**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ**

# СИЛАБУС ВИБІРКОВОГО ОСВІТНЬОГО КОМПОНЕНТУ

# «ОСНОВИ КРИПТОГРАФІЇ»

Мова навчання – ***українська***

Шифр та найменування галузі знань ***12 «Інформаційні технології»***

Код та найменування спеціальності ***122 «Комп'ютерні науки»***

Освітньо-професійна програма ***Інформаційні управляючі системи та технології, Інформаційні технології проєктування***

Ступінь вищої освіти ***бакалавр***

Затверджено на засіданні

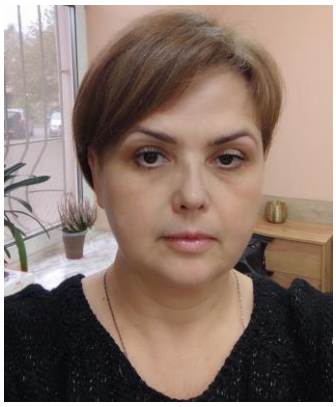
Методичної Ради зі спеціальності ***122 Комп'ютерні науки, 123 Комп'ютерна інженерія***

*«  »  2024 р. протокол №  .*

Реєстраційний номер в навчальному відділі НЦООП

_____

## 1. Загальна інформація



**Кафедра:** Інформаційних технологій та кібербезпеки

**Викладач:** **Владімірова Валентина Борисівна,** старший викладач кафедри інформаційних технологій та кібербезпеки

**Контакти:**
vladimirova.v.b@gmail.com
**Профайл** 048-720-91-18

**Освітній компонент викладається на *2* курсі у *4* семестрі**
**Кількість: кредитів - 5, годин – 150**

| **Аудиторні заняття, годин:** | всього | лекції | практичні | лабораторні |
|---|---|---|---|---|
| **денна** | 54 | 26 | 8 | 20 |
| **заочна** | 12 | 6 | 2 | 4 |
| **Самостійна робота, годин** | Денна – 96 | | Заочна – 138 | |

**Розклад занять**

## 2. Анотація освітнього компоненту

Освітній компонент (ОК) «ОСНОВИ КРИПТОГРАФІЇ» забезпечує ознайомлення здобувачів освіти з теоретичними основами сучасної криптографії та призначений для здобуття навичок у практичному використанні криптоалгоритмів.

Освітній компонент «Основи криптографії» базується на знаннях, отриманих здобувачем вищої освіти в результаті вивчення освітніх компонент «Вища математика», «Алгоритмізація та програмування», «Теорія алгоритмів», «Комп'ютерна схемотехніка, архітектура комп'ютерів та комп'ютерні мережі».

## 3. Мета освітнього компоненту

Мета освітнього компоненту – оволодіння теоретичними основами сучасної криптографії для розуміння суті інформаційних процесів в криптографічних системах.

Основними завданнями вивчення дисципліни «Основи криптографії» є оволодіння теоретичними знаннями про основні криптографічні методи захисту інформації, оволодіння основними способами шифрування даних, виокремлення особливостей криптографічних алгоритмів та криптографічних протоколів.

У результаті вивчення освітнього компоненту студенти повинні знати:

- математичні основи криптографії;
- основні означення сучасної криптографії;
- принципи криптографічного захисту інформації;
- основні симетричні криптоалгоритми (історичні та сучасні);
- основні асиметричні криптоалгоритми (історичні та сучасні);
- основні поняття та аспекти ідентифікації та автентифікації об’єкта;
- моделі криптографічних протоколів;
- механізми та протоколи керування ключами.

У результаті вивчення освітнього компоненту студенти повинні вміти:

- працювати з технічною літературою і документацією;
- оперувати математичними основами понять та методів криптографії;

- вірно визначити та використати криптографічні методи захисту інформації для самостійного розв'язання поставленої задачі;
- забезпечити достовірність та цілісність інформації (зокрема з використанням алгоритмів електронного цифрового підпису) під час обробки інформації, її зберігання і передачі.

## 4. Компетентності та програмні результати навчання

У результаті вивчення освітнього компоненту «ОСНОВИ КРИПТОГРАФІЇ» здобувач вищої освіти отримує наступні програмні компетентності та програмні результати навчання, які визначені в Стандарті вищої освіти зі спеціальності 122 КОМП'ЮТЕРНІ НАУКИ та освітньо-професійній програмі «Інформаційні управляючі системи та технології» підготовки бакалаврів.

### Інтегральна компетентність

Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі комп'ютерних наук або у процесі навчання, що передбачає застосування теорій та методів інформаційних технологій і характеризується комплексністю та невизначеністю умов.

### Загальні компетентності:

**ЗК1** Здатність до абстрактного мислення, аналізу та синтезу.
**ЗК6** Здатність вчитися й оволодівати сучасними знаннями.
**ЗК7** Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
**ЗК11** Здатність приймати обґрунтовані рішення.
**ЗК12** Здатність оцінювати та забезпечувати якість виконуваних робіт.
**ЗК16** Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких проявів недоброчесності.

### Спеціальні (фахові, предметні) компетентності:

**СК1** Здатність до математичного формулювання та досліджування неперервних та дискретних математичних моделей, обґрунтовування вибору методів і підходів для розв'язування теоретичних і прикладних задач у галузі комп'ютерних наук, аналізу та інтерпретування.
**СК3** Здатність до логічного мислення, побудови логічних висновків, використання формальних мов і моделей алгоритмічних обчислень, проєктування, розроблення й аналізу алгоритмів, оцінювання їх ефективності та складності, розв'язності та нерозв'язності алгоритмічних проблем для адекватного моделювання предметних областей і створення програмних та інформаційних систем.
**СК14** Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

### Програмні результати навчання:

**ПР1** Застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук.
**ПР2** Використовувати сучасний математичний апарат неперервного та дискретного аналізу, лінійної алгебри, аналітичної геометрії, в професійній діяльності для розв'язання задач теоретичного та прикладного характеру в процесі проєктування та реалізації об'єктів інформатизації.
**ПРН15** Розуміти концепцію інформаційної безпеки, принципи безпечного проєктування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

## 5. Інформаційний обсяг освітнього компоненту

### 5.1 Перелік лекційних занять

| Тема | Зміст теми | Кількість годин | |
|---|---|---|---|
| | | денна | заочна |
| **Змістовний модуль 1.** ВИДИ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ ІНФОРМАЦІЇ. СИМЕТРИЧНІ КРИПТОГРАФІЧНІ СИСТЕМИ | | | |
| 1 | Введення до курсу «Основи криптографії». Історія розвитку криптографії. Принципи криптографічного захисту. Основні поняття та терміни сучасної криптографії. Математичні основи криптографії. Узагальнена модель криптографічної системи | 2 | 1 |
| 2 | Класифікація методів криптографічного перетворення інформації. Класичні симетричні криптосистеми. Шифри перестановки | 2 | 0,5 |
| 3 | Шифри підстановки. Система Цез. Сисема Цезаря з ключовим словом.аря. Афінна система Цезаря | 2 | 0,5 |
| 4 | Цифри підстановки, Таблиці Трисемуса. Біграмний шифр Плейфейра. Криптосистема Хилла. | 2 | |
| 5 | Шифри складної заміни. Система шифрування Віжинера. Шифр «подвійний квадрат» Вітстона. Одноразова система шифрування . Шифрування методом Вернама. Метод гамування. | 2 | |
| 6 | Сучасні симетричні системи. Алгоритм Lucifer. Американські стандарти шифрування DES, AES. Алгоритм шифрування IDEA. Блочні та потокові сучасні криптосистеми | 2 | |
| **Змістовний модуль 2.** КРИПТОГРАФІЧНІ СИСТЕМИ З ВІДКРИТИМ КЛЮЧЕМ | | | |
| 7 | Концепція криптографічних системи з відкритим ключем. Узагальнена схема асиметричної криптосистеми (з відкритим ключем) . Односпрямовані функції. Криптосистема шифрування даних RSA. Безпека криптосистеми RSA. | 4 | 2 |
| 8 | Криптосистема Ель-Гамаля. Схема Поліга –Хелмана. | 2 | |
| 9 | Ідентифікація та перевірка дійсності. Геш-функції. Електронний цифровий підпис. Алгоритми електронного цифрового підпису (RSA, Ель-Гамаля, алгоритми з додатковими функціональними можливостямі) | 4 | 2 |
| 10 | Управління криптографічними ключами. Генерація, зберігання та розподіл ключів. Алгоритми розподілу ключів. | 2 | |
| 11 | Криптосистема на основі еліптичних кривих | 2 | |
| **Разом за ОК:** | | **26** | **6** |

### 5.2 Перелік практичних робіт

| № з/п | Назва практичної роботи | Кількість годин | |
|---|---|---|---|
| | | денна | заочна |
| 1 | Конгруенції та їх основні властивості. Алгоритми швидкого піднесення до степені | 2 | 1 |
| 2 | Розв’язок конгруенцій першого ступеня | 2 | 1 |
| 3 | Квадратичні лишки | 2 | |
| 4 | Первісні корені | 2 | |
| **Всього за ОК:** | | **8** | **2** |

### 5.3 Перелік лабораторних робіт

| № з/п | Назва лабораторної роботи | Кількість годин | |
|---|---|---|---|
| | | денна | заочна |
| 1 | Шифри перестановки | 2 | |
| 2 | Шифри простої заміни | 4 | 2 |
| 3 | Біграмні шифри | 2 | |
| 4 | Шифрування методом гамування | 2 | |

| | | | |
|---|---|---|---|
| 5 | Асиметричні криптосистеми (RSA) | 4 | 1 |
| 6 | Електронний цифровий підпис (RSA) | 4 | 1 |
| 7 | Метод Диффи-Хелмана | 2 | |
| **Всього за ОК:** | | **20** | **4** |

**5.4 Перелік завдань до самостійної роботи**

| № з/п | Назва теми | Кількість годин | |
|---|---|---|---|
| | | денна | заочна |
| 1 | Опрацювання лекційного матеріалу з відповідями на тестові питання за темами лекцій | 26 | 12 |
| 2 | Підготовка до лабораторних занять | 24 | 6 |
| 3 | Опрацювання теоретичних відомостей, які не виносяться на лекції, а саме: | 26 | 42 |
| 4 | Виконання індивідуальних навчально-дослідних завдань:<br>1. Система шифрування Віжинера<br>2. Криптосистема Ель-Гамаля | <br>10<br>10 | <br>10<br>10 |
| **Всього за ОК:** | | **96** | **138** |

## 6. Система оцінювання та вимоги

Контроль успішності навчання здобувача проводиться у формах вхідного, поточного і підсумкового контролів.

Вхідний контроль якості навчання здійснюється на початку курсу проведенням перевірки залишкових знань здобувачів за ОК, що забезпечують вивчення даного освітнього компоненту (діагностика первинних знань здобувачів).

Формами поточного контролю є:

- тестування знань здобувачів за певних тем або з певних окремих питань ОК;
- виконання і захист лабораторних робіт;
- виконання і захист індивідуальних завдань.

Підсумковий контроль – ***екзамен.***

**Нарахування балів:**

| Вид роботи, що підлягає контролю | Максимальна кількість оціночних балів | |
|---|---|---|
| | Денна | Заочна |
| **Змістовний модуль 1**. ВИДИ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ ІНФОРМАЦІЇ. СИМЕТРИЧНІ КРИПТОГРАФІЧНІ СИСТЕМИ | | |
| Лабораторні роботи* | 24 | 24 |
| Самостійна робота (опрацювання лекційного матеріалу, виконання тестових завдань)* | 5 | 5 |
| Самостійна робота (виконання індивідуальних завдань)* | 6 | 6 |
| Всього за змістовний модуль 1 | **35,0** | **35** |
| **Змістовний модуль 2.** КРИПТОГРАФІЧНІ СИСТЕМИ З ВІДКРИТИМ КЛЮЧЕМ | | |
| Лабораторні роботи* | 22 | 24 |
| Самостійна робота (опрацювання лекційного матеріалу, виконання тестових завдань)* | 5 | 5 |
| Самостійна робота (виконання індивідуальних завдань)* | 6 | 6 |

| | | |
|---|---|---|
| Всього за змістовний модуль 2 | **35** | **35** |
| Екзамен | **30,0** | **30,0** |
| Всього | **100,0** | |

*Є можливість визнання результатів неформальної освіти відповідно до п.2 Положення про порядок перезарахування результатів навчання (навчальних дисциплін) в Одеському національному технологічному університеті.

**Критерії оцінювання програмних результатів навчання здобувачів**

**Підсумковий контроль – екзамен**

| | | |
|---|---|---|
| 27-30 балів | якщо здобувач демонструє повні й глибокі знання навчального матеріалу, достовірний рівень розвитку умінь і навичок, правильне й обґрунтоване формулювання практичних висновків, уміння приймати необхідні рішення в різних нестандартних ситуаціях, вільне володіння науковими термінами, високу комунікативну культуру | відмінно |
| 23-26 балів | якщо здобувач виявляє дещо обмежені знання навчального матеріалу, допускає окремі несуттєві помилки й неточності | дуже добре |
| 18-22 бали | якщо здобувач засвоїв основний навчальний матеріал, володіє необхідними уміннями та навичками для вирішення стандартних завдань, проте при цьому допускає неточності, не виявляє самостійності суджень, демонструє недоліки комунікативної культури | задовільно |
| 0-17 балів | якщо здобувач не володіє необхідними знаннями, уміннями й навичками, науковими термінами, демонструє низький рівень комунікативної культури | незадовільно |

**Лабораторні роботи**

| | | |
|---|---|---|
| **5,2 - 6 балів** | Лабораторна відпрацьована та вчасно захищена, надані повні обґрунтовані відповіді | відмінно |
| **4,6 - 5,1 балів** | Лабораторна відпрацьована та вчасно захищена, при відповіді допущені неточності | дуже добре |
| **3,9 – 4,5 балів** | Лабораторна відпрацьована, відповіді неповні, допущені помилки | добре |
| **2,1 – 3,8 балів** | Лабораторна відпрацьована, відповіді незадовільні, допущені грубі помилки | достатньо |
| **0-2 балів** | Лабораторна не відпрацьована або дані незадовільні відповіді | незадовільно |

**Самостійна робота (тестування: опрацювання лекційного матеріалу)**

| | | |
|---|---|---|
| **4,5 - 5 балів** | 90 - 100 % правильних відповідей | відмінно |
| **4,0 - 4,4 балів** | 74 – 89% правильних відповідей | дуже добре |
| **3,5 – 3,9 балів** | 60 – 73% правильних відповідей | добре |
| **2,1 – 3,4 балів** | 35 – 59 % правильних відповідей | достатньо |
| **0-2 балів** | 0-35 % правильних відповідей | незадовільно |

**Самостійна робота (індивідуальне завдання)**

| | | |
|---|---|---|
| **5,2 - 6 балів** | Самостійна робота відпрацьована та вчасно захищена, надані повні обґрунтовані відповіді | відмінно |
| **4,6 - 5,1 балів** | Самостійна робота відпрацьована та вчасно захищена, | дуже добре |

| | | |
|---|---|---|
| | при відповіді допущені неточності | |
| **3,9 – 4,5 балів** | Самостійна робота відпрацьована, відповіді неповні, допущені помилки | добре |
| **2,1 – 3,8 балів** | Самостійна робота відпрацьована, відповіді незадовільні, допущені грубі помилки | достатньо |
| **0-2 балів** | Самостійна робота не відпрацьована або дані незадовільні відповіді | незадовільно |

## 7. Засоби діагностики успішності навчання

**Методи навчання**, які використовуються у процесі проведення занять, а також самостійних робіт за ОК:

***Лекційні заняття**: Словесні методи: розповідь, пояснення, бесіда, дискусія; Наочні: ілюстрація (мультимедійна презентація), спостереження, демонстрація; пояснювально-демонстративний метод, проблемний виклад.*

***Лабораторні заняття:** виконання лабораторних дослідів з наступних захистом результатів досліджень.*

***Практичні заняття**: групове обговорення питання.*

***Самостійна робота**: робота з навчально-методичними матеріалами, тестування за результати опрацювання теоретичного матеріалу, оцінка виконання індивідуальних завдань; складання планової та звітної документації, науково-дослідна робота студентів (методи пізнання, аналогій, оцінка, ілюстрація тощо)*

## 8. Інформаційні ресурси

**Базові (основні):**

1. Вишняков, Володимир Михайлович. Захист інформації в комп'ютерних системах [Електронний ресурс] : навч. посіб. / В. М. Вишняков ; Київ. нац. ун-т будівництва і архітектури. – Київ, 2022. –120 с. https://repositary.knuba.edu.ua/handle/123456789/11349

2. Захист інформації в комп'ютерних системах [Електронний ресурс] : підручник / В. Д. Козюра, В. О. Хорошко, М. Є. Шелест та ін. – Чернігів, 2020. – 236 с. http://ir.stu.cn.ua/123456789/19248

3. Владімірова, В. Б. Технології захисту інформації : метод. вказівки до самост. роботи [Електронний ресурс] : для здобувачів освіти галузі знань 12 "Інформаційні технології" спец. 122 "Комп’ютерні науки" освітньої програми "Інформаційні управляючі системи та технології" / В. Б. Владімірова ; зав. каф. В. Плотніков ; Каф. інформаційних технологій та кібербезпеки. – Одеса : ОНАХТ, 2022. – 35 с. https://elc.library.ontu.edu.ua/library-w/DocumentDescription?docid=OdONAHT.1835285

4. Захист інформації в комп'ютерних мережах [Електронний ресурс] : навч. посіб. / С. Л. Жуковецька, Н. В. Слушна ; Одес. нац. акад. харч. технологій. — Одеса : ОНАХТ, 2025. — 132 с.
https://elc.library.ontu.edu.ua/library-w/DocumentDescription?docid=OdONAHT.3082391

5. Захист інформації в комп'ютерних мережах: посібник до виконання лабораторних робіт [Електронний ресурс] : для студентів, що навчаються за спец. 123 "Комп’ютерна інженерія" / С. Л. Жуковецька, Н. В. Слушна ; Каф. комп'ютерної інженерії. — Одеса : ОНТУ, 2025. — 62 с. https://elc.library.ontu.edu.ua/library-w/DocumentDescription?docid=OdONAHT.3086440

**Додаткові:**

1. Закон України "Про інформацію". [Онлайн]. Доступно: https://zakon.rada.gov.ua/laws/show/2657-12#Text

2. Криптографія, результати пошуку // Будстандарт Online [Сайт]. URL: https://online.budstandart.com/ua/catalog/searchdoc.html?request=%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F&langbs=ua

**9. Політика освітнього компоненту**

Політика всіх освітні х компонент в ОНТУ є уніфікованою та визначена з урахуванням законодавства України, Корпоративному кодексу, Кодексу академічної доброчесності ОНТУ, Положення про організацію освітнього процесу ОНТУ, Положення про порядок перезарахування результатів навчання (навчальних дисциплін) в ОНТУ, вимог ISO 9001:2015 та роботодавців

Викладач /ПІДПИСАНО/ Валентина ВЛАДІМІРОВА

Розглянуто та затверджено на засіданні кафедри_____

Протокол від «____»_____2024 р. № ___

Завідувач кафедри /ПІДПИСАНО/ Павло ЛОМОВЦЕВ

ПОГОДЖЕНО:

Гарант ОП ІУСТ
*посада, назва кафедри* /ПІДПИСАНО/ Алла СЕЛІВАНОВА
Гарант ОП ІТП
*посада, назва кафедри* /ПІДПИСАНО/ Павло ЛОМОВЦЕВ