**(Ф 21.01 - 03)**

|  |  |  |
| --- | --- | --- |
|  | **Силабус навчальної дисципліни**  **«Безпека мобільних додатків»**  **Освітньо-професійної програми**  **«Управління кібербезпекою та захистом інформації»**  **Галузь знань: 12 «**Інформаційні технології **»**  **Спеціальність: 125 «**Кібербезпека та захист інформації**»** | |
| **Рівень вищої освіти**  (перший (бакалаврський), другий (магістерський) | перший бакалаврський рівень | |
| **Статус дисципліни** | Навчальна дисципліна вибіркового компонента ОП | |
| **Курс** | 3 | |
| **Семестр** | 6 семестр | |
| **Обсяг дисципліни,** | кредити ЄКТС-4.0/години - 120 | |
| **Мова викладання** | українська | |
| **Що буде вивчатися (предмет вивчення)** | Основні загрози мобільним додаткам, їх класифікація та методи захисту | |
| **Чому це цікаво/треба вивчати (мета)** | Метою вивчення дисципліни є формування устудентів фундаментальні знання та практичні навички виявлення, аналізу та запобігання загрозам безпеки мобільних додатків. Зростання кібератак на мобільні додатки вимагає підготовки фахівців, здатних аналізувати ризики та впроваджувати ефективні заходи безпеки. Вивчення дисципліни допоможе оволодіти методами кіберзахисту та підготуватися до роботи у сфері інформаційної безпеки. | |
| **Чому можна навчитися (результати навчання)** | дисципліна охоплює сучасні методи захисту мобільних платформ, аналіз атак, захист конфіденційних даних і впровадження кращих практичних безпечних розробок. | |
| **Як можна користуватися набутими знаннями і уміннями (компетентності)** | Отримані знання та навички будуть корисними під час розробки та аудиту безпечних мобільних додатків, тестування на вразливість, впровадження захисту персональних даних. | |
| **Навчальна логістика** | **Зміст дисципліни:** Дисципліна охоплює основи безпеки мобільних додатків, розглядаючи актуальні загрози, статистику атак та ключові виклики. Вивчаються архітектура безпеки операційних систем iOS та Android, механізми контролю доступу та методи захисту даних. Аналізуються розширені загрози, витоки даних, SQL Injection, зворотний інжиніринг та атаки на API. Розглядаються сучасні підходи до безпечної розробки, включаючи шифрування, аутентифікацію, авторизацію та захист API. Значна увага приділяється тестуванню безпеки, виявленню вразливості та методам тестування на проникнення. Вивчаються регуляторні вимоги, такі як GDPR і CCPA, а також стандарти захисту персональних даних. Практична частина включає аналіз реальних інцидентів безпеки та ключів із витоками даних у популярних мобільних сервісах.  **Види занять:** Лекції, лабораторні роботи, самостійна робота студентів.  **Методи навчання:** Лекційний виклад, аналіз кейсів, обговорення проблемних ситуацій, самостійне опрацювання матеріалу та виконання лабораторних робіт.  **Форми навчання:** очна, заочна | |
| **Пререквізити** | Для успішного засвоєння дисципліни "Соціотехнічна безпека" студенти повинні мати базові знання з технологій програмування, комп'ютерні мережі, криптографія | |
| **Пореквізити** | Знання основних принципів кібербезпеки та захисту інформації.  необхідні для аналізу вразливостей мобільних додатків, тестування на проникнення, впровадження заходів захисту інформації та розробки безпечних мобільних систем. Отримані знання можуть бути застосовані в подальшому навчанні, дослідницькій діяльності, аудиті безпеки, тестуванні програмного забезпечення та професійній сертифікації в галузі інформаційної безпеки.  Навички критичного мислення та розпізнавання загроз.  Розуміння соціальних і психологічних аспектів безпеки.  Знання правових норм у сфері безпеки інформації. | |
| **Інформаційне забезпечення**  **з репозитарію та фонду НТБ ДУ «КАІ»** | 1. OWASP Mobile Security Testing Guide (MSTG) [Електронний ресурс] – Режим доступу: https://owasp.org/www-project-mobile-security-testing-guide/ – Дата звернення: 2025.  2. OWASP Mobile Top 10 [Електронний ресурс] – Режим доступу: https://owasp.org/www-project-mobile-top-10/ – Дата звернення: 2025.  3. Drake J. J., Lanier Z., Mulliner C., Oliva P., Ridley S. A., Wicherski G. Android Hacker’s Handbook. – Indianapolis: Wiley, 2014. – 576 с.  4. Miller C., Blazakis D., Dai Zovi D., Esser S., Iozzo V., Weinmann R. P. iOS Hacker’s Handbook. – Indianapolis: Wiley, 2012. – 384 с.  5. Chell D., Erasmus T., Colley S., Whitehouse O. Mobile Application Security. – Birmingham: Wiley, 2015. – 384 с.  6. Tamma R., Mahalik H., Bommisetty S. Practical Mobile Forensics. – Birmingham: Packt Publishing, 2018. – 468 с.  7. Zdziarski J. Hacking and Securing iOS Applications. – Sebastopol: O'Reilly Media, 2012. – 396 с.  8. Chell D., Erasmus T., Colley S., Whitehouse O. The Mobile Application Hacker’s Handbook. – Indianapolis: Wiley, 2016. – 816 с.  9. Tahiri S. Mastering Mobile Forensics. – Birmingham: Packt Publishing, 2016. – 456 с.  10. Google Security Best Practices for Android Developers [Електронний ресурс] – Режим доступу: <https://developer.android.com/training/articles/security-tips> – Дата звернення: 2025.  11. Apple Security Documentation [Електронний ресурс] – Режим доступу: <https://developer.apple.com/security/> – Дата звернення: 2025.  12. IBM X-Force Threat Intelligence Report [Електронний ресурс] – Режим доступу: https://www.ibm.com/security/xforce – Дата звернення: 2025. | |
| **Локація та матеріально-технічне забезпечення** | 11 корпус 118 аудиторія | |
| **Семестровий контроль, екзаменаційна методика** | залік 6 семестр | |
| **Кафедра** | Кафедра Кібербезпеки | |
| **Факультет** |  | |
| **Викладач(і)** | https://lh7-rt.googleusercontent.com/docsz/AD_4nXeOmsZhwrd1NmBpM9OBfZCaNi7aBYo5oVGZIWgKhnt25c_-RYzBfZcR-xxHTyOBS0KkhVavFzuXmqX2_B7rt8hN8ujXRkio_5O38RjIPlrRGETwThcdK1JRFtQtjM4ss_1XyR8p9MZeVQTxiiiWZfs?key=QNch4zSV0KuesPXNTVzDq345 | **ПІБ викладача: Вишневська Наталія Сергіївна**  **Посада: старший викладач**  **Науковий  ступінь:**  **Вчене звання:**  **Профайл викладача:**  **Тел.:**  **E-mail: nataliia.vyshnevska@npp.nau.edu.ua**  **Робоче місце:11 корпус 424 аудиторія** |
| **Оригінальність навчальної дисципліни** | Дисципліна «Безпека мобільних додатків » забезпечує комплексний підхід до оволодіння навчальним матеріалом, що поєднує фундаментальні знання, сучасні методи аналізу вразливостей та практичні навички тестування. Акцентована увага не лише на теоретичних аспектах, але й на реальних кейсах кіберінцидентів, сучасних загрозах та методах їхнього усунення. | |
| **Лінк на дисципліну** |  | |