ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»	**Силабус навчальної дисципліни** **«Технології організації інфраструктури відкритих ключів»** **«Public key infrastructure technologies»** Освітньо-наукова програма: Кібербезпека Спеціальність: F5 Кібербезпека та захист інформації Галузь знань: F Інформаційні технології
Рівень вищої освіти	Третій (освітньо-науковий)
Статус дисципліни	Навчальна дисципліна вибіркового компонента вибору фахового переліку
Курс	1 (перший)
Семестр	2 (другий)
Обсяг дисципліни, кредити ЄКТС/години	5 кредитів / 150 год
Мова викладання	Українська або англійська
Що буде вивчатися (предмет вивчення)	Предметом вивчення дисципліни «Технології організації інфраструктури відкритих ключів» є принципи, архітектури та практичні методи побудови, управління й захисту PKI-систем для забезпечення довіри в інформаційних середовищах.
Чому це цікаво/треба вивчати (мета)	Метою вивчення дисципліни «Технології організації інфраструктури відкритих ключів» є формування глибокого розуміння принципів побудови та управління PKI-системами для забезпечення надійного захисту інформації в сучасних цифрових середовищах.
Чому можна навчитися (результати навчання)	**РН1.** Мати передові концептуальні та методологічні знання з кібербезпеки та захисту інформації і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з кібербезпеки та захисту інформації, отримання нових знань та/або здійснення інновацій. **РН2**. Планувати і виконувати експериментальні та/або теоретичні дослідження з кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямів з використанням сучасних інструментів та дотриманням норм професійної і академічної етики. **РН5**. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень і математичного та/або комп'ютерного моделювання, наявні літературні дані. **РН7**. Застосовувати загальні принципи та методи математики, інформатики та інших наук, а також сучасні методи та інструменти, цифрові технології та спеціалізоване програмне забезпечення для провадження наукових досліджень у сфері кібербезпеки та захисту інформації. **РН8**. Розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямах.
Як можна користуватися набутими знаннями і уміннями (компетентності)	**Загальні компетентності:** **ЗК1**. Здатність до абстрактного мислення, аналізу і синтезу. **ЗК2.** Здатність до пошуку, оброблення та аналізу інформації з різних джерел. **ЗК3.** Здатність працювати в міжнародному контексті.

	ЗК4. Здатність розв'язувати комплексні проблеми предметної області на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності. **Спеціальні (фахові) компетентності:** **СК1.** Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у сфері кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з кібербезпеки та захисту інформації. **СК2.** Здатність ініціювати, розробляти і реалізовувати комплексні наукові та інноваційні проєкти в сфері кібербезпеки та захисту інформації **СК3.** Здатність розв'язувати значущі проблеми в сфері кібербезпеки та захисту інформації., розширювати та переоцінювати наявні знання і професійні практики. **СК4.** Здатність ефективно застосовувати методи аналізу даних, концептуального, математичного та комп'ютерного моделювання, виконувати натурні та обчислювальні експерименти при проведенні наукових і прикладних досліджень у сфері кібербезпеки та захисту інформації. **СК5.** Здатність генерувати нові ідеї щодо розвитку теорії та практики кібербезпеки та захисту інформації, виявляти, ставити та вирішувати проблеми дослідницького характеру, оцінювати та забезпечувати якість виконуваних досліджень. **СК8**. Здатність до застосування сучасних технологій машинного навчання, штучного інтелекту, обробки великих даних, нейронних мереж, високопродуктивних обчислень для їх оптимізації та синтезу їх нових функціональних можливостей у концепції сталого розвитку.
Навчальна логістика	Зміст дисципліни «Технології організації інфраструктури відкритих ключів» охоплює вивчення принципів та архітектури PKI, компонентів систем довіри (центри сертифікації, реєстраційні органи, сховища ключів), життєвого циклу сертифікатів, алгоритмів шифрування та підпису, протоколів і форматів (X.509, TLS, S/MIME, SCEP/EST, ACME), політик безпеки та управління ключами, фізичного й операційного захисту CA, інтеграції PKI з корпоративними та хмарними сервісами, а також аудиту, сертифікації й правових аспектів. Значна увага приділяється практичним навичкам: проєктуванню PKI-рішень для різних сценаріїв (корпоративна, IoT, код-сайнинг, електронна пошта), розгортанню та автоматизації процесів, оцінці ризиків, відновленню після інцидентів та підготовці до використання постквантових алгоритмів. **Види занять:** лекції, практичні. **Методи навчання:** проблемний виклад, дослідницькі методи, презентації, бесіди та дискусії, робота в Google Classroom (електронні лекції, семінари, практичні роботи, дистанційні консультації, тестування). **Форми навчання:** очна, дистанційна.
Пререквізити	Базові знання з дисциплін «Методологія наукових досліджень у сфері кібербезпеки та захисту інформації»

Інформаційне забезпечення	**Навчальна та наукова література:** 1. Інфраструктури відкритих ключів. Електроний цифровий підпис. Теорія та практика ; Автор: Ю.І. Горбенко, І.Д. Горбенко 2. Теорія та практика інфраструктури відкритих ключів. Частина 1. Теорія інфраструктури відкритих ключів С. В. Кондакова. Київ: КНУБА, 2022. 3. «Системи захисту інформації» Ю.В. Костюк, П.М. Складанний, Г.М. Гулак, Б.Т. Бебешко, К.В. Хорольська, С.Л. Рзаєва, підручник, 2025.
Локація та матеріально-технічне забезпечення	Аудиторія теоретичного навчання, Проектор
Семестровий контроль, екзаменаційна методика	Модульна контрольна робота, залік
Кафедра	Кафедра кібербезпеки
Факультет	Факультет комп'ютерних наук та технологій
Викладач(і)	 **ФЕСЕНКО Андрій Олексійович** **Посада:** декан факультету комп'ютерних наук та технологій **Науковий ступінь:** к.т.н. **Вчене звання:** доцент **Профайл викладача:** https://www.scopus.com/authid/detail.uri?authorId=57209857572 **E-mail:** andrii.fesenko@npp.nau.edu.ua **Робоче місце:** 1.416
Оригінальність навчальної дисципліни	Авторський курс, викладання українською або англійською мовами.
Лінк на дисципліну	Після формування групи слухачів створюється кабінет в Google Classroom з необхідними матеріалами для навчання
Максимальна кількість слухачів	20