліотека розширень, яка постійно збільшується;
- настроюється панель і закріплюються вікна;
- простий робочий процес і файлова ієрархія;
- статистика моніторингу продуктивності в режимі реального часу;
- інструменти автоматизації;
- легкий рефакторинг і вставка фрагментів коду;
- підтримка розділеного екрану;
- список помилок, який спрощує налагодження.

До недоліків можна віднести потрібні значні ресурси та складність використання.

Android Eclipse є найпопулярніше середовище розробки під вільне модульне інтегроване середовище розробки програмного забезпечення для різних мов програмування (Java, Python, Scala, PHP та ін.).

Intel XDK – середовище для розробки кросплатформних мобільних додатків; включає в себе інструменти для створення, налагодження та збірки ПЗ, а також емулятор пристроїв; підтримує розробку для Android, Apple iOS, Microsoft Windows 8, Tizen; підтримує мови розробки: HTML5 і JavaScript.

Intel Beacon Mountain – ще одне середовище розробки від компанії Intel. Надає всі інструменти, необхідні для проектування, розробки, налагодження та оптимізації додатків під Android.

Емулятор – це віртуальний мобільний пристрій, який запускається на комп'ютері. За допомогою емулятора можна розробляти і тестувати програми без використання реальних пристроїв.

До переваг використання емуляторів можна віднести простоту їх використання і низьку вартість. Розробнику не потрібно купувати величезну кількість пристроїв з різними характеристиками, щоб перевірити працездатність програми на різних смартфонах. Досить створити кілька емуляторів з необхідними характеристиками і запустити на них додаток. Стандартний емулятор, що поставляється разом з Android SDK, не влаштовує багатьох. Існують проекти, що підтримують розробку та розвиток альтернативних емуляторів.

Genymotion – швидкий емулятор Android. Він містить попередньо налаштовані образи Android, доступний для Linux, Windows і MacOS X. Genymotion є віртуальною машину з встановленою ОС Android, яку користувач

запускає так само, як і інші віртуальні машини. Проблема високого споживання системних ресурсів. В даний час активно розвивається.

Виділяють такі основні види додатків під ОС Android:

Додатки переднього плану, які виконують свої функції лише тоді, коли видимі на екрані.

Фонові додатки, які після налаштування не потребують взаємодії з користувачем а більшу частину часу перебувають і працюють в прихованому стані.

Змішані додатки, які більшу частину часу працюють у фоновому режимі, проте допускають взаємодію з користувачем і після свого налаштування.

Віджети – це невеликі додатки, які відображаються у вигляді графічного об’єкта на робочому столі.

Висновки. Нативний тип розробки все ще знаходиться на вершині, оскільки набір функцій платформи постійно оновлюється, що робить гібридну розробку складнішою.

Переваги нативних по відношенню до гібридних мобільних додатків - це краща продуктивність. Нативна розробка краще підходить для високо інтерактивних додатків з великою кількістю графіки та анімації або коли вміст потрібно швидко оновлювати. Тут ми маємо на увазі ігри, деякі типи соціальних мереж тощо. У випадку, якщо потрібні деякі ексклюзивні можливості, гібридна розробка може вимагати додаткових зусиль та консультації розробників мови платформи, щоб написати їх з нуля.

Гібриди з'явилися з метою пришвидшення розробки. Використання крос-платформ обмежується лише посібниками для мобільних платформ, які накладають свої конструкції та оновлення ОС. Велика перевага полягає в тому, що цей вид розробки дешевший. Гарно розроблений гібридний додаток не має видимих чи функціональних відмінностей для користувачів. Загалом же кінцевому користувачу не важливо як побудований додаток якщо він зручний та приємний у використанні.

Семінарське заняття № 4. Безпека мобільних застосувань

Кількість годин: 2 год.

Навчальна мета заняття:

1. Придбання теоретичних знань з теми «Структура та компоненти мобільного додатку», розвиток здібностей до творчого мислення, формування навичок самостійної роботи з аналізу і узагальнення інформації, вміння проектувати компонентну архітектуру мобільного додатку.

Рекомендована література:

1. Dawn Griffiths, David Griffiths. Head First. Android Development. A Brain-Friendly Guide. O’REILLY. Beijing. Cambridge. Köln. Sebastopol. Tokyo.2015. 704 p.
2. Казимир В., Карпачев І., Усік А. Моделі системи безпеки ос android. URL: https://www.researchgate.net/publication/328775065_MODELI_SISTEMI_BEZPEKI_OS_ANDROID.

3. Конспект лекцій з дисципліни «Програмування для мобільних пристроїв». Укладачі: Готович В. А., Михайлович Т. В. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2020. 216 с.
4. Розробка застосувань для мобільних пристроїв. Конспект лекцій. Міністерство освіти і науки України ЗНТУ. Кафедра програмних засобів. Запоріжжя 2016. 62с.
5. Сайко В.Г., Казіміренко В.Я., Літвінов Ю.М. Мережі бездротового широкосмугового доступу. Навчальний посібник. Кив: ДУТ, 2015. 216 с.
6. Опорний конспект лекцій з курсу «Мобільні інформаційні системи». Тернопільський національний економічний університет. Факультет комп'ютерних інформаційних технологій. Тернопіль. 2016. 60с.
7. Соколов В. Ю., Бурячок В. Л., Тадждіні М. М. Безпека безпроводових і мобільних мереж. Київ, КУБГ, 2019. 130 с.
8. Шматко О. В., Поляков А. О., Федорченко В. М. Аналіз методів і технологій розробки мобільних додатків для платформи Android: навч. посіб. Харків : НТУ «ХПІ», 2018. 284 с.

Матеріально-технічне забезпечення: комп'ютерний клас.

Навчальні питання:

1. Загрози мобільній безпеці
2. Найкращі методи захисту мобільних пристроїв
3. Шкідливі програми в мобільних пристроях
4. Моделі системи безпеки ОС Android

1. ПОРЯДОК ПРОВЕДЕННЯ ЗАНЯТТЯ:

1.1. Проведення експрес-контролю готовності до заняття.

1.2. Ввести текст підготовленої програми і виконати її відлагодження.

1.3. Підібрати тести і виконати відпрацювання розробленого алгоритму на цих тестах.

1.4. Скласти звіт про виконану роботу і здати роботу викладачу.

1 Загрози мобільній безпеці

Користувачі мобільних пристроїв все частіше піддаються зловмисній діяльності, головним чином щодо надсилання шкідливих програм на смартфони, які використовують мобільну ОС. Хоча Google і Apple пропонують розповсюдження різних видів атак:

– *Фішинг* у *додатку*: це один із способів зміни вихідного коду додатків та розповсюдження їх з допомогою фішингового сайту.

– *Компрометація ланцюжка поставок*: було помічено, що троянську версію законної програми було включено до заводської мікропрограми від невеликого виробника мобільних телефонів і доставлено клієнтам на абсолютно нових телефонах.

– *Код криптомайнера в іграх або утилітах*, якій запускатиметься незалежно від того, чи працює сама програма, і функціонує як постійна розрядка батареї телефону.

Реклама шахрайства за допомогою кліків, вбудована в програми: шахрайство з рекламою є однією з найприбутковіших злочинних компаній на сьогоднішній день, і мобільні програми є ключовою частиною цього хитрого злочину.

Також важливо згадати 10 найбільших ризиків для безпеки веб-додатків згідно з найвідомішою спільнотою безпеки в усьому світі під назвою OWASP Foundation. Пом’якшення цих загроз було б першим кроком у створенні безпечного коду мобільних додатків:

– Ін'єкція
– Порушена автентифікація
– Розкриття конфіденційних даних
– Зовнішні сутності XML (XXE)
– Порушений контроль доступу
– Неправильна конфігурація безпеки
– Міжсайтовий сценарій XSS
– Небезпечна десеріалізація
– Використання компонентів із відомими вразливими місцями
– Недостатня реєстрація та моніторинг

Звичайні віруси не були головною загрозою для смартфонів, ніж ПК. Частіше загрозою є просто фальсифікований код або несправні програми, які не розглядаються виробниками антивірусів, зосереджених на більш небезпечних і легко виявлених ПК-вірусах. Загроза також існує через втрачені/викрадені пристрої або випадкове/зловмисне використання кінцевими користувачами. Адміністратори часто не можуть віддалено перевіряти вміст смартфонів, як це передбачено Міжнародною організацією зі стандартизації (ISO) 27001вимоги безпеки.

Прогнозується, що світовий ринок інформаційної безпеки досягне $170,4 млрд у 2022 році; до найпоширеніших мобільних загроз можна віднести наступні:

– *Витік даних*: 71% порушень були мотивовані фінансовим аспектом, а 25% – шпигунством;
– *Зловмисне програмне забезпечення або зловмисне програмне забезпечення*: серед найбільш шкідливих вкладень електронної пошти є .doc і .dot, які складають 37%, а друге місце займає .exe;
– *Фішинг і соціальна інженерія*: 62% підприємств зазнали такого типу атак;
– *Перехоплення зв’язку*: хакери по всьому світу атакують кожні 39 секунд, тобто в середньому 2244 рази на день;
– *Викрадені та втрачені телефони*;

– *Поведінка користувачів*: 64% американців ніколи не перевіряли, чи постраждали вони від витоку даних;

– *Пряма хакерська атака*.

2 Найкращі методи захисту мобільних пристроїв

Загалом, виробники апаратного та програмного забезпечення окреслюють і просувають процедури та інструкції, які за правильного застосування мають підтримувати або підвищувати рівень безпеки. Хоча немає способу гарантувати 100-відсоткову безпеку, оскільки непередбачені вразливості можуть бути виявлені та використані зловмисниками, давайте поглянемо на деякі нещодавно розроблені найкращі практики для мобільних пристроїв і програм.

1) Зробіть автентифікацію користувача найвищим пріоритетом: більшість мобільних пристроїв можна заблокувати за допомогою блокування екрана та розблокувати за допомогою пароля, біометричного (наприклад, відбитка пальця та розпізнавання обличчя) або персонального ідентифікаційного номера (PIN). Сьогодні багатофакторна автентифікація вважається найкращою практикою для захисту даних користувача. Навпаки, безпека повністю базується на складності пароля та увазі користувача до його конфіденційності.

2) Оновіть мобільні операційні системи та вбудовані програми за допомогою патчів безпеки: підтримка операційної системи (Android та iOS) і встановлених програм є обов’язковою. І Google, і Apple надають користувачам регулярні оновлення, які усувають останні вразливості чи інші загрози, а також надають додаткові функції продуктивності та безпеки. Однак оновлення програми - це палиця з двома кінцями, оскільки новий випуск може зменшити його загальну продуктивність і продуктивність користувача.

З точки зору безпеки, оновлення можуть викликати процес облицювання для підтвердження перевірки безпеки. Щоб переконатися, що мобільний додаток відповідає вимогам безпеки організації вільний від уразливостей, серія суворих і проводяться комплексні аналізи. Треба пам’ятати, що перевірка програм також може включати оновлення зовнішні компоненти (наприклад, сторонні бібліотеки) і нові обов'язкові версії операційних систем.

3) Регулярно створюйте резервні копії даних користувача: резервне копіювання є основним методом запобігання втраті або видаленню даних. Розклад резервного копіювання слід адаптувати до збільшення даних з часом. Приклади даних користувача включають окремі файли користувача (документи та електронні таблиці), медіафайли (наприклад, зображення та відео), контакти та інші конфіденційні дані.

4) Використовуйте шифрування: шифрування даних перетворює дані в іншу форму або код, щоб лише авторизовані сторони можуть розшифрувати та прочитати ці дані. Функція шифрування використовується для даних, що зберігаються на мобільний пристрій, а також для передачі даних через мережі. Тим не менш, за замовчуванням шифрування потрібен пароль для шифрування та дешифрування даних файли. Якщо хтось забув пароль, відбувається відновлення даних зазвичай проблематично і не завжди успішно. Покладаючись на загальнодоступні рішення, користувач може просто заколисати помилкове відчуття незаперечна безпека. Більше того, ще й сильно

радимо не підключатися до загальнодоступних і використовувати їх незахищене місце Wi-Fi без використання безпечної опції передачі, наприклад віртуальної приватної мережі (VPN). У цьому випадку, порівняно зі звичайним підключенням до Інтернету, VPN все ще майже незмінно повільніше, залежно від відстані між сервер і клієнт, поточне завантаження сервера та застосований рівень шифрування.

5) Увімкнути віддалене видалення даних: якщо користувач має свої пристрій з конфіденційними даними вкрадено і є мало можливість отримати їх за відносно короткий проміжок часу, слід увімкнути можливість пристрою, яка дозволяє скинути заводські налаштування повідомлення для дистанційного виконання. Крім того, дистанційне видалення даних є обов'язковим у разі звільнення з роботи або зараження шкідливим програмним забезпеченням, яке неможливо видалити. Поки існуючі рішення є зрозумілими переваги, вони не є панацеєю від усіх для мобільної безпеки.

6) Вимкніть Bluetooth і Wi-Fi, коли вони не потрібні: мінімізація використання Bluetooth і Wi-Fi зменшує ризик використання вразливостей, хоча недоліки не в цих стандартах, а в них реалізації. Тут слід зауважити, що дія вимкнення вимагає навмисної взаємодії від користувача. Однак існують інструменти (наприклад, AutoBluetooth), які вмикають або вимикають Bluetooth без будь-якої взаємодії з користувачем, на основі правил, визначених користувачем.

7) Знати методи соціальної інженерії: соціальні інженерія - це термін, який охоплює широке спектр зловмисної діяльності, як-от фішинг, підказка, цькування,.. Завдяки цій орієнтації на людину пам'ятайте, що користувач має знати про шкідливість «актори», які беруть участь у атаках соціальної інженерії полювання на людську жадібність і невігластво.

Організації, зокрема аналітики безпеки, можуть також розгляньте можливість проведення тестів соціальної інженерії на проникнення (також відомих як тестування соціального пера) серед співробітників. За задумом, тестування соціального пера – це практика застосування шахрайства соціальної інженерії співробітників організації, щоб оцінити їх здатність надавати конфіденційну інформацію. Така оцінка є вигідною, оскільки дає реальну атестацію щодо рівня дотримання вимог компанії політики безпеки конкретних осіб.

8) Обов'язково не робіть джейлбрейк свого пристрою: джейлбрейк - це підвищення привілеїв з метою усунення програмних обмежень, накладених виробником пристрою. Іншими словами, розгортання серії патчів ядра надає root-доступ, який дозволяє інсталювати програмне забезпечення, яке недоступне та розповсюджується через магазин програм. Джейлбрейк може серйозно піддати операційну систему додатковим уразливостям, якими ефективно користуються зловмисники.

Слід також мати на увазі, що в разі зняття обмежень виробника гарантія на пристрій, швидше за все, буде анульована. Крім того, може статися зниження загальної стабільності системи оскільки програми з помилками, як правило, використовують значну кількість апаратних ресурсів.

9) Обов’язково не надавайте непотрібних дозволів додаткам: дозволи додатків – це привілеї, які має додаток, наприклад можливість доступу до периферійних пристроїв, таких як камера, список контактів або місцезнаходження. Поточні версії операційних систем мають різні варіанти залежно від виробника. Основним принципом є надання лише тих дозволів, які необхідні для належної роботи програми. Іншими словами, користувач повинен завжди використовувати принцип найменших привілеїв. Навпаки, надані дозволи можна описати як ключі, які розблоковують функціональність програми.

10) Установіть мобільні програми безпеки та антивірусні програми: оскільки за замовчуванням немає додаткового захисту, сканери мобільної безпеки та антивірусні програми в режимі реального часу захищають від шкідливих програм і вірусів, а також виявляють крадіжки, програми-вимагачі та криптомайнери. Крім того, деякі інструменти також можуть сканувати URL-адреси та блокувати небезпечні сайти, відстежувати посилання в текстових повідомленнях і забезпечувати батьківський контроль.

Безсумнівно, експерти настійно рекомендують використовувати такі інструменти, але нічого не дається безкоштовно. У їхньому випадку побічні ефекти стосуються додаткового розподілу апаратних ресурсів і збільшення розрядки акумулятора через процеси, що виконуються у фоновому режимі.

Звичайно, дотримання цих десяти найкращих практик не гарантує на 100 відсотків безпеку мобільного пристрою; однак він підвищить рівень безпеки, зменшивши вектор атаки та знизивши ризик збоїв у системі та неправильно сформованого запиту

3 Шкідливі програми в мобільних пристроях

Майже всі мобільні телефони завдають двох серйозних несправедливостей своїм користувачам: відстежують їх переміщення і прослуховують їх переговори.

Відстеження розташування користувачів – наслідок того, як працює стільникова мережа: їй потрібно знати, біля яких вишок знаходиться телефон, щоб зв'язуватися з телефоном через навколишню вежу. Це дає мережі дані про місцезнаходження, які вона зберігає на місяці чи роки. Прослуховування переговорів діє на основі універсального чорного ходу в програмі процесора, який зв'язується із мережею.

Відстеження розташування в мережі. Строго кажучи, це відстеження не реалізується конкретними частинами програм; це невід'ємна приналежність мережі. Мережа повинна знати, біля яких стільникових вишок знаходиться телефон, щоб спілкуватися з ним через вищу вежу. Технічно неможливо блокувати або уникати відстеження, користуючись мобільним зв'язком у сьогоднішніх стільникових мережах.

Мережі не обмежуються миттєвим користуванням цими даними. Багато країн (зокрема США та Євросоюз) вимагають, щоб мережа зберігала всі дані про місцезнаходження протягом місяців або років, і поки вони зберігаються, вони доступні для будь-якого застосування, можливого в мережі або необхідного державою. Це може спричинити серйозну небезпеку для

користувача.

Штати США, в яких заборонено аборт, говорять про те, щоб оголосити злочином поїздку до іншого штату з метою аборту. Вони могли б застосовувати різні форми відстеження розташування, у тому числі за допомогою мережі, щоб переслідувати бажаючих зробити аборт. Штат міг би виписувати ордери отримання цих даних, отже політика "конфіденційності" стільникового оператора мала б ніякого значення.

Мережі ніколи не повинні визначати місцезнаходження для викликів допомоги, крім випадків, коли ви викликаєте допомогу або є відповідна постанова суду. Для мережі має бути незаконно робити точне місцевизначення (таке, як необхідно для виклику допомоги), крім як для обробки виклику допомоги, а якщо мережа робить це незаконно, то від неї має бути потрібне оповіщення власника телефону письмово на папері, з вибаченням. Розроблено схеми мереж, які б не відстежували телефони, але застосування цих методів вимагало б як нових мереж, і нових телефонів.

Прослуховування переговорів. У комунікаційному процесорі майже будь-якого телефону є універсальний чорний хід, який часто застосовується, щоб змусити телефон передавати всі розмови, які він чує. Лазейки для прослухування знаходиться у «модемному процесорі», який відповідає за зв'язок із радіомережею. У більшості телефонів модемний процесор контролює роботу мікрофона. У більшості телефонів він може переписувати програми та в головному процесорі. Існують моделі телефонів, спеціально спроектовані, щоб мікрофон не контролювався модемним процесором і щоб він не міг змінювати програми в головному процесорі. Ласка в них є, але принаймні з її допомогою неможливо перетворити телефон на пристрій, що підслуховує. Універсальний чорний хід, очевидно, застосовується також, щоб змушувати телефони передавати навіть коли вони вимкнені. Це означає, що їх переміщення відстежуються, а можливо, включається прослуховування.

Телефони на базі Android, що фінансуються урядом США, поставляються з встановленими програмами реклами та лазівкою для примусової установки додатків. Програми реклами знаходяться в модифікованій версії основної програми конфігурування системи. Лазейка є скритною добавкою до програми, заявлене призначення якої полягає в тому, щоб бути універсальною лазівкою програм для пристроїв. Інакше кажучи, програма, призначення якої шкідливо, є секретне вторинне шкідливе призначення. Все це на додаток до шкідливих програм самої системи Android.

Дуже популярна програма, що знаходиться в магазині Google Play, містила модуль, написаний для того, щоб таємно встановлювати шкідливі програми на комп'ютер користувача. Розробники програми регулярно застосовували його, щоб змушувати комп'ютер отримувати по мережі та виконувати програми за їх бажанням.

Це конкретний приклад того, на що піддаються користувачі, коли вони працюють з невільними додатками. Вони ніколи не можуть бути повністю впевненими, що невільна програма безпечна. Телефони Xiaomi поставляються з універсальним чорним ходом для використання Xiaomi в процесорі для

додатків. Це додатково до універсальної лазівки у процесорі модему, якою може скористатися місцева телефонна компанія. У невільній бібліотеці Baidu, Moplus, є лазівка, за допомогою якої можна “надсилати файли на сервер”, а також примусово встановлювати програми. Вона застосовується у 14000 додатках Android.

У китайській версії Android є універсальний чорний хід. Майже у всіх моделях мобільних телефонів є універсальний чорний хід у модемі. Для чого компанії Coolpad довелося вводити ще один? Тому що цей чорний хід контролює компанія Coolpad.

Пристрої Samsung Galaxy під керуванням невільних версій Android поставляються з лазівкою, яка надає віддалений доступ до файлів, що зберігаються на пристрої.

Передбачається, що система Android запобігатиме витоку даних, виконуючи додатки в ізольованих пісочницях, але розробники знайшли шляхи доступу до даних за допомогою інших засобів, і користувач ніяк не може завадити їм це робити, оскільки як система, так і програми не вільні.

Цифрове керування обмеженнями, або “DRM”, означає функції, спроектовані для обмеження того, що користувачі можуть робити з даними на своїх комп'ютерах. Програма Android Netflix примусово використовує Google DNS. Це один із методів, які застосовують Netflix, щоб здійснювати обмеження за місцезнаходженням користувача, які диктуються кіностудіями.

Вразливість. Вбудований у програмі iOS браузер TikTok вставляє програми на JavaScript для запису дій користувача на зовнішні сторінки сайтів. Ці програми можуть відстежувати діяльність користувача, а також вилучати будь-які персональні дані, що вводяться на сторінках. У нас немає способу перевірити заяву TikTok про те, що ці програми є лише суто технічними цілями. Деякі з даних можуть легко зберігатися на серверах компанії і навіть передаватися третім сторонам. Це відчиняло б двері для широкомасштабного стеження, у тому числі з боку китайського уряду (з яким TikTok опосередковано пов'язаний). Є також ризик, що дані будуть викрадені зловмисниками та застосовуватимуться для організації зломів.

Вбудовані в додатки iOS браузери Instagram і Facebook працюють так само, як і TikTok. Головна відмінність полягає в тому, що Instagram і Facebook дозволяють користувачам заходити на сайти третіх сторін за допомогою їхнього основного браузера, в той час як TikTok робить це майже неможливим.

З 21 безкоштовних антивірусних програм під Android, які були випробувані дослідниками, вісім не змогли виявити вірус. Всі вони запитували небезпечні допуски або містили рекламні програми стеження, причому сім із них несли в собі більший ризик, ніж середня зі 100 найпопулярніших додатків під Android.

Siri, Alexa та всі інші системи голосового управління можуть бути взяті під контроль програмами, які відтворюють команди у нечутному людьми ультразвуковому діапазоні. Деякі телефони Samsung випадково надсилають фотографії людям, записаним в адресній книжці власника.

Багато пристроїв з Android можна взяти під контроль через їхню

підсистему Wi-Fi через помилку в невільних програмах Broadcom, під керуванням яких вона працює. ЦРУ використовувало існуючі вразливості в "розумних" телевізорах і телефонах, щоб скласти шкідливу програму, яка шпигунить через їх мікрофони та камери, причому вони виглядають так, ніби вони вимкнені. Оскільки програма шпигуна перехоплює сигнали, шифрування від цього не захищає.

У телефонах Samsung є прокол у захисті, що дозволяє встановлювати за SMS програми, що потребують викупу. У WhatsApp є особливість, яку описували як “чорний хід”, тому що вона може дозволити державі анулювати шифрування у цьому додатку. Розробники запевняють, що це не замислювалося як чорний хід, і цілком можливо це правда. Але залишається головне питання: чи це функціонує як чорний хід? Якщо програма невільна, ми не можемо перевірити це, вивчивши її.

"Розумні" іграшки "Мій друг Кейла" та i-Que можна контролювати за стільниковим телефоном; фізичний доступ цього не потрібен. Це дозволяє хакерам прослуховувати мову дитини і навіть говорити голосом самих іграшок. Це означає, що злодій може голосом іграшки попросити дитину відчинити двері, доки не бачить мама.

Помилка в невільній бібліотеці ASN.1, що застосовується на стільникових вежах, а також у телефонах та маршрутизаторах, дозволяє отримати контроль над цими системами.

В «інтелектуальному будинку» компанії Samsung є велика дірка безпеки; люди можуть отримувати несанкціонований віддалений контроль за ним. Samsung заявляє, що це "відкрита" платформа, тому за проблему частково відповідальні розробники додатків. Це, зрозуміло, вірно, якщо ці програми не вільні. Все, що називається "інтелектуальним", швидше за все, водитиме вас за ніс. Багато невільних програм платежів передають дані незахищеним чином. Однак ще гірше те, що у цих додатках платежі не анонімні. Багато програм для смартфонів застосовують небезпечні методи автентифікації при зберіганні ваших особистих даних на віддалених серверах. Це наражає на небезпеку таку особисту інформацію, як адреси електронної пошти, паролі, а також медичні дані. Оскільки багато з цих додатків невільні, важко, якщо взагалі можливо, дізнатися, які додатки піддаються цьому.

Додаток для запобігання «крадіжці особистості» (доступу до особистих даних), що зберігав дані користувача на спеціальному сервері, було вимкнено розробником цієї програми, який виявив пролом у захисті. Здається, цей розробник сумлінно захищає особисті дані від третіх сторін взагалі, але не може захистити ці дані від держави. Зовсім навпаки: передача даних чужому серверу, якщо ви шифруєте їх попередньо за допомогою вільних програм, підриває ваші права.

Перешкоди. У цьому розділі наводяться приклади мобільних додатків, що докучають або набридають користувачеві, а також занепокоєння. Ці дії подібні до саботажу, але слово “саботаж” для них занадто сильне. Програма WeddingWire зберігає назавжди весільні фотографії, передає дані іншим, не надаючи людям контролю за їхніми персональними даними. Додаток також

іноді показує користувачеві старі фотографії та записки, і користувачі теж нічого не можуть з цим зробити.

Телефони Samsung продаються з версією Facebook, яку не можна видалити. Facebook запевняє, що це заглушка, яка нічого не робить, але нам залишається тільки вірити їм на слово, і завжди є ризик, що програма буде активована при автоматичному оновленні.

Постачання програм, що захаращують пристрій з невільною операційною системою, - звичайна практика, але роблячи ці програми невидаленими, Facebook і Samsung (в числі інших) роблять ще один крок до захоплення пристроїв користувачів.

Маніпуляція. Додаток "народжуваності" Femm у таємниці є знаряддям пропаганди християн-наталістів. Воно насаджує недовіру до контрацепції. Воно ще й підглядає за користувачами, як і слід очікувати від невільних програм.

Саботаж. Нова програма, опублікована Google, дозволяє банкам і кредиторам дезактивувати людям пристрої з Android, якщо вони не вносять платежів. Якщо пристрій дезактивовано, його функції будуть обмежені найпростішими, такими як виклик екстрених служб або доступ до налаштувань.

Samsung змушує користувачів своїх смартфонів у Гонконгу (і Макао) користуватися публічним DNS у материковому Китаї за допомогою оновлення програм, випущених у вересні 2020 року, що приносить багато занепокоєння та проблем приватності.

У двадцяти дев'яти додатках «фото ретушування», які були колись на Google Play, були шкідливі функції, такі як крадіжка фотографій користувача замість «прикрашання» їх, нав'язування небажаної та часто шкідливої реклами користувачам, а також перенаправлення їх на шахрайські сайти, на яких вони крали посвідчувальну особистість. Більш того, інтерфейс користувача більшої їх частини був спроектований, щоб додаток було важко видалити.

Звичайно, користувачам слід видалити ці небезпечні програми, якщо вони ще цього не зробили, але їм слід взагалі обходити стороною невільні програми. Всі невільні програми пов'язані з потенційним ризиком, тому що немає простого способу дізнатися, що вони насправді роблять. Apple та Samsung навмисно знижують характеристики старих телефонів, щоб змусити користувачів купувати нові.

Стеження. Вище описана універсальна лазівка, яка є по суті у всіх мобільних телефонах і яка дозволяє перетворювати їх на штатні пристрої, що підслухують. Додаток Pinduoduo шпигунить за іншими програмами та захоплює над ними контроль. Він також встановлює додаткові шкідливі програми, які важко видалити. Канада оштрафувала компанію Tim Hortons за те, що її додаток, який відстежує рухи людей, дізнавався про такі речі, як де вони живуть, де працюють і коли відвідують магазини конкурентів. Компанія X-Mode, що торгує даними, придбала дані про місцезнаходження близько 20 тисяч людей, зібраних приблизно сотнею різних шкідливих додатків. Майже всі невільні оздоровчі програми накопичують дані користувачів, зокрема конфіденційну інформацію про стан здоров'я, ідентифікатори стеження, а також куки для відстеження дій користувача. Деякі з цих програм відстежують

користувачів відразу на кількох платформах. Програми TikTok збирають біометричні ідентифікатори та біометричну інформацію зі смартфонів користувачів. Компанія, що випускає програми, робить, що хоче, і збирає всі дані, які може.

Багато програм, розроблених різними компаніями для різних організацій, проводять відстеження розташування без відома цих компаній та цих організацій. Стеження насправді проводять деякі популярні бібліотеки. Незвичайно тут те, що розробник невільних програм А обманом змушує розробників невільних програм Б1…Б50 будувати платформи, на яких А завдає несправедливості кінцевому користувачеві. Програми Baidu викрито у зборі персональних даних, які можуть застосовуватися для довічного відстеження користувачів та ставити їх під загрозу. Під дію цих невільних додатків потрапляє понад 1,4 мільярда людей у всьому світі. Ці невільні небезпечні програми та інструменти стеження підривають недоторканність особистого життя користувачів. Дані, зібрані Baidu, можуть передаватися китайському уряду, це може бути небезпечним для людей у Китаї.

Більшість додатків шкідливі, але додаток кампанії Трампа, як і додаток кампанії Моді, особливо погано: він і допомагає компаніям підглядати за користувачами, і підглядає за ними саме. В додатку Байдена застосовується в цілому менш маніпулятивний підхід, але це не говорить нам, чи є в ньому функції, які ми вважаємо шкідливими, такі як надсилання даних, які користувач не просив надсилати явно.

Телефони Xiaomi повідомляють про багато дій користувача: запуск програми, перегляд каталогів, відвідування сайтів, прослуховування пісень. Вони надсилають і відомості, що ідентифікують пристрій. Інші невільні програми теж шпигуть. Наприклад, Spotify та інші ведмежі послуги трансляції заводять досьє кожного користувача і змушують користувачів ідентифікувати себе під час оплати. Forbes виправдовує ті самі провини, коли відповідальність лежить не на китайцях, але ми засуджуємо це незалежно від того, хто це робить.

Google, Apple і Microsoft (а ймовірно, і деякі інші компанії) збирають точки доступу та координати GPS людей (що визначає точне місце розташування людей), навіть якщо їх GPS відключено, без згоди людини за допомогою невільних програм, реалізованих у його смартфоні. Хоча якби вони просто питали згоди, це не обов'язково робило б це правомірним. Додаток Aliplay Health Code оцінює, чи є у користувача Covid-19, і повідомляє прямо ментам. Додаток ToToc, здається, є засобом шпигунства для правлячого режиму Об'єднаних Арабських Еміратів. Це могли б робити будь-які невільні програми, і це вагомий аргумент користуватися не ними, а вільними програмами.

Ай-потвори та телефони з Android, коли ними користуються для роботи, надають роботодавцям потужні можливості стеження та саботажу, якщо вони встановлюють свої програми на пристрій. Багато роботодавців вимагають цього. Для працівника це просто невільна програма, так само принципово несправедлива та небезпечна, як будь-яка інша невільна програма.

Програма Facebook відстежує користувачів, навіть коли вона вимкнена, після того, як обманом змусить надати застосунку широкі права доступу, щоб використовувати одну з його функцій. Деякі невільні програми для відстеження періоду, у тому числі MIA Fem та Maya, відсилають інтимні подробиці життя користувачів у Facebook. Відстеження того, хто отримує невільну програму, є різновидом стеження. Є невільна програма для юстування прицілу певної телескопічної рушниці. Якби програма була вільною, списку встановили б її не було.

Багато безпринципних розробників мобільних додатків продовжують знаходити способи обходу налаштувань користувача, норм та можливостей операційної системи, пов'язаних із захистом особистого життя, щоб збирати якнайбільше конфіденційних даних.

Таким чином, ми не можемо покладатися на правила проти шпигунства. На що ми можемо покладатися, це на контроль над програмами, з якими ми працюємо. Багато програм Android можуть відстежувати переміщення користувачів, навіть якщо користувач не дозволяє їм отримувати доступ до розташування. Це пов'язано з явно ненавмисною слабкістю в Android, що навмисно використовується шкідливими програмами. Незважаючи на те, що компанія Apple нібито стоїть на варті недоторканності особистого життя, у додатках iPhone є програми відстеження, які ночами відсилають особисті дані користувача третім сторонам.

Microsoft OneDrive, Mint компанії Intuit, Nike, Spotify, Washington Post, Weather Channel (власність IBM), служба оповіщення про злочини Citizen, Yelp та DoorDash. Але, мабуть, програми стеження є у більшості невільних додатків. Деякі з них надсилають дані, що ідентифікують особу, такі як відбиток телефону, точне розташування, адреса електронної пошти, номер телефону і навіть адреса доставки (у випадку DoorDash). Після того, як ця інформація зібрана компанією, неможливо сказати, для чого її використовуватимуть. BlizzCon–2019 накладала вимогу працювати з невільним додатком на телефоні, щоб отримати перепустку на захід. Ця програма - програма-шпигун, яка може заглядати в масу конфіденційних даних, у тому числі розташування користувача та адресну книжку. Він також майже повністю контролює телефон.

Дані, які збираються додатками спостереження за менструацією та вагітністю, часто доступні роботодавцям та страховим компаніям. Хоча дані “анонімізуються та підсумовуються”, їх легко відстежити до жінки, яка користується програмою.

Це призводить до шкідливих наслідків прав жінок на рівні умови праці та свободу приймати рішення про власну вагітність. Не користуйтеся цими програмами, навіть якщо хтось пропонує вам за цю винагороду. Не користуйтеся цими програмами, навіть якщо хтось пропонує вам за цю винагороду. Вільний додаток, який виконує більш-менш ту ж роботу, не шпигун за вами, можна отримати на F-Droid, і розробляється нова програма.

Багато телефонів на базі Android продаються з великою кількістю встановлених невільних програм, які отримують доступ до конфіденційних даних без відома користувача. Ці приховані програми можуть або надсилати ці

дані до себе додому, або передавати їх до програм, встановлених користувачем, які мають доступ до мережі, але немає прямого доступу до даних. Це призводить до масового стеження, над яким у користувача немає абсолютно ніякого контролю.

Ведмежа послуга MoviePass планує застосовувати розпізнавання осіб, щоб відстежувати напрямок погляду людей і стежити за тим, щоб вони не відкладали свої телефони і не дивилися убік під час роботи реклами і програм, що відстежують.

Дослідження показало, що 19 із 24 медичних додатків надсилають конфіденційні персональні дані третім сторонам, які можуть застосовувати їх для нав'язливої реклами чи дискримінації людей із поганим станом здоров'я.

Щоразу, коли програма запитує “дозволи” користувача, воно закопане за умов користування службою, які нелегко зрозуміти. У будь-якому випадку, “згоди” недостатньо, щоб виправдати стеження. Facebook запропонував зручну невільну бібліотеку для побудови мобільних додатків, яка також надсилає персональні дані в Facebook. Багато компаній побудували на ній додатки і випустили їх, очевидно, не усвідомлюючи, що всі персональні дані, які вони зберуть, вирушать і в Facebook. Це показує, що ніхто не може довіряти невільній програмі, навіть розробникам інших невільних програм.

База даних AppCensus містить інформацію про те, як додатки Android використовують персональні дані користувачів та зловживають ними. На березень 2019 року проаналізовано близько 78 тисяч додатків, з яких 24 тисячі (31%) передають рекламний ідентифікатор в інші компанії, а 18 тисяч (23% усіх додатків) пов'язують цей ідентифікатор з ідентифікаторами апаратури, тому скидання ідентифікатора не дозволяє.

Збір апаратних ідентифікаторів порушує правила Google. Але в Google про це ніби не знали, а коли їм повідомили, вони не поспішали з діями у відповідь. Це доводить, що правила платформи розробки фактично не перешкоджають розробникам невільних програм закладати шкідливі функції у їхні програми. У багатьох невільних програмах є запис усіх дій користувачів під час роботи з програмою.

Дослідження 150 найбільш популярних безкоштовних програм VPN у Google Play показало, що 25% з них не захищають особисте життя їхніх користувачів через витоки DNS. На додаток, 85% відрізняються необґрунтованим доступом або функціями у їхньому вихідному тексті — нерідко застосовуваними для нав'язливої реклами, які потенційно можуть бути використані для стеження над користувачами. Виявлено та інші технічні недоліки. Більше того, попереднє дослідження виявило, що в половині з 10 найпопулярніших додатків VPN політика конфіденційності не лізе в жодні ворота.

Програма Weather Channel зберігала розташування користувачів на сервері компанії. На компанію подали до суду з вимогою повідомляти користувачів, що програма робитиме з цими даними. Ми думаємо, що судовий процес торкається побічної проблеми. Що компанія робить із даними - питання другорядне. Головна несправедливість полягає в тому, що компанія взагалі

отримує ці дані. Інші погодні програми, у тому числі Accuweather та WeatherBug, відстежують місцезнаходження людей. Близько 40% безкоштовних програм Android повідомляють про дії користувача в Facebook. Нерідко вони надсилають "рекламний ідентифікатор" машини, щоб Facebook міг зіставити дані, які отримує від однієї і тієї ж машини через різні програми. Деякі з них надсилають до Facebook детальну інформацію про дії користувача в додатку; інші лише повідомляють, що користувач працює з цією програмою, але вже одне це часто дуже інформативно. Це стеження відбувається незалежно від того, чи має користувач обліковий запис Facebook. Додаток Facebook отримував “згоду” на те, щоб автоматично отримувати протоколи телефонних дзвінків з телефонів під Android, даючи неправильне уявлення про те, на що виходить “згода”. Деякі програми Android відстежують телефони користувачів, які їх видалили. Іспанська програма трансляцій футболу відстежує переміщення користувача і підслуховує через мікрофон. Таким чином, вони шпигуть у ліцензійних цілях.

Дослідники виявили, що 50% з 5855 перевірених програм Android підглядають і збирають інформацію про своїх користувачів. Виявилося, що 40% з цих додатків пліткують про своїх користувачів незахищеними каналами. Зверніть увагу, що дослідники могли розкрити лише деякі методи стеження у цих невільних додатках, на вихідний текст яких вони не мали змоги поглянути. Інші програми могли б підглядати іншими способами.

Це свідчить про те, що невільні програми загалом працюють проти своїх користувачів. Для захисту свого особистого життя і свободи користувачам Android потрібно позбутися невільних програм — як невільної системи Android, перейшовши на Replicant, так і невільних додатків, отримуючи їх з магазину F-Droid, в якому розміщуються тільки вільні програми і який виразно попереджає користувача, якщо в додатку є антифункції. Grindr збирає відомості про те, у яких користувачів результати тесту на СНІД є позитивними, і передає ці дані компаніям. Grindr не повинен мати стільки відомостей про його користувачів. Він міг би бути спроектований так, щоб користувачі передавали таку інформацію один одному, але не в базу даних сервера.

Додаток та ведмежа послуга moviepass шпигунить за користувачами навіть більше, ніж вони очікували. Воно записує, де вони подорожують до та після того, як підуть у кіно. Не піддавайтеся стеженню - платіть готівкою! Слідкуючі програми в популярних додатках Android широко поширені і часом дуже хитромудрі. Деякі програми стеження можуть спостерігати за фізичними переміщеннями користувача магазином, відзначаючи мережі WiFi.

Програми зі штучним інтелектом, що обмежують користування телефоном під час водіння, можуть відстежувати кожний ваш рух. Програма Sarahah вивантажує всі номери телефонів та адреси електронної пошти в записнику користувача на сервер розробника. 20 нечесних програм Android записували телефонні дзвінки та надсилали їх у вигляді текстових повідомлень та електронної пошти тим, хто стежить за користувачами.

Компанія Google не навмисне зробила, щоб ці програми шпигували; навпаки, вона вживала різних заходів, щоб запобігти цьому, і видалила ці

програми, коли з'ясувалося, що вони роблять. Отже, ми не можемо звинувачувати Google в тому, що ці програми шпигуни. З іншого боку, Google перепоширює невільні програми Android, а отже, поділяє відповідальність за несправедливість, яка полягає в тому, що вони невільні. Компанія також розповсюджує власні невільні програми, такі як Google Play, які зловмисні. Чи могла компанія Google запобігати шахрайству з боку програм докладніше? Ні для Google, ні для користувачів Android не існує систематичного способу перевіряти виконувані файли невільних програм, щоб зрозуміти, що вони роблять. У Google могли б вимагати вихідний текст цих програм і вивчати якимось чином вихідний текст, щоб визначати, чи вони роблять користувачам щось погане. Якби компанія робила це добре, вона могла б більш-менш запобігати такому підгляданню, крім випадків, коли розробники програми досить розумні, щоб перехитрити перевірку. Але оскільки Google сама розробляє зловмисні програми, ми не можемо довіряти Google наш захист. Ми повинні вимагати випуску вихідного тексту для публіки, щоб ми могли захищати одне одного.

Програми BART стежать за користувачами. Якщо програмні програми вільні, користувачі можуть гарантувати, що вони не стежать. Коли програма невільна, можна тільки сподіватися, що вона не стежить. За результатами одного дослідження, 234 програм Android відстежують користувачів, прослуховуючи ультразвук від маячків, розміщених у магазинах, або з телевізійних передач. Виявляється, Faceapp веде масу стеження, судячи з того, скільки доступу до персональних даних вимагає ця програма.

Користувачі позиваються до Bose за поширення шпигунської програми в навушниках. Саме програма записує імена звукових файлів, які прослуховують користувачі, а також унікальний серійний номер навушників. У суді звинувачено, що це робиться без згоди користувача. Якби програма писала дрібним шрифтом, що користувачі на це погоджуються, чи було б це прийнятно? Ні в якому разі! Закон повинен однозначно забороняти закладати у додатки будь-яке стеження. Пари програм Android можуть змовитися, щоб передавати особисті дані користувача на сервери. Дослідники виявили десятки тисяч пар таких програм.

Компанія Verizon оголосила про встановлення на вибір невільної програми пошуку, встановленої на деяких телефонах компанії. Програма буде передавати Verizon ті ж відомості про запити, введені користувачами, які зазвичай отримує компанія Google, коли користуються пошуковою системою.

В даний час програма визначається тільки на один телефон і користувач повинен явно дати згоду перед тим, як програма запрацює. Однак програма залишається шпигуном - програма-шпигун залишається програмою-шпигуном, навіть якщо вона "необов'язкова".

Програма редагування фотографій Meitu надсилає дані користувача до китайської компанії. Програма Uber відстежує переміщення клієнта до та після поїздки. Цей приклад ілюструє, чому "отримання згоди користувача" на стеження не дає адекватного захисту від масового стеження.

Нова програма Facebook, Magic Photo, сканує фотоколекції знайомих осіб

на ваших телефонах і пропонує вам передавати зняте вами зображення відповідно до тих, хто знаходиться в кадрі. Ця шпигунська функція, мабуть, вимагає доступу до будь-якої бази даних знайомих осіб, а це означає, що зображення, ймовірно, надсилаються на сервери Facebook і обробляються там за алгоритмами розпізнавання осіб. Якщо це так, жодні з зображень користувачів Facebook більше не конфіденційні, навіть якщо користувач не надсилав їх до цієї служби.

Facebook постійно підслуховує, щоб стежити за тим, що люди слухають або дивляться. Крім того, воно, можливо, аналізує переговори користувачів, щоб доставляти їм націлену рекламу. Додаток контролера тесту на вагітність може не тільки шпигувати за всілякими даними в телефоні та в облікових записах сервера, він може і замінювати їх. Такі програми, як програма стеження Symphony, підслуховують, які радіо та телепередачі програються поблизу. А також підглядають, що користувачі пишуть на таких сайтах як Facebook, Google+ та Twitter.

Більше 73% і 47% найпопулярніших програм Android та iOS відповідно надають особисту, поведінкову та місцевизначальну інформацію своїх користувачів третім сторонам. Згідно з Едвардом Сноуденом, агенції можуть брати під контроль смартфони, посилаючи приховані текстові повідомлення, які дозволяють включати та вимикати телефони, прослуховувати по мікрофону, витягувати дані про місцезнаходження з GPS, фотографувати, читати текстові повідомлення, історію дзвінків, пересування, а також перегляду Всесвітньої павутини, та читати список. Ці шкідливі програми спроектовані так, щоб не дозволяти себе виявляти.

Багато підприємств торгівлі публікують додатки, які просять дозволу шпигувати за власними даними користувача - нерідко найрізноманітнішими. Ці компанії знають, що користування телефоном-шпигуном виробляє у людей звичку погоджуватися майже на будь-яке підглядання. Телефони Samsung продають із програмами, які не можуть бути видалені користувачами і які надсилають стільки даних, що передача коштує користувачам досить дорого. Зазначена передача, небажана для користувачів і не затребувана ними, напевно повинна представляти того чи іншого стеження.

Дослідження 2015 показало, що 90% найпопулярніших безкоштовних невільних додатків під Android містило бібліотеки, які можна вважати бібліотеками стеження. Для платних невільних додатків ця величина становила лише 60%.

4 Моделі системи безпеки ОС Android

У галузі забезпечення безпечної та ефективної роботи мобільних застосувань функціональна та інформаційна безпека розглядаються як дві фундаментальні складові, що взаємодоповнюють одна одну. Одним з найефективніших способів отримання зловмисником доступ до конфіденційної інформації є обхід системи одноразової перевірки ОС Android . Одним із засобів підвищення надійності роботи є розробка моделей безперервного захисту.

Проблеми захисту ОС Android пов’язані з недосконалістю багатьох

факторів самої системної платформи ОС, що є зручною і ефективною для використання та інтеграції нових програмних платформ, але при цьому залишає доступ зловмисникам до функціональних вузлів та конфіденційних даних. Ключовою проблемою є необхідність активної взаємодії застосувань між собою на рівні “застосування - ОС Android”, що зумовлює потребу у побудові адекватних моделей прав доступу, та роботи застосувань для кожного додатку ОС Android.

Модель прав доступу. Прикладний програмний інтерфейс застосувань API є найбільш чутливим компонентом ОС Android, а його захист здійснюється через налаштування відповідної системи дозволів «Android Permission» [4]. Таким чином, критичні функції додатків у рамках даної системи мають бути включені через підтвердження запиту на доступ до AndroidManifest.xml. Але ефективність захисту, що базується на системі дозволів, має певні обмеження. При базовому підході, характерному для «Android Permission», здійснюється одноразова перевірка роботи застосування (single-point check), яку зловмисне програмне забезпечення (ПЗ) може обійти і надалі передавати конфіденційні дані за допомогою викликів API без будь яких обмежень.

Для побудови системи безпеки ОС Android пропонується використовувати моделі захисту, що здійснюють безперервний аналіз ПЗ. Основою такого підходу має бути аналіз дозволів на основі латентно-семантичної індексації (LSI: Latent Semantic Indexing).

На сьогоднішній день LSI можна вважати стандартною методикою пошуку інформаційних блоків, у якій для визначення найбільш релевантного набору файлів та текстових документів використовуються ключові елементи коду та слова. Методика спирається на обчисленні матриці, у якій рядки задаються елементами коду та словами, а стовпчики - файлами та документами. При пошуку релевантних файлів та документів матриця зменшується за допомогою методу сингулярного розкладу (SVD: Singular Value Decomposition). Так, наприклад, у рамках задачі пошуку зловмисного ПЗ необхідно провести аналіз на відповідність відомим сигнатурам загроз списків дозволів у файлах XML. Запити формуються на основі списку небезпечних дозволів, після чого вектор запиту використовується для ранжування застосувань. Аналіз списків дозволів у файлах XML має певну специфіку по відношенню до аналізу текстових файлів тому процедура застосування методики LSI має бути визначена згідно особливостей поставленої задачі. На рисунку 1 наведена схема аналізу дозволів ПЗ Android, що базується на LSI.

Алгоритм аналізу дозволів, що працює за даною схемою, складається з таких етапів:

– визначення переліку аномальних додатків для подальшого аналізу їх лістингу за методикою LSI;

– класифікація даних застосувань у відповідності до переліку дозволів;

– включення дозволів у масив ключових слів LSI;

– побудова двовимірної матриці M, стовпчики якої складаються з набору аномальних додатків, а рядки - з переліку дозволів (таким чином, елементи матриці визначають статистику доступу ПЗ до ресурсів ОС);

– застосування по відношенню до матриці M процедури SVD з метою зменшення її розміру та визначення найбільш релевантних до сигнатур зловмисного ПЗ застосувань та їх ранжування;

– визначення набору ПЗ, що підлягає подальшому аналізу та отримання для кожного з даних застосувань набору стандартних дозволів;

– якщо дозвіл на застосування не відповідає згаальному набору типових дозволів з найбільш релевантних категорій, ПЗ позначається як потенційно зловмисне і підлягає динамічному аналізу.

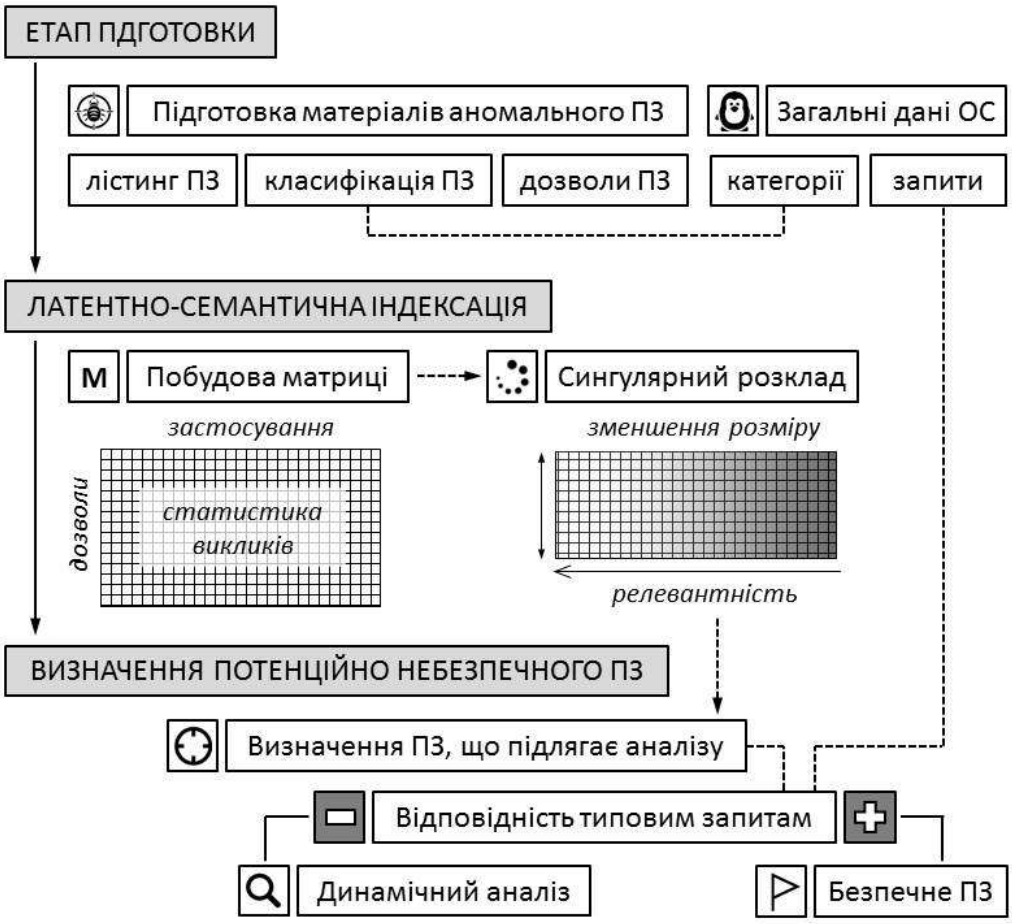


Рис. 1 - Схема аналізу дозволів ПЗ Android, що базується на LSI

Слід зауважити, що представлена схема є загальним алгоритмом забезпечення безпеки ОС Android. Вона не враховує те, що не всі потенційно небезпечні (ризиковані) дозволи викликаються застосуваннями. Тим більше, отримання ризикованого дозволу не характеризує застосування як однозначно зловмисний ПЗ. Але наявність ризикованого дозволу може призвести до хибного позитивного підтвердження. Щоб зменшити відсоток таких випадків необхідно перевірити програму у віртуальному емуляторі (sandbox) і ретельно

проаналізувати рівень його безпеки. Крім того, застосування методики LSI, включаючи формування терм документної матриці та використання сингулярного розкладу (метод SVD), також не є тривіальною задачею, тому для кожною конкретної задачі необхідно визначити актуальні підходи та показати процес аналізу.

Першим етапом аналізу дозволів на основі латентно-семантичної індексації є побудова терм-документної матриці M та вектору запитів q на її основі:

$$\begin{cases} M = [k * n] \\ q = [k * l] \end{cases}$$

де q - кількість дозволів, які відповідають термінам, n- кількість застосувань (що у рамках даної методики характеризуються файлами XML, які відповідають документам), а l — кількість викликів. Отже, множина дозволів p та множина застосувань a можуть бути визначені як:

$$\begin{cases} p = [p_1; p_k] \\ a = [a_1; a_n] \end{cases}$$

Сингулярний розклад зумовлює представлення терм документної матриці M у наступній формі:

$$M = V * S * \left(V^{-1}\right)^T,$$

де V — власний вектор матриці M, а S — діагональна матриця.

Наступним етапом обирається значення m, $m<n$, щоб зменшити розмірність матриці $M(k*n)$ до матриці $M_m(k*m)$. Аналогічно S_i обирається через зменшення розмірності S і вектору $V_m(m*m)$. Таким чином, кожному застосуванню a_i відповідатиме вектор-рядок v_i.

Тепер отримати апроксимоване значення меншої розмірності вектору запиту q_m можна через добуток трьох матриць:

$$q_m(m*l) = q * V_m * S_m^{-1}$$

Після цього можна визначити подібність елементів запиту та застосування через відповідну функцію $F(q_i, a_i)$. У відповідності до задачі нам необхідно застосувати міру подібності для дійснозначних векторів. Тому у рамках роботи пропонується використати коефіцієнт Отіаі-Баркмана:

$$F(q_i, a_i) = \frac{q_i \cdot a_i}{\| q_i \| \cdot \| a_i \|},$$

де $q_i \cdot a_i$ — скалярній добуток q_i і a_i, а $\| q_i \|$ і $\| a_i \|$ — їх потужності.

Для перевірки ефективності роботи алгоритму були використані статистичні дані сервісу Google Play та зразки інформаційного ресурсу «Android Malware Genome Project», ранжовані по категоріям «Розважальні сервіси» (відповідає категоріям «Games» і «Entertainment»), «Комунікаційні засоби» (відповідає категорії «Communication»), «Мультимедійні ресурси» (відповідає категоріям «Music & Audio» та «Media & Video») і «Десктоп-віджети» (відповідає категорії «Music and Video»). Для вказаних категорій можна отримати результати, наведені у табл. 1.

Таблиця 1 - Відсоток зловмисного ПЗ в залежності від категорії застосувань

Категорія ПЗ	**Відсоток ПЗ**	**Звичайне ПЗ**	**Зловмисне ПЗ**
Розважальні сервіси	85%	90%	80%
Комунікаційні засоби	10%	6%	13%
Мультимедійні ресурси	3%	2%	4%
Десктоп-віджети	2%	2%	3%

Зразки були розділені на зразки навчальної вибірки (80% від повної вибірки) та зразки для тестування методики LSI (20% від повної вибірки). Аналіз запитів на отримання дозволів дозволяє перевірити, у якій мірі пов'язані категорії застосувань та категорії запитів та як це співвідноситься з навчальною вибіркою. У даному прикладі, у зв’язку зі специфікою матеріалу, представленого для навчання системи захисту, співвіднесення відбувалося саме зі зразками зловмисного ПЗ, Тому до схеми, представленій на рис. 1, були внесені відповідні зміни.

Всі потенційно небезпечні запити на дозволи були віднесені, відповідно стандартній класифікації, до однієї з трьох категорій (рис. 2): конфіденційність (privacy), трафік (billing), робота ОС та ПЗ (system operation).

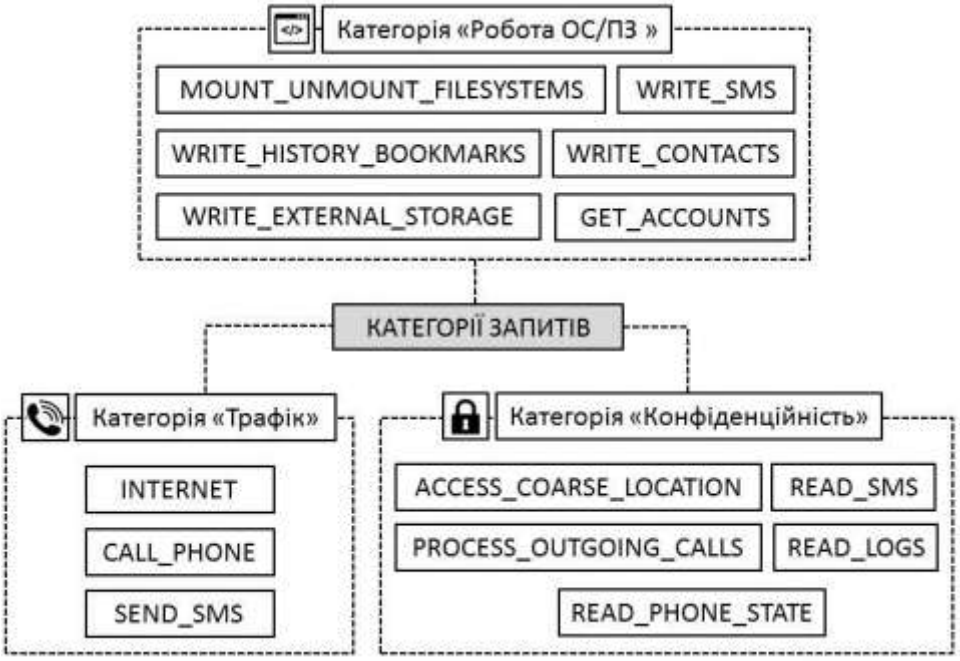


Рис. 2 - Категорії запитів з високим ризиком ОС Android

Найбільш репрезентативні результати тестування запропонованої моделі для даних трьох категорій представлені у табл. 2.

Таблиця 2 - Результати тестування LSI-моделі аналізу ПЗ ОС Android

Розважальні сервіси	Комунікаційні засоби	Мультимедійні ресурси	Десктоп-віджети	Відповідність результатів

88%	6%	3%	3%	84%
92%	5%	2%	1%	93%
94%	3%	2%	1%	98%

Тестування даної моделі показує, що ефективність статичного аналізу залежить від процентного співвідношення найбільш актуальних категорій (у даному випадку категорії «Розважальні сервіси») у навчальній виборці. Але, слід крім того зауважити, що в будь якому випадку залишається певний процент похибок другого роду, для відслідковування яких необхідно використовувати динамічний аналіз.

Модель роботи застосувань. Як показує тестування алгоритму аналізу дозволів на основі латентно-семантичної індексації, на ефективність статичного аналізу значною мірою впливає адекватність моделювання роботи застосувань та повнота відповідних статистичних даних, пов’язаних з використанням зловмисним ПЗ окремих категорій запитів. Для розробки цілісного методу необхідно побудувати узагальнену модель роботи застосувань, залучити до розгляду статистичний аналіз використання запитів та побудувати класифікатор потенційних загроз.

У загальному виді результати аналізу застосувань на потенційно небезпечне ПЗ можна розподілити на чотири види найбільш типових показників (рис. 3):

– істинно позитивні, кількість яких визначається як TP (true positive);

– істинно негативні, кількість яких визначається як TN (true negative);

– хибно позитивні, або помилки другого роду, кількість яких визначається як FP (false positive);

– хибно негативні, або помилки першого роду, кількість яких визначається як FN (false negative);

На основі даних величин можна визначити такі показники, як кількість істинно позитивних рішень *TPR* (true positive rate), кількість хибно позитивних рішень *FPR* (false positive rate), а також точність передбачення позитивних значень *PPV* (positive predictive value) та точність передбачення негативних значень *FPV* (positive predictive value):

$$\begin{cases} TPR = \dfrac{TP}{TP + FN} \\ FPR = \dfrac{FP}{TN + FP} \\ TNR = \dfrac{TN}{TN + FP} \\ FNR = \dfrac{FN}{TP + FN} \end{cases}$$

$$\begin{cases} PPV = \dfrac{TP}{TP + FP} \\ FPV = \dfrac{TN}{TN + FN} \end{cases}$$

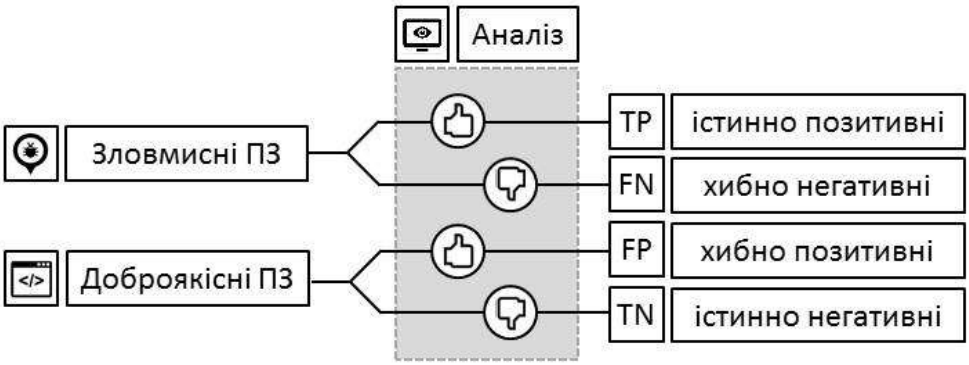


Рис. 3- Розподіл результатів аналізу за видами показників

Одним з найбільш ефективних методів перевірки результатів роботи та вдосконалення розробленої моделі аналізу застосувань ОС Android є Баєсів класифікатор, який відноситься до ймовірнісних класифікаторів та характеризується простим і компактним алгоритмом, що використовує мінімум апаратних ресурсів ОС, але при цьому характеризується високою точністю. Робота з даним класифікатором включає у себе фази навчання та тестування. На етапі навчання модель класифікатору отримує на вхід навчальну вибірку зразків доброякісного та зловмисного ПЗ для ОС Android. Надалі, під час тестування або роботи, модель виявляє належність застосування до зловмисного ПЗ, використовуючи дані, отримані під час навчання.

Для проведення ефективної класифікації необхідно визначити певну статистику отримання запитів на дозволи та API-викликів, приклад якої наведено на рис. 4.

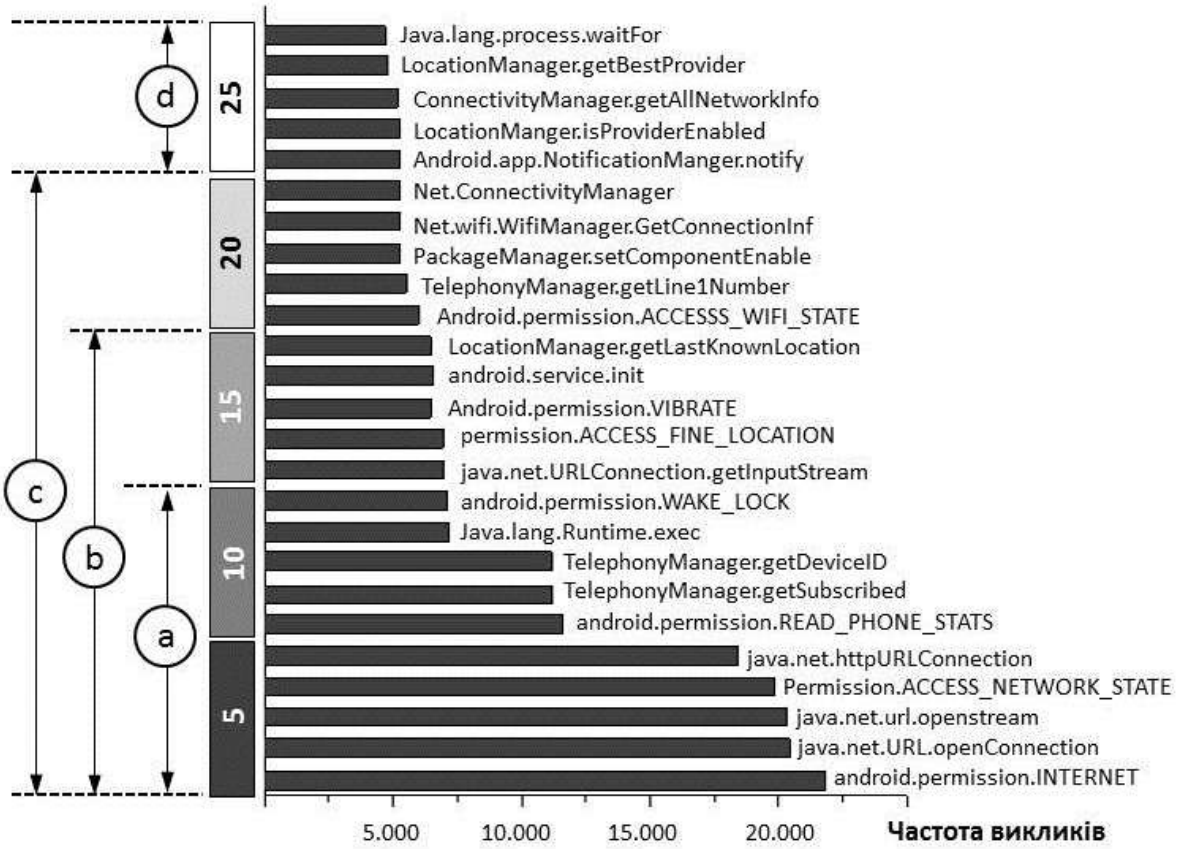


Рис. 4 - Статистика отримання запитів на дозволи ОС Android

У даному випадку запити було поділено на 10-ть тих, що найбільш активно застосовуються (група «a»), 15-ть тих, що найбільш активно застосовуються (група «b»), 20-ть тих, що найбільш активно застосовуються (група «c»), 5-ть тих, що найменш активно застосовуються (група «d»).

Для цих груп запитів були визначені відповідні показники: частота похибок та точність (відповідно, похибок першого та другого роду), відсотковий склад TNR, TPR, FNR, FPR, а також показники точності FPV і PPV (рис. 5 - 9).

Аналіз представлених графіків показує, що зі збільшенням групи збільшується точність аналізу та, відповідно, зменшується кількість похибок. Особливо різниця очевидна при порівнянні груп «a» і «d». В даному випадку різниця пов’язана не лише з розміром групи, а й з її актуальністю. Крім того, слід зауважити, що при тестуванні розроблених моделей на зразках, що знаходяться поза межами категорій, які використовувалися при навчанні, зменшується точність аналізу та, відповідно, збільшується кількість похибок.

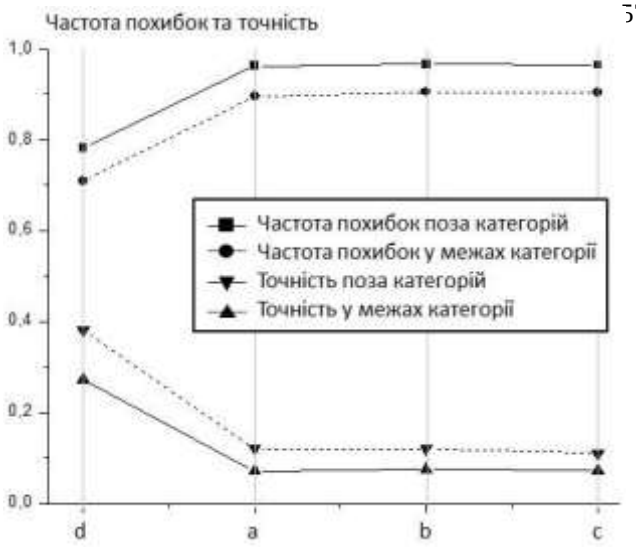


Рис. 5 - Частота похибок та точність аналізу

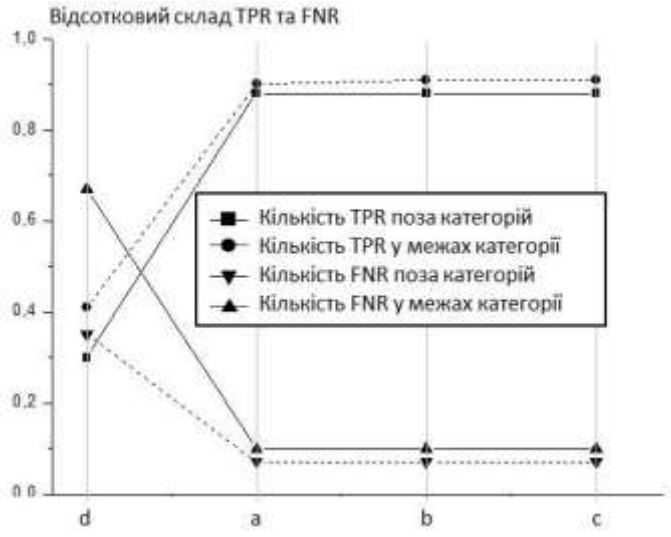


Рис. 6 - Відсотковий склад TPR та FNR

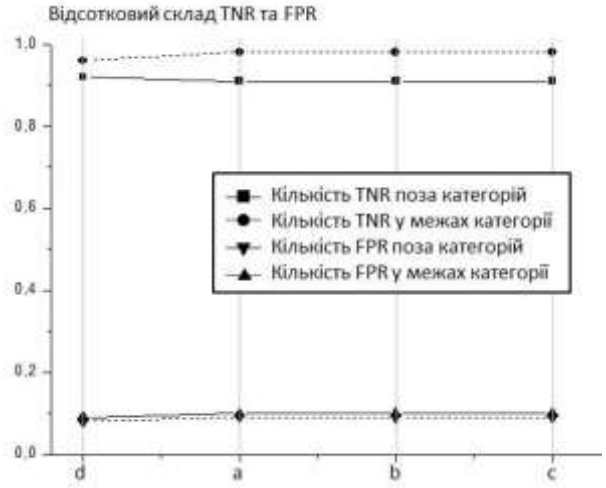


Рис. 7 - Відсотковий склад TNR та FPR

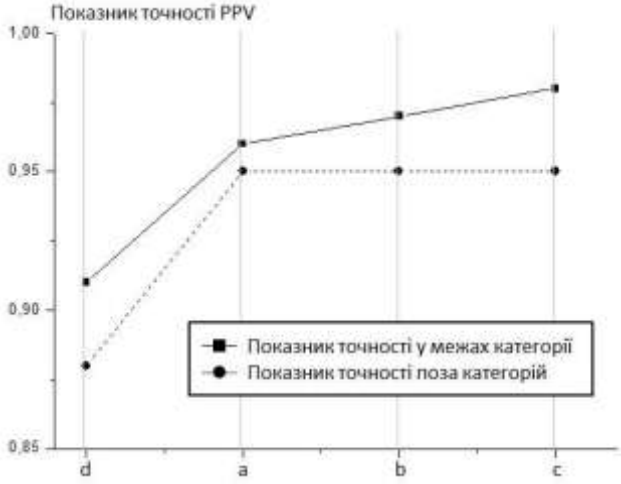


Рис. 8 - Показник точності PPV

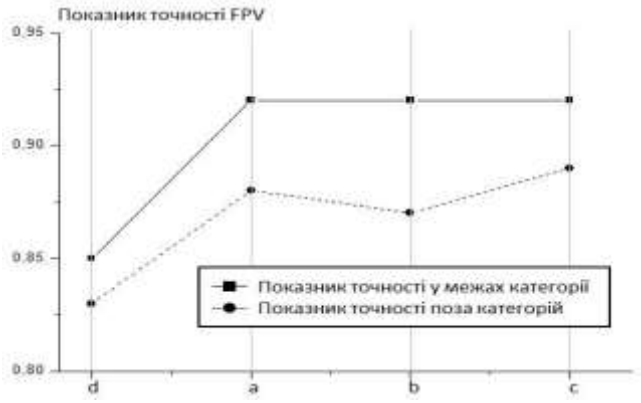


Рис. 9 - Показник точності FPV

Висновки. Безпека – це завжди гонка озброєнь між нападниками та захисниками. Іншими словами, безпека є питання балансу між ризиком і винагородою, захист проти зручності. З огляду на цю думку, потенційні ризики та вигоди, а також їхні компроміси, безсумнівно, заслуговують на подальшу і глибше дослідження. Результатом цієї лекції є цілісну картину цього явища, яка розглядає в негативні події, умови та обставини, які мають можливість

спричинити втрату активів та контрзаходи спрямовані на їх усунення та забезпечення належного та ефективного захисту для користувача.

Останні десять років позначають лише початок глобальної подорожі до кібербезпеки. Нові архітектури та співпраця все ще потрібні на порозі нової ери кіберзлочинності, яка буде посилена новими технологіями. - це три технології, а саме: мережі 5G та конвергенція інфраструктури, штучний інтелект і біометрія, будуть визначати наступні десять років глобальної кібербезпеки.

Запропоновані моделі при постійній перевірці дозволів, які використовуються застосуванням, значно зменшують негативний потенціал зловмисника. Але для забезпечення ефективної безпеки ОС Android необхідно визначити всі способи, за допомогою яких зловмисне ПЗ може асоціювати себе з завданням чи іншим застосуванням, що надає надмірні привілеї і становитиме потенційну загрозу. Це можливо лише через експериментальне вивчення способів управління ОС Android завданнями, що реалізується через дослідження процесу роботи системи за умови встановлення всіх можливих комбінацій перемикачів налаштувань платформи, які можуть вплинути на статус завдання. При цьому має здійснюватися аналіз додаткових привілеїв, які можуть бути отримані застосуванням, коли воно приєднується до завдання.

Семінарське заняття № 5. Месенджери миттєвого обміну повідомленнями та захист мобільних і хмарних обчислювальних середовищах

Кількість годин: 2 год.

Навчальна мета заняття:

1. Придбання теоретичних знань з теми «Структура та компоненти мобільного додатку», розвиток здібностей до творчого мислення, формування навичок самостійної роботи з аналізу і узагальнення інформації, вміння проектувати компонентну архітектуру мобільного додатку.

Рекомендована література:

1. Dawn Griffiths, David Griffiths. Head First. Android Development. A Brain-Friendly Guide. O'REILLY. Beijing. Cambridge. Köln. Sebastopol. Tokyo.2015. 704 p.
2. Казимир В., Карпачев І., Усік А. Моделі системи безпеки ос android. URL: https://www.researchgate.net/publication/328775065_MODELI_SISTEMI_BEZPEKI_OS_ANDROID.
3. Конспект лекцій з дисципліни «Програмування для мобільних пристроїв». Укладачі: Готович В. А., Михайлович Т. В. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2020. 216 с.
4. Розробка застосувань для мобільних пристроїв. Конспект лекцій. Міністерство освіти і науки України ЗНТУ. Кафедра програмних засобів. Запоріжжя 2016. 62с.
5. Сайко В.Г., Казіміренко В.Я., Літвінов Ю.М. Мережі бездротового широкосмугового доступу. Навчальний посібник. Кив: ДУТ, 2015. 216 с.
6. Опорний конспект лекцій з курсу «Мобільні інформаційні системи». Тернопільський національний економічний університет. Факультет комп'ютерних інформаційних технологій. Тернопіль. 2016. 60с.

7. Соколов В. Ю., Бурячок В. Л., Тадждіні М. М. Безпека безпроводових і мобільних мереж. Київ, КУБГ, 2019. 130 с.
8. Шматко О. В., Поляков А. О., Федорченко В. М. Аналіз методів і технологій розробки мобільних додатків для платформи Android: навч. посіб. Харків : НТУ «ХПІ», 2018. 284 с.

Матеріально-технічне забезпечення: комп’ютерний клас.

Навчальні питання:

1. Безпечний миттєвий обмін повідомленнями
2. Найбезпечніші месенджери повідомлень
3. Захист мобільних і хмарних обчислювальних середовищах

1. ПОРЯДОК ПРОВЕДЕННЯ ЗАНЯТТЯ:

1.1. Проведення експрес-контролю готовності до заняття.

1.2. Ввести текст підготовленої програми і виконати її відлагодження.

1.3. Підібрати тести і виконати відпрацювання розробленого алгоритму на цих тестах.

1.4. Скласти звіт про виконану роботу і здати роботу викладачу.

1 Безпечний миттєвий обмін повідомленнями

Сьогодні більшість соціальних мереж надають певну форму онлайн-повідомлень у реальному часі, користувачі дуже вимогливі. Мережі обміну повідомленнями повинні мати як мобільний, так і веб-доступ із розширеними можливостями, такі як медіа, голос або обмін інформацією про місцезнаходження, а також можливість побачити, чи контакт онлайн і доступний для чату.

Через характер цих додатків і більш приватний характер даних, якими обмінюються користувачі з точки зору величезного обсягу даних і з точки зору непридатності для публікації для широкого загалу, як в інших типах соціальних мереж, тому теми безпеки та конфіденційності є важливими в оцінці програм миттєвих повідомлень.

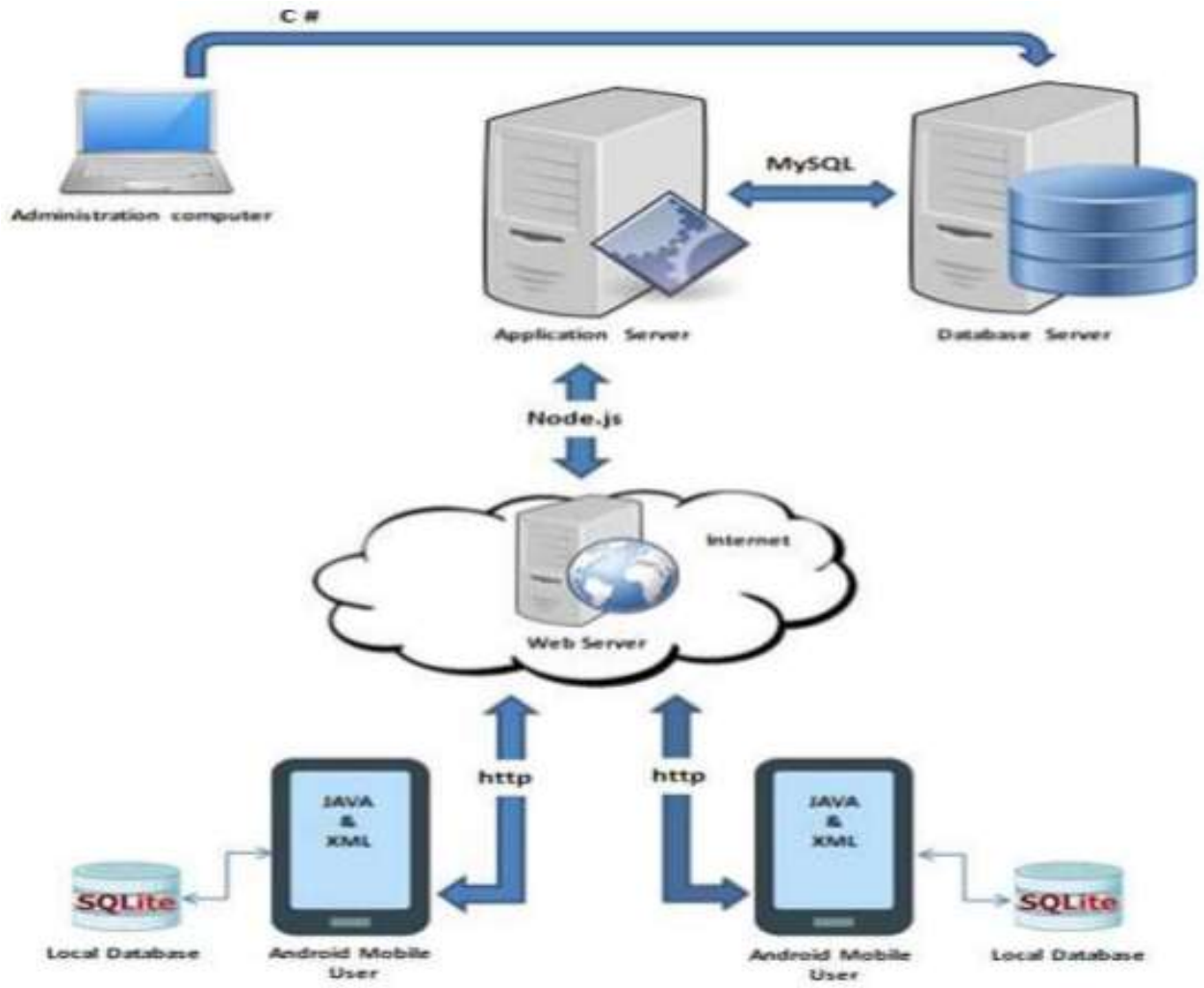


Рисунок 1. Архітектура додатку обміну повідомленнями

На рисунку 1 наведена загальна структура додатку обміну повідомленнями. Ця архітектура є спробою знайти корисні рішення проблем безпеки та конфіденційності у сфері соціальних мереж. Система розроблена як мобільний додаток з використанням мов JAVA та XML у середовищі Android Studio, бази даних MySQL, локальної бази даних SQLite та платформи Node.js (Java Script) для серверного програмування, мова C Sharp використовується для розробки інтерфейсу. Обмін усіма повідомленнями через цей запропонований миттєвий обмін повідомленнями здійснюється наскрізним шифруванням із використанням легких алгоритмів шифрування та дешифрування, щоб бути зручним для обмеження та різноманітності мобільних пристроїв користувачів. Конструкція включає в себе три основні рівні:

Рівень 1: Основні функції додатку. Забезпечує основні функції, необхідні для онлайн повідомлень і включає два типа баз даних, основної системної бази даних на сервері, яка містить користувача інформація, статус, друзі та повідомлення, якими обмінюються всі користувачі в системі, тоді як локальна база даних, яка побудована всередині пристрою користувача для зберігання інформації користувача, розмов і деяких важливих статусів. Ці дві бази даних призначені для зберігання та обробки трьох типів повідомлень (тексту, зображень і файлів) у зашифрованій або незашифрованій формі відповідно до

способу надсилання або отримання повідомлень. Основні завдання представлені наступним чином:

Реєстрація та вхід: коли користувач відкриває програму, буде виконано набір процесів для перевірки локальних і глобальних (серверних) баз даних, якщо цей номер телефону вже зареєстровано, щоб полегшити роботу користувача увійдіть і відкрийте інтерфейс списку друзів у чаті, інакше реалізується новий процес реєстрації, щоб отримати номер телефону нового учасника та надіслати SMS-повідомлення для перевірки особи. Процеси перевірки: програма використовує деякі процеси перевірки, як-от:

Рівень користувача: розглядаються два типи користувачів (VIP і звичайний), визначені адміністратором. У VIP-рівні відносяться додаткові функції безпеки, конфіденційності та деякі додаткові процедури, пов’язані з конфіденційністю.

Нові друзі: якщо будь-який новий друг (контакти) користувача зареєстрований як новий учасник у програмі, список друзів цього користувача буде оновлено. Програма перевіряє всі контакти користувачів під час кожного входу.

Нові повідомлення: коли нове повідомлення надійшло (завантажено) на сервер і стан отримувача знаходиться в режимі онлайн, усі нові повідомлення будуть завантажені з бази даних сервера в локальну базу даних на пристрої користувача (одержувача) зі сповіщеннями про нові непрочитані повідомлення.

Керування контролем доступу: щоб переконатися, що користувач, який реєструється в системі, є реальною людиною, а не роботом або скомпрометованим обліковим записом користувача, а також для уникнення крадіжки особистих даних або клонування профілю. Прийняті основні механізми автентифікації:

Верифікаційне повідомлення (SMS): Під час реєстрації в додатку за номером телефону користувача, сервер надсилає повідомлення перевірки (SMS), що містить випадковий код, який буде використано для перевірки реєстрації за цим номером телефону. Цей механізм може застосовуватися багаторазово та автоматично за потреби відповідно до рівня користувача. Цей механізм вимагає дозволу користувача на доступ його/її мобільний SMS.

Перевірка ICCID: для кожної SIM-карти мобільного телефону існує унікальний неповторюваний номер коду ICCID (Integrated Circuit Card Identifier - ідентифікатор картки інтегральної схеми). Програма використовує ICCID, щоб переконатися, що зареєстрований номер телефону збігається з номером SIM-картки пристрою, який підключається до програми, щоб виявити будь-яку несанкціоновану спробу доступу за номером користувача з пристрою, на якому немає SIM-картки цього зареєстрованого телефонного номера користувача.

Рівень 2: Методи конфіденційності. Ця частина присвячена огляду методів і функцій конфіденційності, які використовувалися для посилення аспектів безпеки та конфіденційності в запропонованій програмі, супроводжуючи проблеми обізнаності користувачів. Ці методи:

А. Робота з повідомленнями: ця техніка використовується для того, щоб

дозволити обмінюватися повідомленнями з користувачем через цю програму лише для контактів, які зберігаються на пристрої мобільного телефону користувача. Коли повідомлення надійде від когось, хто не зберігається в контактах користувача, воно з'явиться в сповіщенні одержувача, щоб мати можливість прийняти повідомлення від цього відправника чи ні.

B. Блокування контактів: запропонована програма дає користувачеві право блокувати будь-які контакти, з якими користувач не хоче спілкуватися, у той же час користувач може також розблокувати. Ця техніка використовується як форма захисту конфіденційності.

C. Знищення сеансу: додатковий вибір дозволяє користувачеві знищити розмову. Це означає, що всі дані розмов і повідомлення буде видалено з локального та глобального бази даних і не можуть бути відновлені.

Рівень 3: Криптографічні методи. Одна з головних проблем, з якою зіткнулася програма миттєвих повідомлень, полягає в тому, як зробити конфіденційну інформацію користувача та обмін даними (повідомленнями) між ними більш безпечними, щоб повідомлення, зашифроване таким чином, не було доступним для постачальника. Це називається наскрізним шифруванням, яке означає, що повідомлення, зашифроване на пристрої відправника, може розшифрувати лише одержувач.

Загальна структура криптографічних методів запропонованої системи зображена на рисунку 2. Складається з двох частин. Перша частина стосується керування ключами між відправником і одержувачем, тоді як друга частина стосується шифрування та дешифрування повідомлень у чаті. Ідея використання алгоритму RSA полягає в тому, щоб забезпечити захист секретного ключа (для алгоритму Trivium) і безпечну передачу між відправником і одержувачем. Події потоку ключової частини управління:

1. Відправник шифрує секретний ключ відкритим ключем одержувача.

2. Одержувач розшифровує зашифрований секретний ключ за допомогою свого закритого ключа алгоритму RSA.

3. Одержувач використав розшифрований ключ для розшифровки повідомлення за допомогою алгоритму Trivium.

Друга частина використовує потоковий шифр Trivium для шифрування повідомлень у чаті між відправником і одержувачем за допомогою секретного випадкового ключа (96 біт), який поєднується зі старшими бітами (64 біт) функції UUID (універсально унікальних ідентифікаторів) для номера телефону одержувача, щоб створити 160-біт як основний вхідний сигнал алгоритму Trivium. UUID — механізм ідентифікації, створений на основі часу.

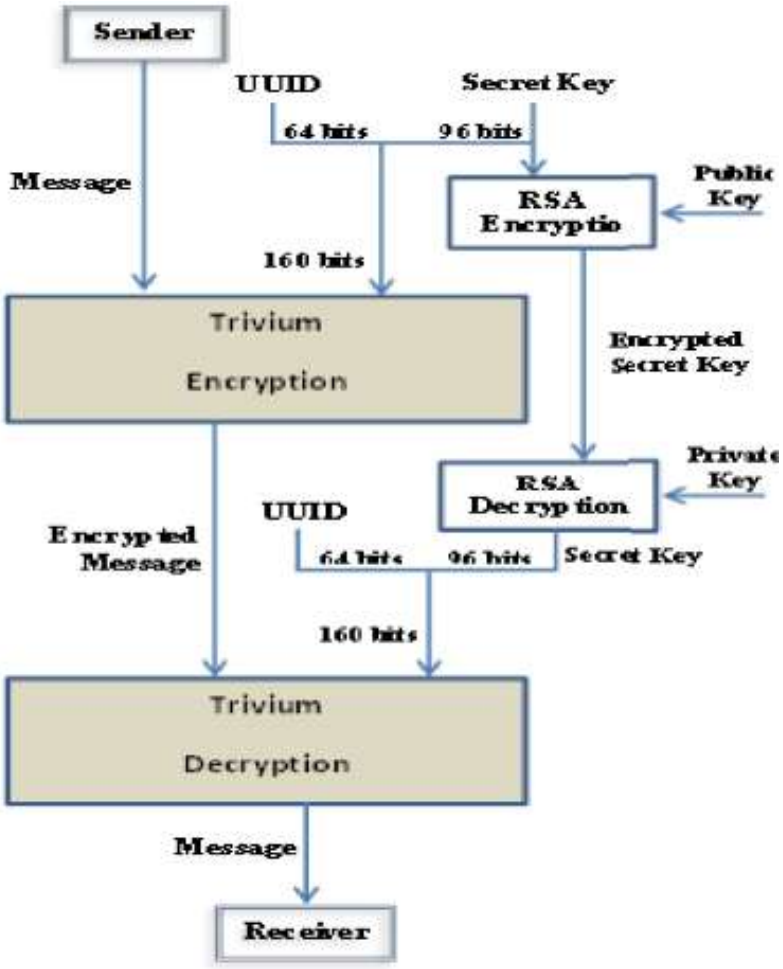


Рисунок 2. Загальна структура криптографічної системи додатку

Більшість користувачів месенджерів, як правило, не усвідомлюють важливості налаштувань конфіденційності для захисту їх особистої інформації, тому вони не мають достатнього усвідомлення, щоб усвідомити ризик кількох загроз, які загрожують їхній конфіденційності, тому необхідно зробити деякі необхідні функції захисту автоматично керованими програмою.

Крім того, найсерйознішу загрозу безпеці та конфіденційності соціальних медіа становлять ненадійні постачальники мережевих послуг, оскільки всі дані користувачів знаходяться в межах їх досяжності.

Крім того, використання концепції наскрізного шифрування та методів обміну ключами є основними векторами в аналізі та оцінці конфіденційності та безпеки соціальних мереж.

2 Найбезпечніші додатки – месенджери обміну повідомленнями

Основною проблемою всіх месенджерів є їхня безпека. Зазвичай у месенджерах використовують один із двох видів шифрування - наскрізне шифрування та шифрування «в транзиті». Завдяки наскрізному шифруванню повідомлення зашифровуються до того, як текст залишає пристрій відправника. Ключі дешифрування є лише на смартфонах користувачів. Проходячи через сервери, повідомлення залишаються в безпеці -їх ніхто не зможе прочитати. Лише пристрій одержувача може розшифрувати повідомлення.

Шифрування «в транзиті» є менш безпечним, ніж наскрізне шифрування.

Воно кодує повідомлення лише дорогою до серверів для оброблення, а потім дорогою з серверів до користувача. Коли повідомлення доставляється на сервери, усі, хто має доступ до інформації на сервері, зможе їх прочитати. Тож наскрізне шифрування забезпечує надійніший захист даних. У месенджерах з наскрізним шифруванням ніхто, окрім співрозмовників, не може побачити вміст повідомлення. Це означає, що і компанії, які забезпечують наскрізне шифрування, не можуть передавати тексти повідомлень своїх користувачів стороннім особам, наприклад, владним структурам будь-яких країн. З наскрізним шифруванням все ваше листування та дзвінки залишаються доступними тільки вам та іншим учасникам чату. Вибір додатка-месенджера зводиться до Вашої конкретної ситуації: потрібно знайти ідеальний баланс безпеки, зручності (зокрема, можливості резервного копіювання) та ширини кола Вашого спілкування. Розглянемо переваги та недоліки кожного додатка – це допоможе Вам зробити правильний вибір.

Viber. Плюси: Можливість дзвонити за кордон безкоштовно. Можна обмінюватися фотографіями, а також відео- та аудіо повідомленнями. Захищений зв'язок. Viber автоматично шифрує текстові повідомлення, відеодзвінки та голосові дзвінки, фотографії, відео та групові чати. Надійні контакти – можна перевіряти достовірність контактів вручну, щоб бути впевненим, що спілкуєтеся саме з тим, хто це має бути. Ви можете видалити текстове або голосове повідомлення навіть після надсилання. Можна платно телефонувати на міські та мобільні телефони, навіть якщо на них не встановлено програму Viber. Послуга має назву Viber Out.

Мінуси: Багато спаму та реклами. Нема веб-версії. Займає багато місця на смартфоні. За замовчуванням файли автоматично переходять у пам'ять телефону. Поганий зв'язок при голосових та відео дзвінках, незалежно від якості інтернету. Можливість злому. Головні мінуси месенджера – відсутність тестів на безпеку (публічних) та закритий код. Застарілий дизайн програми. Viber не зберігає історію листування.

Популярний месенджер Viber про безпеку пише, що на відміну від деяких інших месенджерів, він не може прочитати ваші особисті та групові чати або підслухати особисті голосові та відеодзвінки. Наскрізне шифрування працює за замовчуванням і не вимагає додаткових дій, щоб увімкнути його.

Утім, погана новина у тому, що у січні 2022 року Viber відкрив представництво в росії відповідно до закону про діяльність іноземних осіб в інтернеті на території російської федерації, а також створив особистий кабінет на сайті Роскомнагляду.

А це означає, що Viber повинен зберігати все листування та записи розмов на російських серверах та надавати оперативний доступ ФСБ до цих записів.

А як же шифрування, запитаєте? Воно є, але може працювати тільки до сервера, та від сервера. А от на сервері Viber дані повинні зберігатися та до них може надаватися доступ ФСБ згідно з російськими законами. При цьому візуально ви ніяк не зможете цього побачити.

Facebook Messenger. Плюси: він у кожного є, також у додатку є безліч

цікавих опцій в налаштуваннях конфіденційності (зокрема, опція “таємних розмов”). Мінуси: випадковому користувачу важко знайти, як налаштовується конфіденційність (окрім того, на різних платформах дещо відрізняється інтерфейс).

Facebook Messenger, за останніми підрахунками, має 1,3 мільярда користувачів. Однак розмови за замовчуванням не шифруються на рівні користувача. Для увімкнення шифрування Вам потрібно вступити в “таємні розмови” – цей варіант є лише в додатках iOS та Android, а не в браузерній версії. Ці чати не тільки зашифровані стандартним для цієї індустрії протоколом Signal, але також можуть бути налаштовані на самознищення. Ще одним мінусом, як і плюсом є платформа Facebook. Експерти з конфіденційності насторожено ставляться до того, що гігант соціальних медіа (чия бізнес-модель – продавати дані рекламодавцям) може робити з інформацією про те, як і з ким Ви розмовляєте.

WhatsApp. Плюси: Суцільне шифрування за замовчуванням та масштабне охоплення – по всьому світу. Це місце для групових чатів, де перетинаються користувачі з різних країн та різних платформ (однаково зручно для iOS та Android). Проста форма встановлення та реєстрації. Також месенджер простий у використанні - тут немає нічого зайвого. Можна обмінюватися фотографіями, відео, документами та голосовими повідомленнями, а також безкоштовно дзвонити за кордон. Автоматичне імпортування всіх контактів із телефону до програми. Відсутність реклами та швидка робота програми. Можливість міняти закріплений за обліковим записом номер телефону без втрати даних. Повідомлення WhatsApp можна надсилати та отримувати у браузері на комп'ютері.

Мінуси: Відсутність можливості скасувати надсилання повідомлення. WhatsApp залишається переважно мобільним додатком. Висока можливість злому. Може займати багато місця у пам'яті через накопичення різних файлів. Може стягуватися плата за користування інтернетом. Велика кількість спаму. Крос-платформенна сумісність з Facebook Messenger не викликає довіри.

Така ж настороженість, яка існує щодо Facebook Messenger, поширюється і на добре захищений WhatsApp. Компанія Марка Цукерберга придбала WhatsApp у 2014 році, пообіцявши, що вона буде функціонувати незалежно. Потім через два роки WhatsApp заявив, що розпочне обмін даними з Facebook. WhatsApp маєблизько 1,5 мільярдів користувачів, а компанія заявляє, що додаток може розкривати у Facebook певні деталі – наприклад, коли Ви востаннє використовували додаток і як часто.

Незважаючи на це, WhatsApp також використовує метод Signal для повного шифрування, що означає, що Facebook не може отримати доступ до вмісту Ваших повідомлень незалежно від того, чи можуть бути переглянуті його угоди з користувачами в майбутньому. Представники WhatsApp також говорять, що після збереження повідомлень у користувачів додаток не зберігає повідомлення на своїх серверах. Однак, якщо користувачі вирішать створити резервну копію історії чатів у додатку – наприклад, на iCloud або Google Drive, тоді вони можуть бути під загрозою витоків, якщо ці платформи будуть

зламані.

Telegram. Плюси: Цілий ряд варіантів безпеки в межах “таємних чатів”. Насамперед, це безліч оперативних каналів із новинами про ситуацію в країні. Можливість спілкуватися аудіо- та відеоповідомленнями. Можна надсилати будь-які медіа-файли без обмежень за типом або розміром. Вся історія листування зберігається у хмарі Telegram і майже не займає місця на ваших пристроях. Telegram ніколи не надає доступу до даних третім особам. Можна увійти в Telegram на декількох пристроях одночасно. Обмежень на кількість одночасних сесій немає. Месенджер упаковує дані у мінімально можливу кількість байтів. Ви можете надсилати та отримувати повідомлення навіть зі слабким з'єднанням з інтернетом. Telegram підходить для створення онлайн спільнот та організації робочих процесів.

Мінуси: Часто бувають збої у системі, через що Telegram може деякий час не працювати. Прив'язка до телефонного номера. З одного боку, це добре, але з іншого не дуже. Навіть якщо в Telegram ви дотримуєтеся статусу інкогніто, порівняння бази номерів і бази месенджера видасть вас. Також можна перехопити підтвердження входу за одноразовим кодом.

Самі повідомлення у месенджері не зашифровані. Вони дійсно передаються зашифрованими протоколами, але на серверах зберігаються у відкритому вигляді

Плюси: цілий ряд варіантів безпеки в межах “таємних чатів”. Додаток безкоштовний, не для отримання прибутку і не належить корпорації, що продає дані користувачів. Мінуси: Для програми, яка визначає конфіденційність своїм головним пріоритетом, вона не має найважливішої функції, увімкненої за замовчуванням. Також є багато питань щодо його внутрішнього методу шифрування.

Шифрування на рівні користувачів не вмикається за замовчуванням. Щоб його отримати, Ви повинні використовувати “таємні чати”. Регулярні розмови шифруються між Вашим пристроєм та сервером Telegram, а також між сервером Telegram та пристроєм одержувача. Компанія заявляє, що це – забезпечення хмарного резервного копіювання та доступу до історії ваших чатів на будь-якому пристрої. Деякі фахівці з кібербезпеки також поставили під сумнів метод шифрування Telegram, який був розроблений виключно цією компанією та не є відкритим кодом.

Signal. Плюси: Найвищий стандарт функцій безпеки, включаючи шифрування на кінцевих точках та захист метаданих. Відкритий код. Створений некомерційним фондом Signal Foundation. Signal використовує шифрування, яке забезпечує безпеку користувачів. Повідомлення надходять швидко навіть у повільних мережах. Нема реклами. Signal не збирає даних своїх користувачів. Під одним номером месенджер можна встановити на п'ятьох пристроях одночасно. Але серед цих гаджетів не може бути одразу двох смартфонів. Обмеження зроблено для безпеки.

Мінуси: Під час встановлення месенджера на інший смартфон або зміну номера, листування, файли та інші дані втрачаються. Адже програма зберігає це на пристрої і не синхронізує із серверами. Не можна надсилати файли, що

займають понад 100 МБ. Груповий чат вміщує лише 1000 осіб.

Крім розробки базового протоколу шифрування в кінці, Signal є захисником конфіденційності. Чати повністю зашифровані за замовчуванням, як і метадані – як, коли і з ким ви спілкуєтесь. Повідомлення можуть бути налаштовані на самознищення та можуть бути надіслані анонімно.

3 Захист мобільних і хмарних обчислювальних середовищах

Хмарні обчислення об'єднують різні технології для забезпечення платформ, послуг та інфраструктури для кількох користувачів і бізнес організацій. Хмарні обчислення об'єднують різні технології для надання платформ, послуг та інфраструктури багатьом користувачам і бізнес-організаціям. Мобільні хмарні обчислення (Mobile Cloud Computing - MCC) поєднують мобільні пристрої та бездротові технології, поширені в усьому середовищі, з хмарними обчисленнями для забезпечення безперервного підключення. Зі швидким розвитком технологій все більше і більше користувачів завантажують у хмару різноманітні дані, які також містять конфіденційні дані. Безпека та конфіденційність даних є головною проблемою, коли йдеться про обмін даними.

Мобільні пристрої стикаються з багатьма проблемами конфіденційності в основному через систему відстеження GPS. Безпека MCC поділяється на дві основні категорії – модуль безпеки та модуль конфіденційності. Модуль безпеки стосується безпеки хмари та мобільної мережі. Безпека даних означає, що інформація буде безпечно зберігатися, захищена від будь-якого виду несанкціонованого доступу, а також захищена від пошкодження даних протягом усього життєвого циклу. Це включає в себе шифрування даних, токенізацію та розповсюдження керування ключами. Організаційна інформація зазвичай доступна для спільного використання, а тому безпека даних порушується. Щоб захистити таку конфіденційну інформацію, нам потрібна безпека даних у системах MCC. Якщо організації потрібен вищий рівень безпеки та конфіденційності, організація може створити систему, яка присутня на кількох серверах. Такі типи серверів називаються дзеркальними серверами. Постачальник хмарних сховищ повинен запропонувати мінімальні можливості, які включають: перевірену схему шифрування, яку загальне сховище використовує для захисту даних, суворі протоколи контролю доступу, щоб жоден неавторизований користувач не міг отримати доступ до даних, резервне копіювання даних бути запланованим, а резервне копіювання носіїв має безпечно зберігатися

Дані потрібно захищати в трьох станах. Можливі стани даних:

1) *Дані в дорозі*: даними в дорозі можуть бути такі дані, як голос, відео, текст і метадані. Ці дані переміщуються через мережу в хмару та назад, тому ці дані мають бути зашифровані. Вони передбачають спілкування не лише з віртуальними мережами, а й поза хмарою. Вони мають бути захищені від усіляких атак за допомогою шифрування.

2) *Дані в стані спокою*: це відноситься до неактивних даних, таких як NAS (Network Attached Storage), SAN (Storage AreaNetwork), файлові сервери, сховище даних і зовнішнє резервне копіювання. Ці дані мають бути не тільки

зашифровані, але й для запобігання атакам слід використовувати надійні політики контролю доступу.

3) *Дані, що використовуються*: Дані, що використовуються, стосуються динамічних даних, які зберігаються в непостійному випадку, таких як дані або ключі шифрування в кеші, основній пам'яті, транзакції повідомлень у черзі, дані програми в процесі тощо. Ці дані знаходяться в зрозуміла текстова форма, яка використовується для пошуку, отримання даних. Але для кращої безпеки хмари ці дані повинні бути зашифровані.

Постачальник хмарних послуг повинен перевіряти ризики на хмарному сервері в таких сферах, як цілісність даних, відновлення та конфіденційність. Хмарний постачальник також має оцінити сервер у юридичних питаннях, таких як електронне відкриття, відповідність нормативним вимогам і аудит. Наступні ризики безпеки виникають у хмарних обчисленнях:

– *Привілейований доступ користувача*: витік конфіденційних даних зробить дані незахищеними. Доступ до даних має надаватися певній групі користувачів.

– *Відповідність нормативним вимогам*: постачальники хмарних послуг мають проводити зовнішні аудити та сертифікацію безпеки.

– *Розташування даних*: дані хмари розташовані на кількох серверах, тому точне розташування може бути невідомим. Їх слід попросити дотримуватися місцевих вимог конфіденційності.

– *Сегрегація даних*: дані в хмарі зберігаються в спільному середовищі. Хмарні постачальники повинні допомагати в розподілі даних і надавати докази схем шифрування, які вони використовують, оскільки шифрування може зробити будь-які дані непридатними для використання.

– *Відновлення*: у разі збою хмарний постачальник повинен мати можливість відновити всі дані протягом короткого періоду часу.

– *Розслідування / Підтримка*: Хмарний постачальник повинен мати можливість надавати дослідницьку підтримку, хоча це важко, оскільки багато користувачів входять у систему. Розслідування та запит на відкриття буде неможливим, якщо хмарний постачальник не зможе це зробити.

– *Довгострокова життєздатність*: якщо хмарний постачальник втратить свій бізнес, вони повинні запевнити вас, що ваші дані в безпеці за будь-яку ціну.

Хмарні обчислення мають багато проблем у різних аспектах обробки даних та інформації. Деякі з них перелічені в наступних параграфах:

Безпека та конфіденційність: проблеми з конфіденційністю та безпекою можна подолати за допомогою безпечного апаратного забезпечення, шифрування та програм безпеки. Користувачі завантажують свої дані в хмару, і ці дані зберігаються в хмарі випадковим чином. Користувачі не знають

конкретної позиції своїх даних, що зберігаються в хмарі; це може стикнутися з ризиком конфіденційності.

– *Портативність*: це ще одна перешкода для хмарних обчислень, у яких програмне забезпечення має бути легко переміщено від одного постачальника хмари до іншого. Не повинно бути блокування продавця. Однак це ще не стало можливим, оскільки всі постачальники хмарних технологій використовують різні стандартні мови для своїх платформ.

– *Обчислювальна продуктивність*: програми з інтенсивним об'ємом даних у хмарі потребують високої пропускної здатності мережі, що призводить до високої вартості. Низька пропускна здатність не відповідає бажаній обчислювальній продуктивності хмарних додатків.

– *Надійність і доступність*: для хмарних технологій життєво важливо бути надійними та міцними, оскільки більшість компаній зараз покладаються на послуги, що пропонуються третіми сторонами.

– *Інтероперабельність*: це означає, що програма на одній платформі повинна мати можливість інтегрувати служби з інших платформ. Це можна зробити за допомогою веб-сервісів, але створення цих веб-сервісів досить складне.

Існує багато ризиків, пов'язаних із безпекою даних у хмарному середовищі, і оскільки МСС по суті використовує хмару, він також успадковує будь-які проблеми безпеки, пов'язані з хмарними обчисленнями. Наступні ризики можуть виникнути в мобільній хмарі:

– *Мобільний термінал*: мобільний термінал має відкриту операційну систему, яка має стороннє програмне забезпечення, персоналізацію, постійний бездротовий доступ до Інтернету, тому проблеми з безпекою в мобільному терміналі є серйозними. Зловмисне програмне забезпечення може бути завантажено разом із корисними програмами та може отримати незаконний доступ до особистого дані користувача; Таким чином, мобільний термінал постраждає від витоку інформації. Зловмисне програмне забезпечення також може потрапити через USB-пристрій, мережі 3G або 4G, Bluetooth або вкладення MMS. Хоча деякі постачальники засобів безпеки надають антивірусне програмне забезпечення, вони повинні мати функції, подібні до тих, що пропонуються на настільному комп'ютері. Проблеми безпеки також виникають у прикладному програмному забезпеченні, особливо якщо є помилка або через FTP програми. Помилки також можуть бути присутніми в операційній системі, які можуть бути використані для знищення мобільного телефону.

– *Безпека мобільної мережі*: мобільна мережа може становити ризик через загальнодоступні системи Wi-Fi, і

інформація може потенційно витікати. Навіть у випадку приватного Wi-Fi, якщо механізм шифрування слабкий, безпека мережі піддається значному ризику.

– *Мобільна хмара*: хмара також може бути під загрозою через збільшення кількості користувачів, які обмінюються інформацією. Зловмисником може бути законний користувач хмари, будь-який внутрішній персонал постачальника хмари або будь-який оператор хмари.

Висновки. У МСС визначено три основні питання безпеки: мобільний термінал, мобільна мережа та мобільна хмара. У мобільному терміналі є зловмисне програмне забезпечення, якому CloudAV може запобігти. Уразливості програмного забезпечення також існують у програмах і операційних системах, яким можна запобігти, встановивши системні патчі та перевіривши легітимність і цілісність програмного забезпечення. Кілька інших проблем включають відсутність обізнаності про безпеку або неправильну роботу, якій можна запобігти, регулюючи поведінку користувача. У мобільній мережі може статися витік інформації або будь-яка зловмисна атака, якій можна запобігти за допомогою надійного протоколу безпеки або хорошого шифрування даних. У мобільній хмарі існують такі проблеми, як надійність платформи, захист даних і конфіденційності, яким можна запобігти шляхом інтеграції сучасних технологій безпеки, керування ключами, шифрування даних, автентифікації, контролю доступу, конфіденційності та захисту даних.

ОСНОВНА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна та наукова література:

9. Dawn Griffiths, David Griffiths. Head First. Android Development. A Brain-Friendly Guide. O'REILLY. Beijing. Cambridge. Köln. Sebastopol. Tokyo.2015. 704 p.
10. Казимир В., Карпачев І., Усік А. Моделі системи безпеки ос android. URL: https://www.researchgate.net/publication/328775065_MODELI_SISTEMI_BEZPEKI_OS_ANDROID.
11. Конспект лекцій з дисципліни «Програмування для мобільних пристроїв». Укладачі: Готович В. А., Михайлович Т. В. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2020. 216 с.
12. Розробка застосувань для мобільних пристроїв. Конспект лекцій. Міністерство освіти і науки України ЗНТУ. Кафедра програмних засобів. Запоріжжя 2016. 62с.
13. Сайко В.Г., Казіміренко В.Я., Літвінов Ю.М. Мережі бездротового широкосмугового доступу. Навчальний посібник. Кив: ДУТ, 2015. 216 с.
14. Опорний конспект лекцій з курсу «Мобільні інформаційні системи». Тернопільський національний економічний університет. Факультет комп'ютерних інформаційних технологій. Тернопіль. 2016. 60с.
15. Соколов В. Ю., Бурячок В. Л., Тадждіні М. М. Безпека безпроводових і мобільних мереж. Київ, КУБГ, 2019. 130 с.

16. Шматко О. В., Поляков А. О., Федорченко В. М. Аналіз методів і технологій розробки мобільних додатків для платформи Android: навч. посіб. Харків : НТУ «ХПІ», 2018. 284 с.

ДОДАТКОВА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна та наукова література:

1. Cheng, F. Build Mobile Apps with Ionic 4 and Firebase: Hybrid Mobile App Development. Apress, 2018. 238 p.
2. Heckman R. Designing platform independent mobile apps and services. Hoboken: IEEE Press, 2016. 230 p.
3. John Horton. Android Programming for Beginners: Build in-depth, full-featured Android 9 Pie apps starting from zero programming experience, 2nd Edition.2018. 766 p.
4. Nalwaya, A., Paul, A. React Native for Mobile Development: Harness the Power of React Native to Create Stunning iOS and Android Applications. Apress, 2019.119 p.
5. Nolan G., Cinar O., Truxall D. Android best practices. Springer. 2014. 222p.
6. Six J. Application security for the android platform. Sebastopol, CA: O'Reilly, 2011. 97 p.
7. Windmill, E. Flutter in Action. Manning Publications, 2020 .P.310.

Нормативно-правові акти:

1. Про інформацію. Закон України від 02.10.1992, № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.
2. Про Державну службу спеціального зв'язку та захисту інформації України. Закон України: від 23.02.2006, № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text.
3. Про захист інформації в інформаційно-комунікаційних системах. Закон України: від 05.07.1994, № 1170-VII. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
4. Про електронні комунікації: Закон України від 16.12.2020 : [із змінами і доповненнями]. Офіційний вісник України. 2021. № 6 (21.01.2021). Ст. 306.
5. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
6. Про захист персональних даних. Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
7. Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 10.05.2023).
8. Стратегія інформаційної безпеки України, затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 10.05.2023).
9. Про створення Центру протидії дезінформації: Рішення Ради національної безпеки і оборони України від 11 березня 2021 року, введено в дію Указом Президента України від 19 березня 2021 року № 106/2021. URL: https://zakon.rada.gov.ua/laws/show/106/2021#Text.

10. ДСТУ ISO/IEC 27000:2019 (ISO/IEC 27000:2018, IDT) Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів - На заміну ДСТУ ISO/IEC 27000:2017 (ISO/IEC 27000:2016, IDT).
11. ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; Cor 1:2014, IDT) / Поправка № 2:2019.
12. (ISO/IEC 27001:2013/Cor 2:2015, IDT) Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги.
13. ДСТУ ISO/IEC 27002:2015 (ISO/IEC 27002:2013; Cor 1:2014, IDT) / Поправка № 2:2019 (ISO/IEC 27002:2013/Cor 2:2015, IDT). Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.
14. ДСТУ ISO/IEC 27003:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова (ISO/IEC 27003:2017, IDT).
15. ДСТУ ISO/IEC 27004:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання (ISO/IEC 27004:2016, IDT).
16. ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT) Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки - На заміну ДСТУ ISO/IEC 27005:2015 (ISO/IEC 27005:2011, IDT).

Інформаційні ресурси в Інтернеті:

1. Офіційний блог компанії Google. URL: http://googleblog.blogspot.com/search/label/Android
2. Онлайн-підтримка StackOverflow URL: http://stackoverflow.com/questions/tagged/android
3. Альянс відкритих мобільних пристроїв. URL: http://www.openhandsetalliance.com/
4. Google Play Hits 1 Million Apps. URL: https://mashable.com/archive/google-play-1-million
5. Android App Stats. URL: http://www.androlib.com/appstats.aspx
6. Java Editor URL: https://play.google.com/store/apps/details?id=air.JavaEditor
7. JavaIDEdroid URL: https://play.google.com/store/apps/details?id=ch.tanapro.JavaIDEdroid
8. The Professional Android IDE. URL: http://www.jetbrains.com/idea/features/android.html
9. NBAndroid. URL: http://plugins.netbeans.org/plugin/19545/nbandroid
10. Android Studio. URL: http://developer.android.com/sdk/index.html
11. Backup & restore Android apps using adb. URL: http://jonwestfall.com/2009/08/backup-restore-android-apps-using-adb/
12. SDK Tools. URL: http://developer.android.com/tools/sdk/tools-notes.html
13. Dalvik Executable format. URL: https://source.android.com/devices/tech/dalvik/dex-format.html
14. Android – Invoke JNI Based Methods (Bridging C/C++ And Java) URL: https://davanum.wordpress.com/2007/12/09/android-invoke-jni-based-methods-bridging-cc-and-java/
15. Native C applications for Android. URL: http://benno.id.au/blog/2007/11/13/android-native-apps

16. Android NDK. URL: https://developer.android.com/tools/sdk/ndk/index.html
17. SKIA graphics library in chrome: first impressions. URL: http://www.atoker.com/blog/2008/09/06/skia-graphics-library-in-chrome-first-283