ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»	**Силабус навчальної дисципліни** **«Квантова та постквантова безпека»** **«Quantum and post-quantum security»** Освітньо-наукова програма: Комп'ютерні науки Спеціальність: F3 Комп'ютерні науки 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
Що буде вивчатися (предмет вивчення)	Предметом дисципліни є вивчення сучасних підходів до забезпечення захисту інформації в умовах розвитку квантових технологій.
Чому це цікаво/треба вивчати (мета)	Метою вивчення дисципліни є формування цілісного уявлення про квантові обчислення з акцентом на принципах розробки й оцінювання квантових алгоритмів, а також ознайомлення з основами квантової інформації, квантової та постквантової криптографії. Більшість традиційних криптографічних алгоритмів базуються на складних математичних задачах, які класичні комп'ютери не здатні ефективно розв'язати за поліноміальний час. Водночас квантові комп'ютери зможуть виконувати такі обчислення за лічені секунди, що призведе до втрати надійності існуючих методів шифрування. Тому в межах дисципліни «Квантова та постквантова безпека» здобувачі освіти опановуватимуть знання та практичні навички щодо використання альтернативних методів і протоколів захисту інформації в постквантовий період.
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:** Вступ до квантової та постквантової безпеки (Основні поняття квантової механіки, що застосовуються у криптографії, Класичні криптографічні системи та їх вразливість до квантових атак, Основні загрози квантових обчислень для інформаційної безпеки). Принципи роботи квантових комп'ютерів (кубіти, суперпозиція, квантове переплутування). Алгоритми Шора та Гровера. Поточний стан квантових комп'ютерів: можливості та обмеження. Протоколи квантового розподілу ключів та інші методи квантової комунікації. Вразливості квантових криптографічних систем. Основні підходи до постквантової криптографії. Оцінка безпеки та ефективності постквантових алгоритмів. Політики безпеки та міжнародні стандарти постквантової криптографії. **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», «Технології захисту критичної інформаційної інфраструктури»

Інформаційне забезпечення	**Навчальна та наукова література:** 1. Квантові інформаційні системи. Навчальний посібник для спеціальності «Прикладна фізика та наноматеріали» / Карлаш Г.Ю. – Київ: факультет радіофізики, електроніки та комп'ютерних систем Київського національного університету імені Тараса Шевченка, 2018. – 77 с. 2. M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, (Cambridge University Press, Cambridge, 2010). 3. Новиков, Д. Технології постквантової криптографії / Д. Новиков, В. Полторак // Адаптивні системи автоматичного управління : міжвідомчий науково-технічний збірник. – 2023. – № 1 (42). – С. 171-183. 4. Vorobets P., Horpenyuk A., Opirskyy I. Transition to post-quantum cryptography: challenges, standardization, and prospects // Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 2, pp. 303-312. 5. Proskurin, D., Gnatyuk, S., Okhrimenko, T. Predicting Pseudo-Random and Quantum Random Number Sequences using Hybrid Deep Learning Models, CEUR Workshop Proceedings, 2023, 3426, p. 77–88	
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)		**ОХРІМЕНКО Тетяна Олександрівна** **Посада:** заступник декана з наукової роботи **Науковий ступінь**: к.т.н. **Вчене звання**: ст. дослідник **Профайл викладача:** https://www.scopus.com/authid/detail.uri?authorId=57210116999 **E-mail:** t.okhrimenko@npp.kai.edu.ua **Робоче місце:** 1.416
Оригінальність навчальної дисципліни	Авторський курс, викладання українською	
Лінк на дисципліну	Після формування групи слухачів створюється кабінет в Google Classroom з необхідними матеріалами для навчання	
Максимальна кількість слухачів	20	