АНОТАЦІЯ
ВИБІРКОВОЇ ДИСЦИПЛІНИ
СТУПІНЬ ВИЩОЇ ОСВІТИ – PhD

Назва дисципліни	**КРИПТОГРАФІЧНИЙ ЗАХИСТ ЦИФРОВОЇ ІНФОРМАЦІЇ**
Кількість кредитів	3 кредити (90 годин)
Назва кафедри	Кафедра алгебри та системного аналізу
ПІБ викладача, науковий ступінь та вчене звання	Тоічкіна Олена Олександрівна, кандидат фізико-математичних наук
Зміст дисципліни	Подаються основні поняття і розділи, що дозволяють отримати уявлення про задачі та проблеми сучасної криптографії. Розглядаються як традиційні питання класифікації й оцінки надійності шифрів, так і системні питання використання криптографічних методів забезпечення конфіденційності та цілісності цифрових даних, орієнтованих на застосування обчислювальної техніки. **Метою** вивчення дисципліни є формування знань про основні принципи криптографічних методів і алгоритмів захисту цифрової інформації, а також практичних навичок безпечної роботи в інформаційних системах. **Завдання** дисципліни полягають у оволодінні теоретичними знаннями про основні методи криптографічного захисту інформації та способи шифрування даних; дослідженні особливостей криптографічних алгоритмів та криптографічних протоколів; формуванні підходів до вибору й організації використання криптографічних засобів захисту інформації. Внаслідок вивчення дисципліни здобувач повинен: **Знати** основні поняття, етапи історичного розвитку, закони й методи криптографічного захисту інформації; принципи побудови сучасних криптосистем; основні вимоги до шифрів та їх характеристики, а також способи шифрування даних; принципи побудови криптографічних алгоритмів та криптографічних стандартів, їх використання в задачах захисту інформації; основні положення нормативно-правового регулювання у галузі криптографічного захисту інформації; основні напрямки розвитку сучасних систем криптографічного захисту інформації; зміст стандартних і складних задач асиметричної криптографії з використанням ІКТ.

	Вміти обирати необхідні криптографічні методи та алгоритми для розв'язання практичних задач інформаційної безпеки; програмно реалізовувати криптографічні алгоритми розв'язання типових задач захисту інформації; використовувати програмні засоби, які реалізують основні криптографічні функції; оцінювати і запобігати загрозам безпеки інформаційних ресурсів методами криптографії
Компетентності	**Загальні:** 1) здатність до критичного аналізу та оцінки сучасного стану науки та формулювання нових підходів для вирішення теоретичних та практичних наукових завдань; 2) здатність планувати науково-професійний та особистий розвиток; 3) здатність саморозвиватися і самовдосконалюватися протягом життя, нести відповідальність за навчання інших; 4) здатність до абстрактного мислення, аналізу та синтезу; 5) здатність до дослідницької незалежності автономності в роботі, до самостійної індивідуальної роботи, здійснення комплексного дослідження, керівництва науко-дослідною групою; 6) здатність використовувати основні методологічні підходи до вивчення природних і суспільних явищ в межах різних типів наукової раціональності; 7) здатність до організації та проведення наукових досліджень в області математики, процесів, відносин із залученням сучасних наукових методів, інформаційних технологій та програмного забезпечення в галузі математики; 8) здатність представляти результати власної наукової діяльності в публікаціях різного виду, їх підготовка на протязі навчання в аспірантурі в тому числі засобами інформаційних технологій, спеціального програмного забезпечення; 9) здатність і готовність очолювати роботу вітчизняної або міжнародної наукової програми чи проекту, бути активним суб'єктом міжнародної наукової діяльності, та співпрацювати із міжнародною науковою спільнотою; 10) здатність застосовувати закони формальної логіки в процесі інтелектуальної діяльності. Вміння робити узагальнення і висновки. 11) здатність до цілеспрямованого накопичування знання; 12) розуміння особливостей розвитку науки. Розуміння сутності та причин наукових революцій, особливостей 4-х загальнонаукових революцій і сутності сучасної наукової революції. Розуміння

	типів наукової раціональності. Вміння розглядати проблеми своєї науки в контексті сучасної наукової ситуації. 13) здатність застосування сучасних інформаційних технологій у науковій діяльності, використовувати основні сучасні інформаційні технології, методи видобування та обробки інформації; 14) здатність застосовувати методи математичного аналізу і моделювання складних систем. **Фахові:** 1) здобуття глибинних знань із спеціальності 111 «Математика» та її розділами, за якими проводяться дослідження; 2) засвоєння основних концепцій, розуміння теоретичних і практичних проблем, історії розвитку та сучасного стану наукових знань з математики; 3) набуття універсальних навичок дослідника математики; 4) здатність застосовувати основні математичні структури, методи сучасної математики, математичні методи аналізу та опису процесів та систем; 5) здатність оцінювати складність криптографічної системи; 6) здатність створювати, оцінювати та застосовувати сучасні криптографічні алгоритми розподілу ключів і цифрового підпису; 7) здатність створювати нові криптографічні алгоритми захисту інформації; 8) здатність оцінювати і запобігати загрозам безпеки інформаційних ресурсів методами криптографії; 9) розуміння змісту стандартних і складних задач асиметричної криптографії з використанням ІКТ; 10) здатність діагностувати, аналізувати і консультувати в галузі ІТ рішень; 11) здатність розробляти інформаційні системи та застосовувати до розробки, аналізу і верифікації алгоритмів і програмних систем і комплексів
На кого орієнтований курс	Для третього освітньо-наукового рівня доктор філософії (PhD) освітніх програм спеціальності 111 «Математика»
Попередня підготовка	Сформовані компетентності, знання та вміння, отримані здобувачами в результаті опанування навчальних кредитів з таких компонент освітньої програми першого та/або другого рівня вищої освіти, як „Лінійна алгебра та аналітична геометрія”, “Дискретна математика”, “Загальна алгебра”, “Алгоритми та структури даних”, “Математична логіка та теорія алгоритмів”
Форма викладання дисципліни	Очна або онлайн за допомогою Zoom та Moodle на «Освітньому порталі»