Назва дисципліни		Програмне забезпечення захисту інформації в мобільних пристроях			
Рівень вищої освіти		Другий (магістерський) рівень			
Назва спеціальності		Комп'ютерні науки та інформаційні технології			
Назва спеціалізації		Програмне забезпечення систем захисту інформації			
Форма навчання		денна			
Кафедра, що забезпечує		Інформатики та управління захистом інформаційних систем			
курс	5	семестр	9	**Викладач**	Трифонова К.О.
А	**Мета і задачі дисципліни**				
	Метою дисципліни «Програмне забезпечення захисту інформації в мобільних пристроях» є поглиблене вивчення сучасних атак на мобільні пристрої, проектування та розробка програмного забезпечення захисту інформації в мобільних пристроях. Основними *задачами* дисципліни є: вивчення архітектури платформи Android; 2. отримання теоретичних та практичних навичок розробки мобільних додатків на платформі Android; 3. дослідження моделі забезпечення безпеки в Android; 4. розгляд особливостей між процесорного обміну інформацій; 5. дослідження та захист від атак на мобільні пристрої, що використовують вразливості базових мобільних технологій, 6. дослідження та захист від атак на мобільні пристрої, що використовують вразливості технологій SMS, 7. дослідження та захист від атак на мобільні пристрої, що використовують вразливості технологій Bluetooth; 8. аналіз вірусів для Android, огляд існуючих антивірусів для Android; 9. захист даних, що передаються по мережі, VPN-з'єднання та Android, проект Tor в Android, мережа I2P.				
В	**Тематика дисципліни**				
	1. Основи платформи Android 1.1. Рівень ядра: драйвер IPC , управління енергоспоживанням, драйвери обладнання 1.2. Рівень бібліотек: системна бібліотека libc, менеджер поверхонь, функціональні бібліотеки 1.3. Середовище виконання: Dalvik Virtual Machine, Core Libraries 1.4. Рівень каркаса додатків 1.5. Рівень додатків 2. Розробка мобільного додатку в Android 2.1. Віртуальні пристрої Android 2.2. Вивчення структури додатку в Android 2.3. Побудова користувальницького інтерфейсу з використанням елементів управління 2.4. Життєвий цикл додатку 2.5. Відладка мобільного додатку 3. Дослідження безпеки та служб, заснованих місці розташування 3.1. Модель забезпечення безпеки в Android 3.1.1.Огляд концепцій, пов'язаних з безпекою 3.1.2.Підпис додатків для розгортання 3.2. Перевірка безпеки системи під час виконання 3.2.1.Безпека на межі процесів 3.2.2.Визначення та використання прав доступу 3.2.3.Спеціальні права доступу 3.2.4.Права доступу URI до та робота з ними 3.3. Робота зі службами, заснованими не місці розташування 3.3.1. Пакет Mapping 3.3.2.Пакет Location 4. Побудова та застосування служб 4.1. Застосування HTTP-служб				

	4.1.1. Застосування HttpClient для побудови запитів HTTP GET 4.1.2. Застосування HttpClient для побудови запитів HTTP POST 4.1.3.Робота з виключеннями 4.1.4.Розв'язок задач, що пов'язані з багатопоточністю 4.2. Забезпечення між процесорного обміну інформацій 4.2.1.Побудова простої служби 4.2.2. Служби в Android 4.2.3.Локальні служби 4.2.4.Служби AIDL 4.2.5.Визначення службового інтерфейсу на AIDL 4.2.6.Вбудовування AIDL-інтерфейсу 4.2.7.Виклик служби з клієнтського додатку 4.2.8.Передача комплексних типів службам 5. Дослідження та захист від атак на мобільні пристрої 5.1. Атаки, що використовують вразливості базових мобільних технологій 5.2. Атаки, що використовують вразливості технологій SMS 5.3. Атаки, що використовують вразливості технологій Bluetooth 5.4. Атаки, що використовують вразливості мобільних Інтернет - технологій 5.5. Віруси для мобільних пристроїв 5.6. Атаки на мобільні пристрої з розширеними можливостями
C	**Стиль та методика навчання**
Організаційно-методичні форми вивчення	Лекційні та лабораторні заняття
Форми контролю	Поточний контроль, модульні контрольні роботи, індивідуальні завдання, усний екзамен
D	**Компетентності**
	ЗК1. Навички використання інформаційних і комунікаційних технологій. ЗК2. Вміння виявляти, ставити та вирішувати проблеми ЗК8. Знання та розуміння предметної області та розуміння професійної діяльності ЗК9. Визначеність і наполегливість щодо поставлених завдань і взятих обов'язків ЗК10. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. СК10. Здатність оцінювати впливи зовнішніх і внутрішніх факторів на інформаційну безпеку, розробляти програмні методи протидії СК11. Здатність до оцінки ефективності, зокрема обчислювальної складності методів і алгоритмів, що використовуються в програмному забезпеченні систем захисту інформації СК12. Здатність здійснювати протидію несанкціонованому проникненню в ІТ-системи шляхом програмного захисту СК14. Здатність застосовувати інформаційні, комп'ютерні технології для забезпечення захисту інформації в стільникових мережах.
E	**Основні результати навчання**
	РН1. Вміти використовувати методи та правила управління інформацією та роботу з документами за професійним спрямуванням. Володіти методиками та сучасними засобами інформаційних технологій. РН2. Вміти використовувати комунікаційні технології для підтримування гармонійних ділових та особистісних контактів, як передумову ділового успіху. РН3. Знати та розуміти закони та методи міжособистісних комунікацій, норми толерантності, ділових комунікацій у професійній сфері, ефективної праці в колективі, адаптивності. РН4. Уміти складати психологічний портрет людини, підбирати робітників на визначені посади, знаходити шляхи виходу з конфліктної ситуації для ефективного управління персоналом. РН5. Знати та розуміти закономірності, методи та підходи творчої та креативної діяльності, системного мислення у професійній сфері. РН8. Уміння застосовувати знання і розуміння для розв'язання задач, які

	характерні обраній спеціальності. РН9. Вміти використовувати методи та методики проведення наукових та прикладних досліджень. РН10. Знати методологію системних досліджень, методів дослідження та аналізу складних об'єктів та процесів, розуміти їх складність, їх різноманіття, багатофункціональність для розв'язання прикладних завдань в галузі професійної діяльності. РН11. Систематично читати літературу за фахом (у тому числі закордонну), складати реферати, анотації, аналітичні огляди тощо РН12. Знати методи проведення досліджень та вміти аналізувати складність технічних систем, розуміти складність задач оптимізації цих систем та їх елементів, та вдосконалювати методики їх проведення. РН13. Розуміти необхідність бути наполегливим у досягненні мети та якісного виконання робіт у професійній сфері РН14. Вміти чітко, послідовно та логічно висловлювати свої думки та переконання. РН28. Вміти використовувати сучасні математичні методи, моделі, інформаційні технології для розробки, аналізу та вдосконалення програмного забезпечення захисту інформації. РН29. Вміти удосконалювати або розробляти нові програмні методи, алгоритми і засоби забезпечення захисту інформації при її зберіганні, комп'ютерній обробці та передачі РН30. Вміти розробляти нові, використовувати та вдосконалювати існуючі програмні методи перевірки цілісності, автентичності інформації. РН33. Вміти оцінювати впливи зовнішніх і внутрішніх факторів на інформаційну систему. РН34. Вміти оцінювати рівень інформаційної захищеності інформаційних систем, розробляти пропозиції щодо його підвищення РН35. Вміти розробляти додатки для мобільних пристроїв на розповсюджених мовах та технологіях програмування, що забезпечують захист інформації