Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Кафедра прикладної математики

# КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФРМАЦІЇ

## Робоча програма навчальної дисципліни (Силабус)

| Реквізити навчальної дисципліни | |
|---|---|
| **Рівень вищої освіти** | ***Перший (бакалаврський)*** |
| **Галузь знань** | *11 Математика та статистика* |
| **Спеціальність** | *113 Прикладна математика* |
| **Освітня програма** | *Наука про дані та математичне моделювання* |
| **Статус дисципліни** | *Вибіркова* |
| **Форма навчання** | *Очна (денна)* |
| **Рік підготовки, семестр** | *2 курс, весняний семестр* |
| **Обсяг дисципліни** | *4 кредити* |
| **Семестровий контроль/ контрольні заходи** | *Залік* |
| **Розклад занять** | *Лекції – 1 раз на тиждень (18 лекцій)*<br>*Лабораторні заняття – 1 раз на тиждень (18 занять)* |
| **Мова викладання** | *Українська* |
| **Інформація про керівника курсу / викладачів** | Лектор: *к.ф.-м.н., Бай Юлія Петрівна, ju.p.bai@gmail.com*<br>Лабораторні: *Бай Юлія Петрівна, ju.p.bai@gmail.com* |
| **Розміщення курсу** | - |

## Програма навчальної дисципліни

### 1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

*Дисципліна «Криптографічні методи захисту інформації» є областю прикладних та інженерно-технічних досліджень, що заснована на фундаментальних поняттях математики, фізики, теорії інформації. Криптографія необхідна в основному для збереження державної таємниці, військової таємниці, а також комерційної, юридичної, лікарської та інших. Основними завданнями сучасної криптографії є забезпечення конфіденційності інформації, впевненість у відсутності змін в інформації, що передається, встановлення автентичності джерела переданих повідомлень, неможливість відмови від факту вчинення певних дій. Предметом вивчення навчальної дисципліни є симетричні та асиметричні методи шифрування інформації, можливості застосування криптоаналізу, а також вивчення криптографічних протоколів.*

***Метою*** *кредитного модуля є формування у студентів здатностей:*

- *розуміти основні аспекти застосування сучасної криптографії;*
- *виконувати шифрування та розшифрування інформації за допомогою симетричних та асиметричних алгоритмів;*
- *оцінювати теоретичну і практичну стійкість шифрів;*
- *здійснювати криптоаналіз інформації, зашифрованої з використанням класичних алгоритмів;*
- *розуміти основні криптографічні протоколи та сфери їх застосування.*

***Основні завдання кредитного модуля.***

*Згідно з вимогами програми навчальної дисципліни, студенти після засвоєння кредитного модуля мають продемонструвати такі результати навчання:*

***знання:***

- *історичні етапи розвитку методів захисту інформації*
- *основні терміни і поняття криптографії;*
- *традиційні методи захисту інформації, такі як шифр Цезаря, шифр Тритемія, шифр Віженера, шифр двійкового гамування;*
- *основні симетричного криптографічні алгоритми потокового шифрування (DES, AES);*
- *класичні асиметричні алгоритми шифрування - RSA, Діффі-Хелмана, Ель-Гамаля;*
- *принципи створення електронного цифрового підпису з використанням асиметричних алгоритмів;*
- *методи аналізу стійкості криптографічних систем;*
- *базові стандарти в галузі криптографічного захисту інформації.*

***уміння:***

- *використовувати сучасні симетричні та асиметричні криптографічні методи для шифрування конфіденційної інформації;*
- *використовувати систему електронного цифрового підпису;*
- *застосовувати методи захисту інформації в автоматизованих системах;*
- *моделювати алгоритми криптографічних перетворень та елементи криптографічного аналізу;*

***досвід:***

- *програмування алгоритмів шифрування та розшифрування інформації та їх застосування для захисту конфіденційної інформації ;*
- *створення та використання електронного цифрового підпису;*
- *обґрунтування та висування пропозицій щодо стандартних криптографічних систем і протоколів захисту ресурсів в інформаційних системах;*
- *здійснення загальної оцінки якості криптографічного захисту інформації в комп'ютерних системах та мережах.*

## 2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

*Дисципліна базується на знаннях і навичках, які студенти одержали при вивченні наступних дисциплін: «Дискретна математика», «Програмування», «Програмування на мові Python», «Алгоритми і структури даних», «Теорія ймовірності».*

*Дисципліна забезпечує засвоєння студентами наступних дисциплін: «Бази даних та інформаційні системи» навчального плану підготовки бакалаврів за спеціальністю 113 Прикладна математика.*

## 3. Зміст навчальної дисципліни

***Розділ 1. «Основні поняття криптографії. Криптографія з симетричним ключем»***

*Тема 1.1. Базові поняття криптографії. Історичні етапи розвитку КМЗІ.*
*Тема 1.2. Шифри простої та складної заміни.*
*Тема 1.3. Поліалфавітні шифри.*
*Тема 1.4. Криптоаналіз шифрів заміни.*
*Тема 1.5. Прості шифри перестановки.*
*Тема 1.6. Криптоаналіз шифрів перестановки.*
*Тема 1.7. Шифри гамування.*
*Тема 1.8. Сучасні симетричні алгоритми (DES, 3DES, IDEA, AES).*

***Розділ 2. «Криптографія з відкритим ключем»***

*Тема 2.1. Принципи функціонування асиметричних криптографічних алгоритмів.*
*Тема 2.2. Алгоритм RSA: математичні основи та загальна схема застосування.*
*Тема 2.3. Алгоритм Діффі-Хелмана генерації спільного ключа.*
*Тема 2.4. Алгоритм шифрування Ель-Гамаля.*
*Тема 2.5. Хеш-функції та аутентифікація повідомлень.*
*Тема 2.6. Створення електронного цифрового підпису з використанням асиметричних криптографічних алгоритмів. Порівняння алгоритмів.*

***Розділ 3. «Криптографічні протоколи»***

*Тема 3.1. Поняття, задачі й застосування криптографічних протоколів.*

*Тема 3.2. Протоколи аутентифікації та протоколи розподілу й управління ключовою інформацією.*

***Розділ 4. «Основні напрямки розвитку сучасної криптографії. Правові аспекти застосування КМЗІ.»***

*Тема 4.1. Шифрування на еліптичних кривих. Методи диференціального криптоаналізу. Квантова криптографія.*

*Тема 4.2. Правове регулювання криптографічного захисту та ЕЦП в Україні і світі.*

## 4. Навчальні матеріали та ресурси

***Базова література:***


1. *Вербіцький О.В. Вступ до криптології. – Львів: Науково-технічна література, 1998. — 248 с.*
2. *Тарнавський Ю.А. Технології захисту інформації: підручник / Ю. А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.*
3. *Основи криптографічного захисту інформації: підручник / Г.М. Гулак, В.А. Мухачов, В.О. Хорошко, Ю. Є. Яремчук; Ред.: В. О. Дружиніна. – Вінниця: ВНТУ, 2011. – 199 с.*
4. *Бабак В.П. Теоретичні основи захисту інформації: підручник / В.П. Бабак – К.: Кн. вид-во НАУ, 2008. – 752 с.*
5. *Задірака В. К. Комп'ютерна криптологія: Підручник / В.К. Задірака, О.С. Олексюк. – К.: Ін-т кібернетики ім. В.М.Глушкова, 2002. – 504 с.*
6. *Смарт Н. Криптография. – М.: Техносфера, 2005, – 528 с.*
7. *с.*


***Додаткова література:***


1. *Горбенко І.Д. Захист інформації в інформаційно-телекомунікаційних системах : Навч. посіб. для студ. спец. "Комп'ютерні науки", "Комп'ютена інженерія", "Прикладна математика", "Інформаційна безпека" вищ. навч. закл. / І.Д. Горбенко, Т.О. Гріненко. – Х: ХНУРЕ, 2004. – 368 с.*
2. *Ємець В. Сучасна криптографія. Основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів: БаК, 2003. – 144 с.*
3. *Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення: підручник / О.К. Юдін. – Київ: НАУ, 2011. – 639 с.*
4. *Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd edition / Schneier B. – Wiley; 1998. – 758 p.*
5. *Stallings W. Cryptography and Network Security: Principles and Practice, 7th edition / W. Stallings. – Pearson, 2016. – 768 p.*
6. *Smart N. Cryptography Made Simple (Information Security and Cryptography) 1st edition / N. Smart. – Springer, 2016. – 493 p.*
7. *Menezes A.J., Van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. ‑ New York: CRC Press, Inc., 1997. ‑ 795 p.*


## Навчальний контент

## 5. Методика опанування навчальної дисципліни (освітнього компонента)

### 5.1. Лекційні заняття

| *№ з/п* | *Назва теми лекції та перелік основних питань* | *Кількість ауд. годин* |
|---|---|---|
| *1* | *Мета і задачі дисципліни. Основні поняття та визначення. Наука про шифрування. Роль криптографії у захисті даних. Історичні етапи розвитку КМЗІ.* | ***2*** |
| *2* | *Шифри простої та складної заміни. Основи шифрування. Компоненти криптосистеми та їх функціональні характеристики. Перестановка та підстановка Шифри однозначної заміни. Шифр Цезаря. Шифр Атбаш. Полібіанський квадрат. Шифрувальна система Тритемія. Криптоаналіз шифрів однозначної заміни.* | ***2*** |
| *3* | *Поліалфавітні шифри. Диск Альберті. Таблиця Тритемія. Система шифрування Віженера. Роторні машини. Принцип дії роторної машини «Енігма».* | ***2*** |

| № з/п | Назва теми лекції та перелік основних питань | Кількість ауд. годин |
|---|---|---|
| 4 | Криптоаналіз поліалфавітних шифрів. | **2** |
| 5 | Прості шифри перестановки. Шифри простої одинарної перестановки. Шифр блокової одинарної перестановки. Шифри маршрутної та табличної маршрутної перестановки.. Шифри на основі гратів і таблиць. Магічні квадрати. Шифри множинної перестановки. | **2** |
| 6 | Криптоаналіз шифрів одинарної та множинної перестановки. | **2** |
| 7 | Шифри гамування. Основи шифрування. Генерація гами. Шифр Вернама. Шифр «одноразового блокноту». Шифр двійкового гамування. | **2** |
| 8 | Сучасні симетричні алгоритми. Блочні та поточні шифри. Принципи побудови, функціонування та криптоаналізу симетричних блокових алгоритмів шифрування DES (Digital Encryption Standard), ГОСТ 28147-89, AES. | **2** |
| 9 | Принципи функціонування асиметричних криптографічних алгоритмів. Поняття односторонньої функції. Розподіл ключів. | **2** |
| 10 | Алгоритм RSA: математичні основи та загальна схема застосування. | **2** |
| 11 | Алгоритм Діффі-Хелмана генерації спільного ключа. | **2** |
| 12 | Алгоритм шифрування Ель-Гамаля. | **2** |
| 13 | Хеш-функції та аутентифікація повідомлень. | **2** |
| 14 | Створення електронного цифрового підпису з використанням асиметричних криптографічних алгоритмів RSA та Ель-Гамаля. Порівняння алгоритмів. | **2** |
| 15 | Поняття, задачі й застосування криптографічних протоколів. | **2** |
| 16 | Протоколи аутентифікації та протоколи розподілу й управління ключовою інформацією. | **2** |
| 17 | Основні напрямки розвитку сучасної криптографії. Шифрування на еліптичних кривих. Методи диференціального криптоаналізу. Квантова криптографія | **2** |
| 18 | Правове регулювання ЕЦП в Україні та світі. Державний контроль та право суспільства на криптографію. Міжнародні стандарти в сфері КЗІ. Стандартизація в сфері КЗІ в Україні. | **2** |

### 5.2. Лабораторні заняття

| № з/п | Назва та завдання лабораторної роботи | Кількість ауд. годин |
|---|---|---|
| 1 | Розробка криптосистем на основі шифрів Цезаря та Тритемія. | 6 |
| 2 | Розробка криптосистем на основі шифру Віженера та шифру з використанням гамування. | 6 |
| 3 | Стандарти симетричного шифрування DES, 3DES, IDEA, AES. | 6 |
| 4 | Шифрування з відкритим ключем на основі алгоритму RSA. | 6 |
| 5 | Криптографічні асиметричні алгоритми Діффі-Хеллмана та Ель-Гамаля. | 6 |
| 6 | Хеш-функції та їх застосування. Створення електронного цифрового підпису з використанням асиметричних алгоритмів RSA та Ель-Гамаля. | 6 |

## 6. Самостійна робота студента

*Самостійна робота студента полягає в підготовці до аудиторних занять, проектуванні та програмування криптографічних алгоритмів, підготовці до контрольних робіт та заліку. В тому числі:*

- *опрацювання лекційного матеріалу та підготовка до аудиторних занять — до 2 години на тиждень;*

- *проектування та програмування криптографічних алгоритмів — до 4 годин на 1 лабораторну роботу;*
- *підготовка до контрольних робіт та заліку — до 12 годин за семестр.*

## Політика та контроль

### 7. Політика навчальної дисципліни (освітнього компонента)

- ***Відвідування лекцій та лабораторних занять.*** *Відсутність на лекціях та лабораторних заняттях без поважної причини не допускається.*
- ***Правила поведінки на заняттях.*** *На лекційних та лабораторних заняттях студенти мають вимкнути мобільні телефони або увімкнути їх на беззвучний режим.*
- ***Правила захисту лабораторних робіт****. Усі лабораторні роботи оформляються і здаються студентами у вигляді звітів – doc або pdf-файлів. Захист лабораторних робіт відбувається у вигляді усної співбесіди зі студентом за результатами оформленого звіту, також студенту можуть бути поставлені запитання зі списку контрольних питань, що міститься в кінці кожної лабораторної роботи.*
- ***Правила призначення заохочувальних та штрафних балів****. За активну участь на лекціях та лабораторних заняттях передбачаються заохочувальні бали в кількості до 4-х балів за семестр. Штрафні бали призначаються за несвоєчасне виконання лабораторних робіт (див. нижче РСО)*
- ***Політика дедлайнів та перескладань.*** *Залік проводиться на останньому лекційному занятті в семестрі. У випадку неотримання студентом заліку, він має здавати його на додатковій сесії, згідно з розкладом перескладань.*
- ***Політика щодо академічної доброчесності****. Згідно з Кодексом честі студента КПІ, при виконанні лабораторних робіт* ***забороняється*** *користуватися чужими виконаними лабораторними роботами та їх фрагментами. У випадку виявлення плагіату лабораторна робота може бути оцінена від 0 до 1/3 сумарної кількості запланованих за неї балів.*

### 8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Рейтинг студента з кредитного модуля складається з балів, які він отримує:

1) за виконання та захист лабораторних робіт;
2) за виконання модульної контрольної роботи;
3) за виконання залікової контрольної роботи.

Алгоритм процесу оцінювання успішності студентів наведено на рис. 1.

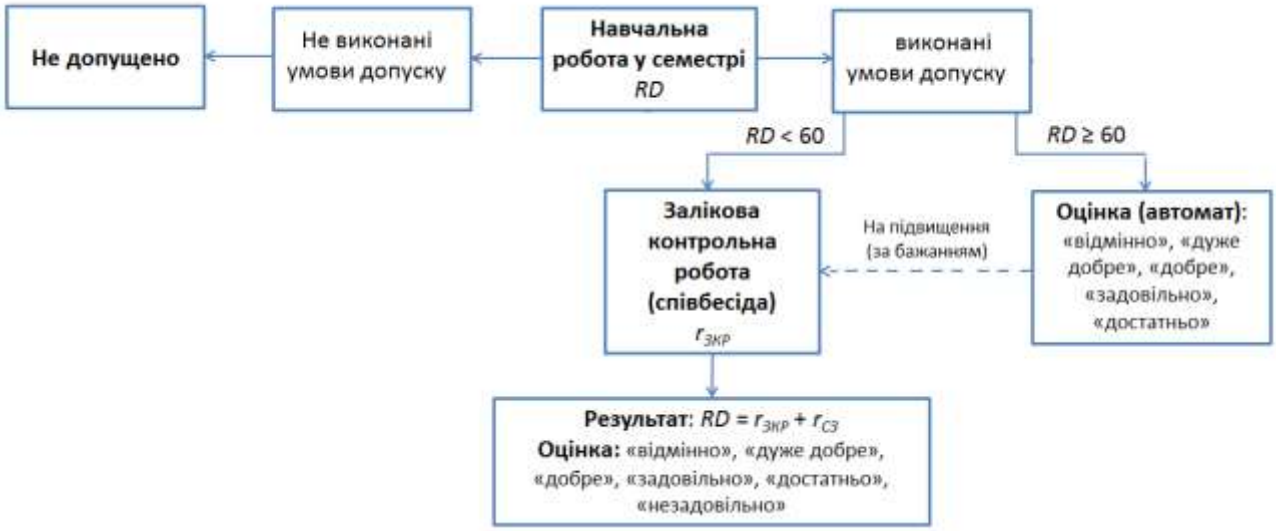


Рис. 1. Схема функціонування РСО

## СИСТЕМА РЕЙТИНГОВИХ БАЛІВ

### 8.1. Бали за виконання та захист лабораторних робіт

Протягом семестру студенти виконують 6 лабораторних робіт:

1) Розробка криптосистем на основі шифрів Цезаря та Тритемія.
2) Розробка криптосистем на основі шифру Віженера та шифру з використанням гамування.
3) Стандарти симетричного шифрування DES, 3DES, IDEA, AES.
4) Шифрування з відкритим ключем на основі алгоритму RSA.
5) Криптографічні асиметричні алгоритми Діффі-Хеллмана та Ель-Гамаля.
6) Хеш-функції та їх застосування. Створення електронного цифрового підпису з використанням асиметричних алгоритмів RSA та Ель-Гамаля.

Максимальна кількість балів за кожну лабораторну роботу: **10 балів**.

Бали нараховуються за:

- якість реалізації роботи: 0-7 балів;
- відповідь під час захисту лабораторної роботи: 0-2 бали.
- вчасність виконання: 0-1 бали.

*Критерії оцінювання **якості реалізації роботи**:*

*7 балів — робота виконана якісно, в повному обсязі;*

*5-6 балів — робота виконана якісно, в повному обсязі, але має вади;*

*4 бали — робота виконана в повному обсязі, але містить незначні помилки;*

*0-3 бали — робота виконана не в повному обсязі чи містить суттєві помилки.*

*Критерії оцінювання **відповідей під час захисту** лабораторної роботи:*

*2 бали — відповіді під час захисту повні, добре аргументовані;*

*1 бал — у відповідях є суттєві помилки;*

*0 балів — немає відповідей або відповіді неправильні.*

*Критерії оцінювання **вчасності виконання** лабораторної роботи:*

*1 бал — роботу здано вчасно, в зазначений термін;*

*0 балів — роботу здано пізніше, ніж через 1 тиждень від зазначеного терміну.*

**Максимальна кількість балів за виконання та захист лабораторних робіт**:

**10 балів × 6 лабораторних робіт = 60 балів**.

### 8.2. Бали за виконання модульної контрольної роботи

Модульна контрольна робота поділяється на дві 45-хвилинні контрольні роботи, кожна з яких містить 20 запитань тестового характеру, що стосуються як теоретичної так і практичної частини курсу.

Максимальна кількість балів за відповідь на кожне запитання: **1 бал**.

*Критерії оцінювання:*

*1 бал — відповідь правильна;*

*0 балів — відповідь неправильна.*

**Максимальна кількість балів за модульний контроль**:

**1 бал × 20 питань × 2 КР** = **40 балів**.

### 8.3. Бали за виконання залікової контрольної роботи

Залікова контрольна робота містить 10 завдань. Ваговий бал: **4 бали** за кожне завдання.

Максимальна кількість балів за залікову роботу:

**4 бали × 10 завдань = 40 балів.**

*Критерії оцінювання:*

*4 бали – повна та правильна відповідь;*

*3 бали – повна та в цілому правильна відповідь з незначними помилками;*

*1-2 бали – відповідь неповна або містить суттєві помилки;*

*0 балів – відповідь неправильна або немає відповіді.*

**8.4. Розрахунок шкали (R) рейтингу:**

Рейтингова шкала з дисципліни складає **R = 100 балів.**

Сума вагових балів протягом семестру складає:

$$\mathbf{R_C = 60 + 40 = 100 \text{ балів.}}$$

Необхідною умовою допуску студента до заліку є виконання усіх лабораторних робіт. Студенти, які допущені до заліку, отримують оцінку з дисципліни ($\mathbf{R_D}$) автоматично.

Якщо студент не згоден із попередньою оцінкою, яку він отримав «автоматом», то він пише залікову контрольну роботу. Остаточний результат ($\mathbf{R_D}$) складається з балів за виконання залікової контрольної роботи та балів за виконання лабораторних робіт і виставляється в залікову відомість. Оцінка (**ECTS** та традиційна) виставляється відповідно до значення $\mathbf{R_D}$, згідно з таблицею

**8.5. Поточна атестація**

На першій атестації, 8-й тиждень, студент отримує «атестовано», якщо його поточний рейтинг складає не менше, ніж **25 балів,** тобто 50% від максимальної кількості балів, яку може отримати студент до першої атестації.

На другій атестації, 14-й тиждень, студент отримує «атестовано», якщо його поточний рейтинг складає не менш, ніж **50 балів**, тобто 50% від максимальної кількості балів, яку може отримати студент до другої атестації.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

| *Сумарний рейтинг,* $\mathbf{R_D}$ | *Оцінка* |
|---|---|
| 100 - 95 | Відмінно |
| 94 - 85 | Дуже добре |
| 84 - 75 | Добре |
| 74 - 65 | Задовільно |
| 64 - 60 | Достатньо |
| < 60 | Незадовільно |
| Не виконані умови допуску | Не допущено |

**Робочу програму навчальної дисципліни (силабус):**

**Складено** *к.ф.-м.н., старшим викладачем кафедри ПМА Бай Ю.П.*

**Ухвалено** кафедрою *прикладної математики* (протокол № _7_ від _09.02.2022_)

**Погоджено** Методичною комісією факультету прикладної математики (протокол № _6_ від _25.03.2022_)