**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ**
Кафедра комп'ютерних систем, мереж та кібербезпеки

**ЗАТВЕРДЖЕНО**
**Факультет інформаційних технологій**
**02 червня 2025 р**

# РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Основи криптоаналізу»

Галузь знань 12 Інформаційні технології
Спеціальність 125 Кібербезпека
Освітня програма «Кібербезпека»
Факультет (ННІ) інформаційних технологій
Розробники: доцент, к.т.н., доцент, Сагун А.В.
*(посада, науковий ступінь, вчене звання)*

Київ – 2025 р.

## Опис навчальної дисципліни

Дисципліна вивчає основи криптоаналізу, принципи, методи та засоби проведення різних видів криптоаналізу, а також створення систем компрометації шифрованих повідомлень. В курсі вивчаються методи лінійного, диференційного та аналітичного криптоаналізу, допоміжні методи та алгоритми криптоаналізу (алгоритм Евкліда, алгоритм Ферма, частотний аналіз та ін.), базові принципи та методи проведення криптоаналізу в системах симетричних блокових та асиметричних двоключових схемах шифрування, системах електронного цифрового підпису.

| **Галузь знань, спеціальність, освітня програма, освітній ступінь** | | |
|---|---|---|
| Освітній ступінь | *бакалавр* | |
| Спеціальність | *125 – Кібербезпека* | |
| Освітня програма | *Кібербезпека* | |
| **Характеристика навчальної дисципліни** | | |
| Вид | обов'язкова | |
| Загальна кількість годин | 120 | |
| Кількість кредитів ECTS | 4 | |
| Кількість змістових модулів | 2 | |
| Курсовий проект (робота) (за наявності) | - | |
| Форма контролю | *іспит* | |
| **Показники навчальної дисципліни для денної та заочної форм здобуття вищої освіти** | | |
| | **Форма здобуття вищої освіти** | |
| | **денна** | **заочна** |
| Курс (рік підготовки) | 3 | - |
| Семестр | 6 | - |
| Лекційні заняття | *30 год.* | *год.* |
| Практичні, семінарські заняття | *год.* | *год.* |
| Лабораторні заняття | *30 год.* | *год.* |
| Самостійна робота | *60 год.* | *год.* |
| Кількість тижневих аудиторних годин для денної форми здобуття вищої освіти | *4 год.* | |

### 1. Мета, компетентності та програмні результати навчальної дисципліни

Мета вивчення дисципліни «Основи криптоаналізу» є ознайомлення з основними теорії чисел, числових полів та аналітичної алгебри, надання студентам знань з основ криптоаналізу, принципів, методів та засобів проведення різних видів криптоаналізу, а також створення систем компрометації шифрованих повідомлень.

***Набуття компетентностей:***

***Інтегральна компетентність (ІК):*** здатність застосовувати знання та розуміння основ криптоаналізу у практичних ситуаціях професійної діяльності, здійснювати моніторинг, аналіз і оцінку вразливостей криптографічних систем в межах впровадженої політики інформаційної та кібербезпеки, використовуючи методи і засоби контролю за інформаційними процесами.
***Загальні компетентності (ЗК):*** здатність застосовувати знання у практичних ситуаціях; знання та розуміння предметної області і розуміння професійної діяльності.
***Спеціальні (фахові) компетентності (СК):*** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою; здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
***Програмні результати навчання (ПРН***): застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності; застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення; Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

## 2. Програма та структура навчальної дисципліни

| **Назви змістових модулів і тем** | **Кількість годин** | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **денна форма** | | | | | | | **заочна форма** | | | | | |
| | тижні | усього | у тому числі | | | | | усього | у тому числі | | | | |
| | | | л | п | лаб | інд | с.р. | | л | п | лаб | інд | с.р. |
| **Змістовий модуль 1. Симетричні криптосистеми та методи їх криптоаналіз** | | | | | | | | | | | | | |
| **Тема 1.** Вступ до курсу. Задачі криптоаналізу. Основні терміни і формулювання. | 1 | 2 | 2 | | - | | - | | | | | | |
| **Тема 2.** Види та системи криптоаналізу. Криптоаналіз симетричних шифрів. Частотний статистичний криптоаналіз. | 2 | 14 | 2 | | 4 | | 8 | | | | | | |
| **Тема 3**. Методи статистичного (частотного) та повного перебору шифрограми Цезаря та Віженера. Криптоаналіз шифрів простої заміни методом статистичних властивостей тексту | 4 | 12 | 2 | | 4 | | 6 | | | | | | |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Тема 4.** Методи криптоаналізу шифрів підстановки та перестановки. Криптоаналіз шифрів підстановки (афінних). | 6 | 8 | 4 | | 4 | | - | | | | | | |
| **Тема 5.** Методи криптоаналізу симетричних блокових шифрів. | 7 | 8 | 2 | | - | | 6 | | | | | | |
| **Тема 6.** Лінійний та диференційний криптоаналіз. Криптоаналіз симетричних шифрів аналітичним методом. | 8 | 8 | 2 | | 2 | | 4 | | | | | | |
| **Разом за модулем 1** | | **52** | **14** | | **14** | | **24** | | | | | | |
| **Змістовий модуль 2. Методи криптоаналізу асиметричних криптосистем** | | | | | | | | | | | | | |
| **Тема 7.** Криптоаналіз асиметричних криптоалгоритмів. Основні методи показники криптостійкості | 9 | 2 | 2 | | | | - | | | | | | |
| **Тема 8.** Методи криптоаналізу асиметричних криптосистем. Проблеми факторизації алгоритму RSA. Обчислювальна складність факторизації | 10 | 14 | 2 | | 6 | | 6 | | | | | | |
| **Тема 9.** Тести простоти для параметрів асиметричних криптосистем. Проблема генерування простих чисел для криптосхеми DSA. Тест Мілера-Рабіна. Тест простоти Люка | 12 | 16 | 4 | | 4 | | 8 | | | | | | |
| **Тема 10.** Оцінка параметрів хеш-функції для застосування в задачах криптології (обчислювальна складність, сумісність, цілісність). | 13 | 2 | 2 | | - | | - | | | | | | |
| **Тема 11.** Елементи криптоаналізу односторонніх (хеш-функцій) | 13 | 18 | 4 | | 2 | | 12 | | | | | | |
| **Тема 12.** Потокові шифри. Шифри сімейства A5. Шифр «СТРУМОК». Криптоаналіз та стійкість потокових шифрів. | 15 | 16 | 2 | | 4 | | 10 | | | | | | |
| **Разом за модулем 2** | | **68** | **16** | | **16** | | **36** | | | | | | |
| **Усього годин за курс** | | **120** | **30** | | **30** | | **60** | | | | | | |

## 3. Теми лекцій

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| 1 | Основні поняття, визначення, принципи криптоаналізу | 2 |

| | | |
|---|---|---|
| 2 | Статистичний криптоаналіз | 2 |
| 3 | Криптоаналіз простих шифрів. Шифр Віженера | 4 |
| 4 | Криптоаналіз лінійних і зсувних шифрів. Властивості криптоаналізу афінних шифрів | 4 |
| 5 | Побудова та методи криптоаналізу криптографічних алгоритмів. Принципи Керкхофа | 2 |
| 6 | Диференційний та лінійний криптоаналізу симетричних шифрів | 2 |
| 7 | Криптоаналіз асиметричних криптоалгоритмів. Визначення криптостійкості | 2 |
| 8 | Криптоаналіз асиметричних криптосистем. Криптоаналіз RSA | 2 |
| 9 | Тести простоти для параметрів асиметричних криптосистем | 4 |
| 10 | Криптостійкість односторонніх геш-функцій та методи криптоаналізу геш-функцій. Криптографічна сіль | 2 |
| 11 | Потокові шифри та їх базові вразливості. Шифри A5, "Струмок". Постулати Голомба | 4 |
| 12 | Методи криптоаналізу потокових шифрів | 2 |

## 4. Теми лабораторних занять

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| 1 | Основи частотного криптоаналізу | 4 |
| 2 | Криптоаналіз шифрів простої заміни методом статистичних властивостей тексту | 4 |
| 3 | Криптоаналіз шифрів підстановки (афінних) | 4 |
| 4 | Лінійний криптоаналіз. Криптоаналіз симетричних шифрів аналітичним методом | 4 |
| 5 | Методи криптоаналізу асиметричних криптосистем. Факторизація алгоритму RSA | 6 |
| 6 | Криптоаналіз асиметричних криптоалгоритмів. Тести простоти. Тест Мілера-Рабіна. Тест простоти Люка | 4 |
| 7 | Елементи криптоаналізу асиметричних криптосистем та їх компонент (хеш-функцій) | 2 |
| 8 | Потокові шифри. Стійкість та криптоаналіз потокових шифрів | 4 |

## 5. Теми самостійної роботи

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| 1 | Методи частотного аналізу поліалфавітних шифрів підстановки | 8 |
| 2 | Криптоаналіз поліалфавітних шифрів з використанням індексі збігів | 6 |
| 3 | Диференційний криптоаналіз симетричного шифру на базі мережі Файстеля | 6 |
| 4 | Аналітичний криптоаналіз симетричних шифрів | 4 |
| 5 | Криптоаналіз асиметричного криптоалгоритму RSA з невідомими початковими даними | 6 |
| 6 | Формування сертифікату простоти для асиметричних схем | 8 |
| 7 | Криптоаналіз геш-функцій, захищених "сіллю" та веселкових таблиць | 12 |
| 8 | Криптоаналіз генератора ключової гами потокових шифрів на базі незвідних поліномів | 10 |

## 6. Методи та засоби діагностики результатів навчання:

***(вибрати необхідне чи доповнити)***

– усне або письмове опитування;

– співбесіда;
– тестування;
– захист лабораторних робіт;
– пірінгове оцінювання, самооцінювання.

**7. Методи навчання *(вибрати необхідне чи доповнити):***

– метод проблемного навчання;
– метод практико-орієнтованого навчання;
– метод командної роботи, мозкового штурму
– метод гейміфікованого навчання.

**8. Оцінювання результатів навчання.**

Оцінювання знань здобувача вищої освіти відбувається за 100-бальною шкалою і переводиться в національну оцінку згідно чинного «Положення про екзамени та заліки у НУБіП України».

### 8.1. Розподіл балів за видами навчальної діяльності

| Вид навчальної діяльності | Результати навчання | Оцінювання |
|---|---|---|
| **Змістовий модуль 1.** | | |
| Лабораторна робота 1 - Основи частотного криптоаналізу | застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності; | 4 |
| Лабораторна робота 2 - Криптоаналіз шифрів простої заміни методом статистичних властивостей тексту | | 6 |
| Лабораторна робота 3 - Криптоаналіз шифрів підстановки (афінних) | | 5 |
| Лабораторна робота 4 - Лінійний криптоаналіз. Криптоаналіз симетричних шифрів аналітичним методом | Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. | 4 |
| Самостійна робота 1 - Методи частотного аналізу поліалфавітних шифрів підстановки | | 2 |
| Самостійна робота 2 - Криптоаналіз поліалфавітних шифрів з використанням індексі збігів | | 3 |
| Самостійна робота 3 - Диференційний криптоаналіз симетричного шифру на базі мережі Файстеля | застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення; | 3 |
| Самостійна робота 4 – Аналітичний криптоаналіз симетричних шифрів | | 2 |
| Модульна контрольна робота 1 | Контроль засвоєння матеріалу | **5** |
| **Всього за модулем 1** | | **34** |
| **Змістовий модуль 2.** | | |
| Лабораторна робота 5 - Методи криптоаналізу асиметричних | застосовувати знання й розуміння математики та фізики в професійній | 4 |

| | | |
|---|---|---|
| криптосистем. Факторизація алгоритму RSA | діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення; | |
| Лабораторна робота 6 - Криптоаналіз асиметричних криптоалгоритмів. Тести простоти. Тест Мілера-Рабіна. Тест простоти Люка. | Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. | 4 |
| Лабораторна робота 7 - Елементи криптоаналізу асиметричних криптосистем та їх компонент (хеш-функцій) | застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення; | 5 |
| Лабораторна робота 8 Потокові шифри. Стійкість та криптоаналіз потокових шифрів | Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. | 7 |
| Самостійна робота 5 - Криптоаналіз асиметричного криптоалгоритму RSA з невідомими початковими даними | | 2 |
| Самостійна робота 6 - Формування сертифікату простоти для асиметричних схем | Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. | 2 |
| Самостійна робота 7 - Криптоаналіз геш-функцій, захищених "сіллю" та веселкових таблиць | застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення; | 3 |
| Самостійна робота 8 - Криптоаналіз генератора ключової гами потокових шифрів на базі незвідних поліномів | | 3 |
| Модульна контрольна робота 2 | Контроль засвоєння матеріалу | **5** |
| **Всього за модулем 2** | | |
| | | **(М1 + М2)*0,7 ≤ 70** |
| **Екзамен** | | **30** |
| **Всього за курс** | | **(Навчальна робота + екзамен) ≤ 100** |

## 8.2. Шкала оцінювання знань здобувача вищої освіти

| Рейтинг здобувача вищої освіти, бали | Оцінка за національною системою (екзамени/заліки) |
|---|---|
| 90-100 | відмінно |
| 74-89 | добре |
| 60-73 | задовільно |
| 0-59 | незадовільно |

## 8.3. Політика оцінювання

| | |
|---|---|
| **Політика щодо** | Роботи, які здаються із порушенням термінів без поважних причин, |

| | |
|---|---|
| **дедлайнів та перескладання** | оцінюються на нижчу оцінку (пропорційно інтервалів пропущеної дати складання). Перескладання модульних контрольних та тестів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний). |
| **Політика щодо академічної доброчесності** | Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних девайсів). Лабораторні роботи мають бути виконані виключна за індивідуальними завданнями варіантів. |
| **Політика щодо відвідування** | Відвідування занять є обов'язковим. За об'єктивних причин (хвороба, участь в заходах від кафедри або факультету, міжнародне стажування). В узгоджених офіційно випадках навчання може відбуватись індивідуально (в он-лайн формі) |

## 9. Навчально-методичне забезпечення:

## 10. Рекомендовані джерела інформації

Електронний навчальний курс навчальної дисципліни (на навчальному порталі НУБіП України eLearn - https://elearn.nubip.edu.ua/course/view.php?id=4936), що складається з:

- лекцій та їх презентації (в електронному вигляді);
- завдань для виконання лабораторних та самостійних завдань;
- модульних контрольних робіт;
- блоку підсумкового оцінювання знань.
- методичні матеріали щодо вивчення навчальної дисципліни для здобувачів вищої освіти денної та заочної форм здобуття вищої освіти;
- програма навчальної дисципліни.

## 11.Рекомендовані джерела інформації

1. УДК 004.9:336.74(О75) Основи криптоаналізу: навчальний посібник. Сагун А.В., Хайдуров В.В., Нікітенко Є.В., Мамченко С.М. – Київ : НУБіП України, 2024. –23.

2. Dooley F. John History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms – Springer, 2018. – URL: https://books.google.com.ua/books?id=q61qDwAAQBAJ&printsec =frontcover&hl=uk#v=onepage&q&f=false

**Допоміжні:**

1. Фільштінський В. А. Математичні основи криптографії: конспект лекцій для студ. спец. 7.080202 "Прикладна математика" денної форми навчання / В. А. Фільштінський, А. В. Бережний.– Суми: СумДУ, 2011. – 138 с.

2. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C. – John Wiley & Sons, 2015. – 784 p. – URL: https://books.google.com.ua/books?id=VjC9BgAAQBAJ&printsec =frontcover&hl=uk#v=onepage&q&f=false