КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015

Кафедра інженерії програмного забезпечення та кібербезпеки

ЗАТВЕРДЖЕНО
вченою радою КНТЕУ
(пост. п. 17 від «25» 11 2021 р.)
Ректор
_____ А. А. Мазаракі

БЕЗПЕКА МОБІЛЬНИХ ДОДАТКІВ / SECURITY OF MOBILE APPS

ПРОГРАМА / COURSE SUMMARY

Київ 2021

Автори: Т.О. ЖИРОВА, кандидат педагогічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Н.О. КОТЕНКО, кандидат педагогічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки
В.В. ТОКАР, докт. екон. наук, професор кафедри інженерії програмного забезпечення та кібербезпеки,

Програму розглянуто і затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки «15» листопада 2021 р., протокол № 12.

Рецензенти: А.М. ДЕСЯТКО, PhD, доцент кафедри інженерії програмного забезпечення та кібербезпеки;
О.О. РУДЕНКО, SFCC Front-End Team Lead, Raccoon LLC;

БЕЗПЕКА МОБІЛЬНИХ ДОДАТКІВ / SECURITY OF MOBILE APPS

ПРОГРАМА / COURSE SUMMARY

ВСТУП

Програма дисципліни «Безпека мобільних додатків» призначена для студентів освітнього ступеня «магістр» галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека», спеціалізації «Безпека систем електронних комунікацій в економіці».

Програму підготовлено відповідно до Стандарту вищої освіти України за даною спеціальністю та відповідної освітньо-професійної програми підготовки магістрів КНТЕУ.

Програма складається з таких розділів:

1. Мета, завдання та предмет дисципліни.
2. Передумови вивчення дисципліни як вибіркової компоненти освітньої програми
3. Результати вивчення дисципліни.
4. Зміст дисципліни.
5. Список рекомендованих джерел.

1. МЕТА, ЗАВДАННЯ ТА ПРЕДМЕТ ДИСЦИПЛІНИ

Метою викладання дисципліни «Безпека мобільних додатків» є формування у майбутніх спеціалістів умінь та компетенцій для забезпечення захисту інформації в мобільних ОС.

Завданням вивчення дисципліни «Безпека мобільних додатків» є теоретична та практична підготовка майбутніх фахівців з таких питань:

- основні загрози для мобільного ПЗ;
- захист інформації в мобільних ОС;
- безпека Apple iOS;
- безпека Google Android;
- тестування безпеки мобільних додатків.

Предметом вивчення дисципліни є сукупність теоретичних і практичних проблем, які пов’язані з інструментальними засобами та методами забезпечення захисту інформації в мобільних ОС.

2. ПЕРЕДУМОВИ ВИВЧЕННЯ ДИСЦИПЛІНИ ЯК ВИБІРКОВОЇ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ

знання: основ кібербезпеки;

вміння: працювати з офісними додатками Microsoft, хмарними сервісами Office 365, пошуковою системою Google.

3. РЕЗУЛЬТАТИ ВИВЧЕННЯ ДИСЦИПЛІНИ

Дисципліна «Безпека мобільних додатків», як вибіркова компонента освітньої програми, забезпечує оволодіння студентами загальними та фаховими компетентностями і досягнення ними програмних результатів навчання за відповідною освітньо-професійною програмою:

Безпека систем електронних комунікацій в економіці (ОС магістр, ОП 2022 р.)

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Загальні компетентності за освітньою програмою		
КЗ-1	Здатність застосовувати знання у практичних ситуаціях.	1-10
КЗ-2	Здатність проводити дослідження на відповідному рівні.	1-10
КЗ-5	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).	1-10
Фахові компетентності за освітньою програмою		
КФ1	Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.	4-10
КФ2	Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.	1-3

Програмні результати навчання за освітньою програмою		
РН4	Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	4-10
РН6	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	5-10
РН7	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	1-3
РН20	Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.	
РН23	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.	5-10

4. ЗМІСТ ДИСЦИПЛІНИ

Тема 1. Вступ. Історія розвитку мобільних додатків та їх класифікація

Вступ. Мета та завдання дисципліни, її місце в освітньому процесі.

Сучасні мобільні пристрої (мобільний телефон, комунікатор, смартфон, планшет) та еволюція розвитку їх екосистем. Сучасні мобільні платформи: огляд, критерії оцінювання та порівняння.

Основні загрози для мобільного ПЗ. Характеристики сучасних бездротових технологій передачі даних: Wi-Fi, Bluetooth, NFC, Wireless Application Protocol. Покоління мереж мобільного зв'язку: 3G, 4G, 5 G. Принципи взаємодії мобільних додатків з web-сайтми та хмарними технологіями.

Стандарти комп'ютерно-технічної експертизи: SWGDE.

Список рекомендованих джерел

Основний: 2, 4.

Додатковий: 6-8

Інтернет-джерела: 10-17.

Тема 2. Захист інформації в мобільних ОС

Основні загрози для мобільних пристроїв. Аналіз ризиків та методика ліквідації загроз. Практичні аспекти захисту інформації у системах мобільного зв'язку стандарту GSM. Платформи безпеки мобільних ОС.

Огляд сучасного мобільного противірусного ПЗ. Особливості забезпечення безпеки, механізми автентифікації, цілісності, конфіденційності та анонімності.

Практичні аспекти захисту інформації в системах мобільного зв'язку з кодовим розподілом каналів стандарту IS-95. Програмні засоби протидії загрозам інформації: розділення коду і даних; кордони безпеки, партиціювання; перевірка прав компонентів, що викликаються; використання capabilities; модель можливостей; файли конфігурації, Code Access Permission.

Список рекомендованих джерел

Основний: 1-5.

Додатковий: 8.

Інтернет-джерела: 11, 13, 18.

Тема 3. Загальні принципи безпеки і конфіденційності даних мобільних пристроїв

Техніки захисту даних. Безпека та ізоляція ПЗ. Шифрування файлів і дисків. Безпечне апаратне забезпечення пристроїв. Безпечне

резервне копіювання та робота з хмарними системами. Модель загроз.

Конфіденційні дані мобільних пристроїв: IMEI, MEID/ESN та інші дані абонента стільникової мережі; контакти, адресна книга, календар, нотатки тощо; журнали вхідних та вихідних дзвінків; SMS, MMS, миттєві повідомлення; файли: аудіо, відео, документи; електронна пошта; активність браузера: історія, закладки; GPS та геолокаційні дані; соціальні мережі: облікові записи, контент; SIM/UICC, провайдер, IMSI, MSISDN і т.д.

Список рекомендованих джерел

Основний:1, 2, 4.

Додатковий: 6-8

Інтернет-джерела: 10-17.

Тема 4. Безпека Apple iOS

Основні принципи роботи додатків Apple iOS. Огляд еволюції захисту Apple iOS: шифрування даних, від кодів до біометрії, SEP-архітектура і посилення апаратних компонентів пристроїв, iCloud Keychain.

Сучасний захист даних користувачів iOS: аутентифікація, підпис коду додатків, пісочниця та аналіз коду, шифрування. Class key шифрування: повний захист (CP), захищено поки не відкрито (PUO), повний захист даних (CP) після того, як файл було створено та закрито, захист до першої автентифікації користувача – першого розблокування (AFU).

Ієрархія ключів iOS Data Protection. Keychain, резервне копіювання, iCloud і iCloud Keychain, SEP: TouchID і FaceID. Обробка ключа Secure Enclave Processor. Робота Apple TouchID и FaceID.

Актуальні техніки обходу користувацьких даних iOS. Джейлбрейк та програмні експлойти. Підбір паролів. Оцінка часу перебору цифрових паролей в iOS. Взлом SEP. Обхід блокування екрану. Локальне вилучення даних. Вилучення даних з хмари.

Список рекомендованих джерел

Основний: 1, 2, 4, 5.

Додатковий: 6-8

Інтернет-джерела: 10, 16, 17.

Тема 5. Підвищення захисту Apple iOS

Зменшення фронту атак. Підсилення захисту даних. Динамічний захист даних. Наскрізне шифрування бекапів і iCloud. Ліквідація особливих випадків обходу шифрування. Паролі і локальні бекапи. Підсилення iCloud Keychain. Обмеження на USB-інтерфейс. Обмеження на режими DFU і JTAG. Прозорість і функціональні протиріччя. Вплив iOS-спільнот.

Список рекомендованих джерел

Основний: 1, 2, 4, 5.

Додатковий: 6-8

Інтернет-джерела: 10, 16, 17.

Тема 6. Безпека Google Android

Основні принципи роботи додатків Google Android. Огляд еволюції захисту Android: ізольоване середовище додатків, шифрування даних, контроль цілісності APK (Android Package), надійність апаратного забезпечення.

Сучасний захист даних користувача Android: аутентифікація, пісочниця для додатків, шифрування, знімний носій даних (SD-картка), апаратні елементи безпеки, Android Verified Boot (AVB), Google Mobile Services, підпис APK і перевірка коду, резервне копіювання, повідомлення і відеозвязок.

Шифрування: повне шифрування диску, файлове шифрування, поєднання шифрування на основі Файлів з шифруванням метаданих.

Список рекомендованих джерел

Основний: 1, 2, 4, 5.

Додатковий: 6-8

Інтернет-джерела: 10, 16, 17.

Тема 7. Техніки обходу захисту користувацьких даних та підвищення захисту Android

Отримання рут-доступу і використання експлойтів. Альтернативні і потенційні техніки обходу захисту. Атака на довірене апаратне та програмне забезпечення. Брутфорс пароля і паттерна. Локальне вилучення даних інструментами форензики. Вилучення даних із Google Cloud.

Шифрування даних користувача під час блокування екрану. Використання наскрізного шифрування для обміну повідомленнями та інших продуктів Google. Безпечний доступ в роботі з прошивкою. Посилення компонентів апаратної частини. Підвищення частоти оновлення Android.

Список рекомендованих джерел

Основний: 1, 2, 4, 5.

Додатковий: 6-8

Інтернет-джерела: 10, 16, 17.

Тема 8. Тестування безпеки мобільних додатків

Основні поняття тестування ПЗ. Типи тестування мобільних додатків: тестування зручності використання, тестування сумісності,

тестування інтерфейсу, тестування сервісів, тестування ресурсів низького рівня, тестування продуктивності, тестування експлуатації, тестування встановлення, тестування безпеки.

Стратегія тестування мобільних додатків. Техніки тестування безпеки мобільних додатків. Автентифікація, авторизація, безпека даних, уразливості для злому, управління сеансами.

Список рекомендованих джерел

Основний: 5.

Додатковий: 6

Інтернет-джерела: 9, 11, 12, 14, 15, 16.

Тема 9. Інструменти тестування безпеки мобільних додатків

Тестування програмних додатків для мобільних пристроїв, на предмет їх функціональності, зручності використання, безпеки, продуктивності. Інструменти тестування мобільних додатків: ImmuniWeb MobileSuite; Zed Attack Proxy; Kiuwan; QARK; Micro Focus; Android Debug Bridge; CodifiedSecurity; Drozer; WhiteHat Security; Synopsys; Veracode; Mobile Security Framework.

Список рекомендованих джерел

Основний: 5.

Додатковий: 6

Інтернет-джерела: 9, 11, 12, 14, 15, 16.

Тема 10. Автоматизація тестування безпеки мобільних додатків

Види тестів в тестуванні API: оглядове тестування, юзабіліті тестування, тестування безпеки, тестування безпеки, автоматизація тестування, тестування документації.

Дефекти, які виявляються під час API тестування: збій обробки помилкових умов; невикористані прапори; відсутній або дублюється функціонал; питання надійності: труднощі при підключенні і отриманні відповіді від API; проблеми з безпекою; питання багатопоточності; проблеми з продуктивністю: час відгуку API дуже високо; помилкові дефекти; некоректна обробка валідних значень; дані відповіді некоректно структуровані (JSON або XML).

Інструменти для роботи з API: Postman, jMeter, Fiddler, SoapUI, Runscope, Advanced REST Client.

Список рекомендованих джерел

Основний: 5.

Додатковий: 6

Інтернет-джерела: 9, 11, 12, 14, 15, 16.

5. СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

1. Шматко О.В. Аналіз методів і технологій розробки мобільних додатків для платформи Android : навч. посіб. / О. В. Шматко, А. О. Поляков, В. М. Федорченко. – Харків : НТУ «ХПІ», 2018. – 284 с.
2. Бурячок В.Л. Технології забезпечення безпеки мережевої інфраструктури. Підручник / В.Л. Бурячок, А.О. Аносов, В.В. Семко, В.Ю. Соколов, П.М. Складанний. – К.:КУБГ, 2019. –218 с.
3. Gupta B. B. Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives (Security, Privacy, and Trust in Mobile Communications) Auerbach Publications; 1st edition (September 30, 2020) 694 pages
4. *Хорошко О.В. Захист систем електронних комунікацій: навч.посіб./ В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ: Київ. нац. торг.-екон. ун-т, 2019. – 164 с.*
5. Khorikov V. Unit Testing Principles, Practices, and Patterns: Effective testing styles, patterns, and reliable automation for unit testing, mocking, and integration testing with examples in C# 1st Edition./ Vladimir Khorikov – Apress ,January 14, 2020. – 304 p.

Додатковий

6. Інформаційна безпека: навчальний посібник / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник, А.П. Бондарєв та інші; за заг. ред. д-ра техн. наук, проф. Ю.Я. Бобала та д-ра техн. наук, доц. І.В. Горбатого. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.
7. Бурячок В.Л. Основи інформаційної та кібернетичної безпеки. Навчальний посібник / В.Л. Бурячок, Р.В. Киричок, П.М. Складанний – К. , 2018. – 320 с.
8. Соколов В.Ю. Безпека безпроводових і мобільних мереж : Лабораторний практикум / В. Ю. Соколов, М. Тадж-Діні / ред. перекл. О. П. Райтер. — К. : ДУТ, 2018. — 122 с.

Інтернет-джерела

9. Implementing Automated Software Testing – Continuously Track Progressand Adjust Accordingly. – URL: http://www.methodsandtools.com/archive/archive.php?id=94
10. Мобільні віруси. Виявлення та протидія. – URL: https://www.mil.gov.ua/ukbs/mobilni-virusi-viyavlennya-ta-protidiya.html
11. 10 Best Mobile App Security Testing Tools 2021. – URL: https://uk.myservername.com/10-best-mobile-app-security-testing-tools-2021#Recommended_Reading
12. Автоматизація тестування мобільних додатків. – URL: https://uk.myservername.com/11-best-automation-tools
13. Мобільні віруси. виявлення та протидія. URL: https://www.mil.gov.ua/ukbs/mobilni-virusi-viyavlennya-ta-protidiya.html
14. Тестування мобільних додатків. – URL: https://qagroup.com.ua/publications/testuvannia-mobilnykh-dodatkiv-vid-a-do-ia/
15. Підходи до тестування мобільних додатків. – URL: https://training.qatestlab.com/blog/technical-articles/approaches-to-testing-mobile-applications/
16. Що таке OWASP? Топ 10 вразливостей. – URL: https://training.qatestlab.com/blog/technical-articles/what-is-owasp-top-10-vulnerabilities/
17. Принципи забезпечення безпеки архітектури інформаційної системи на базі клієнтських додатків для ОС Android. – URL: https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/156
18. CDMA: IS-95. URL: https://www.osp.ua/nets/2000/03/141014

** Курсивом виділені назви видань, які знаходяться в бібліотеці КНТЕУ.*