МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

Кафедра протидії кіберзлочинності факультету № 4

РОБОЧА ПРОГРАМА

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.

1. Опис навчальної дисципліни

Найменування показників	Шифри та назви галузі знань, код та назва спеціальності, ступень вищої освіти	Характеристика навчальної дисципліни
Кількість кредитів ECTS – 3 Загальна кількість годин – 90 Кількість тем – 10	12 Інформаційні технології; (шифр галузі) (назва галузі знань) 125 – Кібербезпека _____магістр_ (назва СВО)	Цикл обов'язкових дисциплін Навчальний курс – 1 Семестр – 2 Види контролю: підсумковий модульний контроль – екзамен
Тижневих годин для денної форми навчання: аудиторних – 3,5 самостійної роботи – 3,5		Розподіл навчальної дисципліни за видами занять: (денна/заочна форма навчання) Лекції – 20/8; Практичні заняття – 10/8; Семінарські заняття – 10/-; Самостійна робота – 50/74;

2. Мета та завдання навчальної дисципліни

Метою викладання навчальної дисципліни "Розробка захищених мобільних застосувань" 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.

Забезпечити студентам здобуття знань, умінь та розуміння, що відносяться до області кібербезпеки і дати їм можливість виконувати свою роботу самостійно. Бути підготовленими до успішного засвоєння складніших програм для: наукових дослідників та розробників, викладачів і аналітиків в області кібербезпеки.

Основними завданнями вивчення дисципліни є формування у студентів компетенції розробки програмного забезпечення мобільних систем на основі технологій проектування захищених мобільних додатків для сучасних мобільних платформ. Також студенти мають отримати компетенції щодо обґрунтованого вибору інструментів та середовищ розробки відповідно до сформульованих функціональних та нефункціональних вимог до захищеного мобільного додатку.

Міждисциплінарні зв'язки: Вища математика, Фізика, Інформаційні технології, Метрологія та вимірювання в сфері захисту інформації, Технічна та комп'ютерна графіка, Алгоритмізація та програмування, Електроніка та схемотехніка, Операційні системи та комп'ютерні мережі, Методи та засоби технічного захисту інформації.

2.3. Згідно з вимогами освітньо-професійної програми студент повинен:

знати:

– загальні принципи організації та теоретичні основи побудови програмного забезпечення для мобільних платформ;

– основи функціонування мобільних пристроїв та принципів їх взаємодії з інформаційними системами;

– основні можливості застосування мобільних додатків у бізнесі;

– основні засади процесів пошуку та обробки інформації мобільними додатками;

– основні мобільні операційні системи та платформи для мобільних пристроїв та особливості їх функціонування;

– особливості різних етапів життєвого циклу розробки захищених мобільних додатків;

– засоби розробки мобільних рішень;

– основні процедури та протоколи захисту даних у мобільних пристроях на різних операційних системах (платформах);

– принципи розгортання додатків на мобільних пристроях;

– принципи розробки мобільних додатків на платформі Android;

– основи інтеграції мобільних додатків з іншими інформаційними системами;

вміти:

– здійснювати аналіз можливостей сучасних інструментальних середовищ розробки мобільних додатків та їх інсталяції на персональному комп'ютері;

– розробляти додатки для мобільних пристроїв з використанням розповсюджених мов (технологій) програмування;

– розробляти захищені мобільні додатки на платформі Android відповідно до сформульованих вимог;

– розгортати програмні продукти на мобільних пристроях;

– використовувати програмні засоби формування основних процедур захисту інформації в мобільних пристроях;

– користуватися раніше складеними програмами і здійснювати супровід програм, вносити зміни в додатки, виконувати відлагодження програм за допомогою інструментальних засобів;

мати уяву про:

– перспективи розвитку та використання сучасних мобільних додатків для обробки інформації в корпоративних інформаційно-аналітичних системах;

– основні способи та методи розробки нових перспективних мобільних програмних продуктів для широкого кола задач.

Предметом вивчення навчальної дисципліни є теорія і практика моделювання та розробки мобільних додатків на базі сучасних технологій розробки програмного забезпечення.

В навчальному плані для вивчення дисципліни передбачені такі організаційні форми занять як лекції, практичні і лабораторні заняття.

Програмні компетентності:

Програмні компетентності, які формуються при вивченні навчальної дисципліни:	
Інтегральна компетентність, загальні компетентності (КЗ)	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Фахові компетентності спеціальності (ФК)	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.
Програмні результати навчання (ПРН)	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.

3. Програма навчальної дисципліни

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.

4. Структура навчальної дисципліни

4.1. 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**	

4.2. Розподіл часу навчальної дисципліни за темами (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**	

4.3. Питання, що виносяться на самостійне опрацювання

Завдання що виносяться на самостійну роботу студента	Література:
Тема № 1. Бездротові локальні мережі 1. Характеристики бездротових технологій передачі даних. 2. Технології Wi-Fi, Bluetooth, NFC. Wireless Application Protocol. 3. Покоління мереж мобільного зв'язку: 3G, 4G 5G.	[5] с. 109-192
Тема № 2. Сучасні мобільні операційні системи та мові програмування додатків 1. Порівняння мобільних платформ (iOS, Android,Windows Mobile, Symbian, BlackBerry та інших). 2. Мови програмування мобільних додатків: Java, Kotlin, Rust, Swift, HTML5.	[3] с. 8-42
Тема № 3. Інструменти і середовища розробки мобільних додатків 1. Характеристика та порівняння типів додатків (натівний додаток, веб-додаток, гібридний додаток). 2. Інструменті розробки мобільних додатків (Java, JDK, SDK, Android Studio, Android Eclipse, Intel XDK, Intel Beacon Mountain). 3. Інтегроване середовище розробки.	[3] с. 29-69 [8] с. 39-90
Тема № 4. Середовище розробки платформи Android 1. Установка та налаштування інструментів розробки додатків Android. 2. Налаштування інструментів розробки додатків Android Studio. 3. Встановлення Java та Android Studio.	[1] 23-33
Тема № 5. Побудова інтерактивних програм 1. Основні крокі в створенні інтерактивних програм. 2. Зв'язування макету з активністю.	[1] с. 33-105
Тема № 6. Множинні активності та інтенти 1. Послідовність дій створення додатків із множинною активністю. 2. Створення базової програми з однією активністю та макетом.	[1] с. 105-147
Тема № 7. Користувацький інтерфейс 1. Ключові макети та компонентів графічного інтерфейсу. 2. Типи активностей: активності верхнього рівня, активності категорій та активності деталізації/редагування. 3. Адаптер масив. Фрагменти.	[1] с. 147-301
Тема № 8. Робота з базами даних 1. Структура бази даних SQLite. 2. Спільна робота потоків. 3. Потоки у фоновому режимі роботи бази.	[1] с. 469-579
Тема № 9. Безпека мобільних застосувань 1. Загрози мобільній безпеці. 2. Найкращі методи захисту мобільних пристроїв. 3. Моделі системи безпеки ОС Android.	[2] с. 1-11 [7] с. 15-53
Тема № 10. Месенджери миттєвого обміну повідомленнями та захист мобільних і хмарних обчислювальних середовищах 1. Безпечний миттєвий обмін повідомленнями. 2. Найбезпечніші месенджери повідомлень. 3. Захист мобільних і хмарних обчислювальних середовищах.	[7] с. 55-103

5. Індивідуальні навчально-дослідні завдання

Індивідуальне завдання (розрахунково-графічне завдання) – форма організації навчання, яка має на меті поглиблення, узагальнення та закріплення знань, які студенти отримують у процесі навчання, а також застосування цих знань на практиці. Студенти виконують за даною програмою різновид індивідуального завдання – індивідуальне навчально-дослідні завдання (ІНДЗ) на тему: «Робота на мобільній платформі Android».

Вимоги до аналітичної записки: структура записки – зміст, вступ, виклад основного матеріалу, висновки (порівнянна характеристика параметрів

електронних схем), список використаних джерел (не менш 10 джерел); обсяг не менш 20 сторінок; форма представлення – електронна з використанням стилів оформлення тексту, автоматизованим формуванням змісту, посилань на джерела, ілюстрації, виноски тощо.

Захист індивідуальних завдань складає 30 балів від 100 бального підсумкового модульного контролю з дисципліни і включає : аналітична записка – 10 балів, практикум формування штатного розкладу організації – 10 балів, співбесіда по матеріалам індивідуального завдання – 10 балів.

6. Методи навчання

В навчальному плані для вивчення дисципліни передбачені такі організаційні форми занять як лекції практичні та лабораторні заняття.

На лекційних заняттях викладаються теоретичні засади тем, що вивчаються, а також приклади їх використання для розв’язання конкретних навчальних задач.

На практичних та лабораторних заняттях студенти досліджують під керівництвом викладача прийоми розв’язання типових задач.

Перед лабораторним заняттям студент повинен вивчити певний теоретичний матеріал і виконати завдання у відповідності до методичних вказівок до лабораторних занять з дисципліни. Після закінчення лабораторного заняття студент надає звіт з лабораторної роботи та виконує захист результатів роботи.

Основним видом інформаційно-методичного забезпечення дисципліни є:

- конспект лекцій;
- методичні вказівки до практичних та лабораторних занять;
- навчальні посібники з дисципліни.

Перелічені складові елементи інформаційно-методичного забезпечення існують як у друкованому вигляді так і в електронній формі, а також у вигляді електронного навчального комплексу з дисципліни.

7. Перелік питань та завдань, що виносяться на підсумковий контроль

Питання для проведення заліку та екзамену з дисципліни

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.

8. Критерії та засоби оцінювання результатів навчання здобувачів

Контрольні заходи оцінювання результатів навчання включають в себе поточний та підсумковий контролі. Засобами оцінювання результатів навчання можуть бути екзамени (комплексні екзамени); тести; наскрізні проекти; командні проекти; аналітичні звіти, реферати, есе; розрахункові та розрахунково-графічні роботи; презентації результатів виконаних завдань та досліджень; завдання на лабораторному обладнанні, тренажерах, реальних об'єктах тощо; інші види індивідуальних та групових завдань.

Поточний контроль. До форм поточного контролю належить оцінювання:

- рівня знань під лабораторних занять;
- якості виконання самостійної роботи.

Поточний контроль здійснюється під час проведення практичних занять і має на меті перевірку набутих здобувачем вищої освіти (далі – здобувач) знань, умінь та інших компетентностей з навчальної дисципліни.

У ході поточного контролю проводиться систематичний вимір приросту знань, їх корекція. Результати поточного контролю заносяться викладачем до журналів обліку роботи академічної групи за національної системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Оцінки за самостійну роботу виставляються в журналі обліку роботи академічної групи окремою графою за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»). Результати цієї роботи враховуються під час виставлення підсумкових оцінок.

При розрахунку успішності здобувачів враховуються такі види робіт: навчальні заняття (лабораторні тощо); самостійна робота (виконання домашніх завдань, ведення конспектів першоджерел та робочих зошитів, виконання розрахункових завдань, підготовка рефератів, наукових робіт, публікацій, розроблення спеціальних технічних пристроїв і приладів, моделей, комп’ютерних програм, виступи на наукових конференціях, семінарах та інше); контрольні роботи (виконання тестів, контрольних робіт у формі, передбаченій в робочою програмою навчальної дисципліни). Вони оцінюються за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Здобувач, який отримав оцінку «незадовільно» за навчальні заняття або самостійну роботу, зобов’язаний перескласти її.

Загальна кількість балів (оцінка), отримана здобувачем за семестр перед підсумковим контролем, розраховується як середньоарифметичне значення з оцінок за навчальні заняття та самостійну роботу, та для переводу до 100-бальної системи помножується на коефіцієнт **10.**

Загальна кількість балів (перед підсумковим ***=((Результат навчальних занять за семестр + Результат самостійної роботи за семестр) / 2) *10***

контролем)

Підсумковий контроль. Підсумковий контроль проводиться з метою оцінки результатів навчання на певному ступені вищої освіти або на окремих його завершених етапах.

Для обліку результатів підсумкового контролю використовується поточно-накопичувальна інформація, яка реєструються в журналах обліку роботи академічної групи. Результати підсумкового контролю з дисциплін відображуються у відомостях обліку успішності, навчальних картках здобувачів, залікових книжках. ***Присутність здобувачів на проведенні підсумкового контролю (заліку, екзамену) обов'язкова.*** Якщо здобувач вищої освіти не з'явився на підсумковий контроль (залік, екзамен), то науково-педагогічний працівник ставить у відомість обліку успішності відмітку «не з'явився».

Підсумковий контроль (екзамен, залік) оцінюється за національною шкалою. Для переводу результатів, набраних на підсумковому контролі, з національної системи оцінювання в 100-бальну вводиться коефіцієнт **10**, таким чином максимальна кількість балів на підсумковому контролі (екзамені, заліку), які використовуються при розрахунку успішності здобувачів, становить **50.**

Підсумкові бали з навчальної дисципліни визначаються як сума балів, отриманих здобувачем протягом семестру, та балів, набраних на підсумковому контролі (екзамені, заліку).

$$\textit{Підсумкові бали навчальної дисципліни} = \textit{Загальна кількість балів (перед підсумковим контролем)} + \textit{Кількість балів за підсумковим контролем}$$

Здобувач вищої освіти, який під час складання підсумкового контролю (екзамен, залік) отримав незадовільну оцінку, складає його повторно. Повторне складання підсумкового екзамену чи заліку допускається не більше двох разів з кожної навчальної дисципліни: один раз – викладачеві, а другий – комісії, до складу якої входить керівник відповідної кафедри та 2-3 науково-педагогічних працівники.

Якщо дисципліна вивчається протягом двох і більше семестрів з семестровим контролем у формі екзамену чи заліку, то результат вивчення дисципліни в поточному семестрі визначається як середньоарифметичне значення балів, набраних у поточному та попередньому семестрах.

$$\textit{Підсумкові бали навчальної дисципліни} = \frac{\textit{Підсумкові бали за поточний семестр} + \textit{Підсумкові бали за попередній семестр}}{2}$$

У цьому розділі також повинні бути розроблені чіткі критерії оцінювання здобувачів вищої освіти під час поточного контролю *(робота на семінарських, практичних, лабораторних та інших аудиторних заняттях, самостійна робота, виконання індивідуальних творчих завдань)* та підсумкового контролю. Кафедра визначає вимоги до здобувачів стосовно засвоєння змісту навчальної дисципліни, а саме: кількість оцінок, яку він повинен отримати під час аудиторної роботи, самостійної роботи. Наприклад:

Робота під час навчальних занять	**Самостійна робота**	**Підсумковий контроль**
Отримати не менше 4 позитивних оцінок	Підготувати реферат, підготувати конспект за темою самостійної роботи, виконати практичне	Отримати за підсумковий контроль не менше 30

	завдання тощо	балів

9. Шкала оцінювання: національна та ECTS

Оцінка в балах		Оцінка за національною шкалою	Оцінка	
			Оцінка	Пояснення
12	**97-100**	Відмінно («зараховано»)	A	**«Відмінно»** – теоретичний зміст курсу засвоєний **цілком,** необхідні практичні навички роботи з освоєним матеріалом сформовані, **усі** навчальні завдання, які передбачені програмою навчання, **виконані** в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
11	**94-96**			
10	**90-93**			
9	**85-89**	Добре («зараховано»)	B	**«Дуже добре»** – теоретичний зміст курсу засвоєний **цілком**, необхідні практичні навички роботи з освоєним матеріалом **в основному** сформовані, **усі** навчальні завдання, які передбачені програмою навчання, **виконані**, якість виконання **більшості** з них оцінено числом балів, близьким до **максимального,** робота з двома - трьома незначними помилками.
8	**80-84**			
7	**75 – 79**		C	**«Добре»** – теоретичний зміст курсу засвоєний **цілком**, практичні навички роботи з освоєним матеріалом **в основному** сформовані, **усі** 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 незначними помилками, або з однією – двома значними помилками.
6	**70-74**	Задовільно («зараховано»)	D	**«Задовільно»** – теоретичний зміст курсу засвоєний **частково**, але **прогалини не 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.
5	**65-69**			
4	**60-64**		E	**«Достатньо»** – теоретичний зміст курсу засвоєний **частково, деякі** практичні навички роботи **не сформовані, частина** передбачених програмою навчання навчальних завдань **не виконана** або якість виконання деяких з них оцінено числом балів, близьким до **мінімального**, робота, що задовольняє мінімуму критеріїв оцінки.
3	**40–59**	Незадовільно («не зараховано»)	FX	**«Умовно незадовільно»** – теоретичний зміст курсу засвоєний **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.
2	**21-40**			
1	**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 значного **підвищення якості** виконання навчальних завдань, робота, що потребує повної переробки.

10. 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., 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.

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

SKIA graphics library in chrome: first impressions. URL: http://www.atoker.com/blog/2008/09/06/skia-graphics-library-in-chrome-first-283