МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
Харківський національний університет внутрішніх справ
Факультет № 4
Кафедра протидії кіберзлочинності
Факультет №6
Кафедри кібербезпеки та DATA-технологій

ЗАТВЕРДЖЕНО
Спільне засідання кафедри протидії кіберзлочинності факультету №4 та кафедри кібербезпеки та DATA-технологій факультету №6
Протокол № 3 від 23.06.2023 (магістри)

Завідувач кафедри

_____Олександр МАНЖАЙ
Завідувач кафедри

_____Юрій ГНУСОВ

РОЗРОБКА ЗАХИЩЕНИХ МОБІЛЬНИХ ЗАСТОСУВАНЬ (ОК.07)

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Кафедра	Кафедра протидії кіберзлочинності (univd.edu.ua/uk/dir/1740/kafedra-informatsiynykh-tekhnologiy-ta-kiberbezpeky)
Контактний телефон	+38 057 73-98-385 (роб.)
E-mail	klimushyn@ukr.net
ЛЕКТОР (ЛЕКТОРИ)	
	**Клімушин Петро Сергійович,** доцент кафедри протидії кіберзлочинності факультету № 4, к.т.н., доцент klimushyn@ukr.net **Лекційний потік:** факультет № 4, шифр навчальних груп Ф5-104м
Назва освітньо-професійної програми	Кібербезпека та захист інформації (безпека інформаційних та комунікаційних систем) Cybersecurity and information protection (security of

	information and communication systems)
Рівень вищої освіти	Другій (магістерській) (НРК України – 7 рівень та другий цикл вищої освіти Рамки кваліфікацій Європейського простору вищої освіти)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Статус дисципліни	Обов'язкова компонента освітньої програми, вивчається в 2 семестрі І курсу навчання
Мета вивчення дисципліни	Метою викладання навчальної дисципліни є формування системи теоретичних знань і придбання практичних умінь і навичок щодо технологій моделювання, проектування, розробки, тестування та впровадження захищених мобільних додатків, створених на базі сучасних мобільних платформ.
Завдання вивчення дисципліни	Формування компетенції розробки програмного забезпечення мобільних систем на основі технологій проектування захищених мобільних додатків для сучасних мобільних платформ. Отримання компетенції щодо обґрунтованого вибору інструментів та середовищ розробки відповідно до сформульованих функціональних та нефункціональних вимог до захищеного мобільного додатку.
Обсяг дисципліни в кредитах ECTS/годинах	Кількість кредитів ECTS (загальний обсяг – 90 год.) З них (денна/заочна): - аудиторна робота: 40/16 год. - самостійна робота: 50/74 год.
Форми та види проведення навчальних занять	Форма навчання – денна Види навчальних занять: - лекції: 20 год.; - семінарські заняття:10 год.; - практичні заняття:10 год; - лабораторні заняття:0 год. Форма навчання – заочна Види навчальних занять: - лекції: 8 год.; - семінарські заняття:0 год.; - практичні заняття: 8 год.; - лабораторні заняття: 0 год.
Самостійна робота	Опрацювання рекомендованої літератури, підготовка тез доповідей до конференцій,

	самостійне вирішення практичних завдань.
Індивідуальні завдання	Наукові доповіді, реферати
Необхідне обладнання	Мультимедійне обладнання (ноутбук та проектор), комп'ютерне забезпечення з виходом у мережу Інтернет.
Мова викладання	Українська
Контроль	Поточний та підсумковий контроль Поточний: опитування на практичних заняттях; участь в дискусіях, веб-квестах, обговоренні доповідей, рефератів; підготовка рефератів та доповідей, тестування, виконання самостійних робіт, захист лабораторних робіт. Критерії оцінки поточного контролю викладач повідомляє на першому занятті та перед кожними оцінюванням. Підсумковий контроль: **іспит.**
Інтегральна компетентність, загальні компетентності (КЗ)	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Спеціальні (фахові) компетентності (КФ)	КФ-8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ЗА ТЕМАМИ

Тема № 1. Бездротові локальні мережі

Загальна характеристика бездротових комп'ютерних мереж. Напрями застосування. Компоненти. Режими роботи. Класифікація бездротових мереж: за технологією та передавальних середовищ; за дальністю дії. Стільниковий зв'язок. Характеристики бездротових технологій передачі даних. Технології Wi-Fi, Bluetooth, NFC. Wireless Application Protocol. Покоління мереж мобільного зв'язку: 3G, 4G 5G. Безпека бездротових мереж. Концепції мережевої безпеки. Загальні рекомендації щодо захисту мережі. Автентифікація. Шифрування.

Тема № 2. Сучасні мобільні операційні системи та мові програмування додатків

Характеристика сучасних операційних систем (платформ) для мобільних пристроїв. Порівняння мобільних платформ (iOS, Android,Windows Mobile, Symbian, BlackBerry та інших). Мови програмування мобільних додатків: Java, Kotlin, Rust, Swift, HTML5.

Тема № 3. Інструменти і середовища розробки мобільних додатків

Призначення і типи інтегрованих середовищ розробки мобільних додатків. Інтегроване середовище розробки (ICP). Характеристика та порівняння типів додатків (натівний додаток, веб-додаток, гібридний додаток). Інструменті розробки мобільних додатків (Java, JDK, SDK, Android Studio, Android Eclipse, Intel XDK, Intel Beacon Mountain). Основні види додатків під ОС Android.

Тема № 4. Середовище розробки платформи Android

Установка та налаштування інструментів розробки додатків Android, Android Studio. Встановлення Java та Android Studio. Побудова простої програми. Створення нового проекту. Налаштування проекту. Вибір рівня API. Активності та макети. Створення активності. Налаштування активності. Створення віртуального пристрою Android. Запуск програми в емуляторі. Модифікація програми.

Тема № 5. Побудова інтерактивних програм

Основні крокі в створенні інтерактивних програм (створення проекту, оновлення макету, зв'язування макету з активністю, оновлення активності). Створення інтерактивного проекту. Оновлення макету. Зв'язування макету з активністю. Оновлення активності.

Тема № 6. Множинні активності та інтенти

Послідовність дій створення додатків із множинною активністю. Створення базової програми з однією активністю та макетом. Додавання другої активності та макета. Організація виклику другої активності з першої. Організація передачі з першої активності в другу.

Тема № 7. Користувацький інтерфейс

Ключові макети та компонентів графічного інтерфейсу. Визначення відносного макету. Розташовування уявлень. Відступи. Рядки. Інтервали. Атрибути для позиціонування уявлень. Визначення лінійного макету. Ідентифікатори уявлень. Ширина та висота уявлень. Визначення табличного макета. Завдання Стовпців та рядків. Компоненти графічного інтерфейсу. Аспекти функціональності. Читання та запис властивостей. Розмір та позиція. Обробка фокусу. Обробка подій та слухачі. Основні уявлення: надпис, текстове поле, кнопка, двопозиційна кнопка, вимикач, прапорець, перемикач, список, що розкривається, графічне уявлення, зображення/текст на кнопках, повідомлення. Спискові уявлення та адаптери. Типи активностей: активності верхнього рівня, активності категорій та активності деталізації/редагування. Адаптер масив. Фрагменти.

Тема № 8. Робота з базами даних

Структура бази даних SQLite. Набір класів керування базою даних SQLite: засоби для створення та управління базами даних, доступ до бази даних, читання та запису до бази даних. Визначення бази даних. Створення таблиць. Оновлення записів бази даних. Зміна записів бази даних. Зміна структури бази даних. Підключення до баз даних. Курсор доступу до наборів записів бази даних. Побудова запитів до бази даних. Функції SQL у запитах для обчислень характеристик. Спільна робота потоків. Основний потік подій. Потік візуалізації. Потоки у фоновому режимі роботи бази. Служби. Запускові

служби. Пов'язана служба. Виведення повідомлення служб. **Тема № 9. Безпека мобільних застосувань** Загрози мобільній безпеці. Фішинг у додатку. Компрометація ланцюжка поставок. Реклама шахрайства за допомогою кліків, вбудована в програми. Код криптомайнера в іграх або утилітах. Найкращі методи захисту мобільних пристроїв. Надійна автентифікація користувача. Оновлення мобільні операційні системи. Створення резервні копії даних користувача. Використання шифрування. Методи соціальної інженерії. Увага до налаштувань безпеки системи та додатків. Мобільні програми безпеки та антивірусні програми. Шкідливі програми в мобільних пристроях. Відстеження розташування в мережі. Прослуховування переговорів. Цифрове керування обмеженнями. Вразливості. Перешкоди. Маніпуляція. Саботаж. Стеження. Моделі системи безпеки ОС Android. Модель прав доступу. Модель роботи застосувань. **Тема № 10. Месенджери миттєвого обміну повідомленнями та захист мобільних і хмарних обчислювальних середовищах** Безпечний миттєвий обмін повідомленнями. Архітектура додатку обміну повідомленнями. Основні рівні захисту: основні функції додатку, методи конфіденційності, криптографічні методи. Загальна структура криптографічної системи додатку. Найбезпечніші месенджери повідомлень. Переваги та недоліки месенджерів:Viber, Facebook Messenger, WhatsApp, Telegram, Signal. Захист мобільних і хмарних обчислювальних середовищах. Можливі стани захисту даних: дані в дорозі, дані в стані спокою, дані, що використовуються. Ризики безпеки у хмарних обчисленнях.	
Програмні результати навчання (РН)	РН.13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури РН.19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН.21. Використовувати методи натурного, фізичного і комп’ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. РН.23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
Критерії	Оцінювання навчальної дисципліни проводиться за

<table>
<tr><td>оцінювання</td><td colspan="3">результатами поточного та підсумкового контролю:
• поточний контроль - 50 балів;
• підсумковий контроль - 50 балів.
Оцінка за поточний контроль складається з оцінювання аудиторної та самостійної роботи здобувача вищої освіти. Оцінка за аудиторну роботу визначається як середнє арифметичне балів, які ним отримані на семінарських заняттях (здобувач має отримати не менш 5 позитивних оцінок) з коефіцієнтом 5. Оцінка за самостійну роботу визначається як середнє арифметичне балів, які отримані здобувачем за: реферати, програми (здобувач має підготувати не менш 2 проектів) з коефіцієнтом 5.
Підсумкові бали з навчальної дисципліни визначаються як сума балів, які отримані здобувачем протягом семестру, та балів, які набрані на підсумковому контролі (іспиту).</td></tr>
<tr><td colspan="4">КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ</td></tr>
<tr><td rowspan="2">Оцінка в балах</td><td rowspan="2">Оцінка за національною шкалою</td><td colspan="2">Оцінка за шкалою ECTS</td></tr>
<tr><td>Оцінка</td><td>Пояснення</td></tr>
<tr><td>97-100
94-96
90-93</td><td>Відмінно (“зараховано”)</td><td>A</td><td>„Відмінно” – теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом сформовані, всі навчальні завдання, які передбачені програмою навчання виконані в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.</td></tr>
<tr><td>85-89
80-84</td><td rowspan="2">Добре (“зараховано”)</td><td>B</td><td>„Дуже добре” – теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконані, якість виконання більшості з них оцінено числом балів, близьким до максимального, робота з двома – трьома незначними помилками.</td></tr>
<tr><td>75-79</td><td>C</td><td>„Добре” – теоретичний зміст курсу освоєний цілком, практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконані, якість виконання жодного з них не оцінено мінімальним числом балів, деякі види завдань виконані з помилками, робота з декількома</td></tr>
</table>

			незначними помилками, або з однією – двома значними помилками.
70-74	Задовільно (“зараховано ”)	D	**„Задовільно”** – теоретичний зміст курсу освоєний не повністю, але прогалинине носять істотного характеру, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, більшість передбачених програмою навчання навчальних завдань виконано, деякі з виконаних завдань, містять помилки, робота з трьома значними помилками.
65-69			
60-64		E	**„Достатньо”** – теоретичний зміст курсу освоєний частково, деякі практичні навички роботи не сформовані, частина передбачених програмою навчання навчальних завдань не виконані, або якість виконання деяких з них оцінено числом балів, близьким до мінімального,робота, що задовольняє мінімуму критеріїв оцінки.
40-59	Незадовільно („не зараховано”)	FX	**„Умовно незадовільно”** – теоретичний зміст курсу освоєний частково, необхідні практичні навички роботи не сформовані, більшість передбачених програм навчання, навчальних завдань не виконано, або якість їхнього виконання оцінено числом балів, близьким до мінімального; при додатковій самостійній роботі над матеріалом курсу можливе підвищення якості виконання навчальних завдань (з можливістю повторного складання), робота, що потребує доробки
21-40			
1-20		F	**„Безумовно незадовільно”** – теоретичний зміст курсу не освоєно, необхідні практичні навички роботи не сформовані, всі виконані навчальні завдання містять грубі помилки, додаткова самостійна робота над матеріалом курсу не приведе до значимого підвищення якості виконання навчальних завдань, робота, що потребує повної переробки

Перелік питань, що виносяться на підсумковий контроль

1. Загальна характеристика бездротових комп'ютерних мереж.

2. Класифікація бездротових мереж.
3. Напрями застосування, компоненти, режими роботи бездротового зв’язку.
4. Принципи роботи технології бездротового зв’язку Bluetooth.
5. Технології бездротового зв’язку Wi-Fi стандарту IEEE 802.11a, b і g.
6. Технологія WIMAX стандарту IEEE 802.16.
7. Призначення технології NFC.
8. Протоколи безпровідної передачі даних (WAP, Wireless Application Protocol).
9. Порівняння характеристик поколінь технологій бездротового зв'язку.
10. Безпека бездротових мереж та загальні рекомендації щодо їх захисту.
11. Характеристика операційної системи iOS.
12. Характеристика операційної системи Android.
13. Характеристика операційної системи Windows Mobile.
14. Характеристика операційної системи Symbian.
15. Характеристика операційної системи BlackBerry.
16. Мови програмування для розробників мобільних додатків.
17. Інтегровані середовища розробки мобільних додатків.
18. Характеристика та порівняння типів додатків.
19. Інструменті розробки мобільних додатків.
20. Архітектура системи Android.
21. Середовище розробки Java, XML, Android SDK, Android Studio.
22. Налаштування інструментів розробки додатків Android.
23. Побудова простої програми та запуск програми в емуляторі.
24. Поняття активності та макету додатку.
25. Створення віртуального пристрою Android.
26. Основні крокі в створенні інтерактивних програм.
27. Створення інтерактивного проекту.
28. Оновлення макету додатку.
29. Зв'язування макету з активністю.
30. Оновлення активності.
31. Множинні активності та інтенти.
32. Створення додатків із множинною активністю.
33. Створення базової програми з однією активністю та макетом.
34. Додавання другої активності та макета.
35. Організація виклику другої активності з першої.
36. Організація передачі з першої активності в другу.
37. Користувацький інтерфейс додатку.
38. Ключові макети: відносний, лінійний та табличний.
39. Компоненти графічного інтерфейсу.
40. Спискові уявлення та адаптери.
41. Створення фрагментів.
42. Структура бази даних SQLite.
43. Визначення бази даних.
44. Оновлення записів бази даних.
45. Спільна робота потоків.

46. Підключення до баз даних.
47. Робота зі службами повідомлень.
48. Загрози мобільній безпеці.
49. Найкращі методи захисту мобільних пристроїв.
50. Шкідливі програми в мобільних пристроях.
51. Моделі системи безпеки ОС Android.
52. Безпечний миттєвий обмін повідомленнями.
53. Архітектура додатку обміну повідомленнями.
54. Загальна структура криптографічної системи додатку.
55. Характеристика сучасних додатків-месенджерів повідомлень.
56. Захист мобільних і хмарних обчислювальних середовищах.
57. Мобільне противірусне програмне забезпечення.
58. Захист інформації у мережах мобільного зв'язку.
59. Механізми автентифікації, цілісності, конфіденційності та анонімності.
60. Контроль доступу до даних мобільних додатків.
61. Захист інформації у перспективних системах мобільного зв'язку.

ОСНОВНА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна та наукова 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., Таджділні 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.

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