**Силабус освітнього компонента**
Програма навчальної дисципліни

# Методи криптоаналізу

**Шифр та назва спеціальності**
К4 – Управління інформаційною безпекою

**Інститут**
ННІ комп`ютерних наук та інформаційних технологій

**Спеціалізація**

**Кафедра**
Кібербезпеки (328)

**Освітня програма**
Управління інформаційною безпекою

**Тип дисципліни**
Вибіркова

**Рівень освіти**
Перший (бакалаврський)

**Форма навчання**
Денна

**Семестр**
6

**Мова викладання**
Українська

## Викладачі, розробники


**ЄВСЕЄВ Сергій Петрович**

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».


Лауреат національної премії імені Бориса Патона.
Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статтей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus, гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти.

Детальніше про викладача на сайті кафедри

## Загальна інформація

### Анотація

Навчальна дисципліна "Методи криптоаналізу" є вибірковою навчальною дисципліною. Дисципліна спрямована формування у студентів на основі системного підходу наукового світогляду, який дозволяє їм вільно орієнтуватись у теоретичних підходах до реалізації сучасних принципів побудови сучасних криптографічних систем і формування знань по визначенню стійкості криптографічних систем до сучасних методів криптоаналізу.

## Мета та цілі дисципліни

Основні завдання курсу "Методи криптоаналізу" сформульовані в навчальній програмі таким чином:
- передати знання студентам відповідно до сучасних методів криптоаналізу шифрів та систем захисту інформації;
- навчити здобувачів використовувати основні положення теорії криптоаналізу для вирішення проблем оцінки криптографічних властивостей та показників шифрів;
- ознайомити студентів з основними областями розробки методів криптоаналізу та сучасними математичними методами оцінки властивостей та показників стабільності шифрів та криптографічних систем, які використовуються при побудові та тестуванні інструментів захисту інформації в телекомунікаційних та комп'ютерних системах.

## Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

## Компетентності

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК5. Здатність спілкуватися іноземною мовою.
ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
СК5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
СК6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань управління інформаційною безпекою, взаємодіяти з іноземними партнерами.
СК7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
СК8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.
СК9. Здатність організації реагування на загрози на об’єктах критичної інфраструктури, установах та підприємствах.
СК10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.
СК11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

## Результати навчання

РН3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов’язань.
РН4. Вільно спілкуватися державною мовою.
РН5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.
РН6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки
РН7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
РН8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.

РН10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
РН11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.
РН12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
РН13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.
РН14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
РН17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
РН18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
РН19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
РН20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
РН22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

### Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 12 год., лабораторні роботи – 24 год., самостійна робота – 84 год.

### Передумови вивчення дисципліни (пререквізити)

Вища математика.

### Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

## Програма навчальної дисципліни

### Навчальні заняття

#### Лекції

| Теми лекцій | Кількість годин |
|---|---|
| **Тема 1. Основні поняття. Введення в методи криптоаналізу.** Класифікація криптоаналітичних атак. Загроза-атака. Атаки на асиметричні криптосистеми. Метод повного перебору. Атаки «грубої сили». Атаки «колізій» | 2 |

| | |
|---|---|
| шифртекстів. Лінійний криптоаналіз. Диференціальний криптоаналіз.<br>Поняття криптоаналізу. Історія криптоаналізу. Криптоаналіз та стандартизація алгоритмів шифрування. Блокові шифри. Фестелеви шифри. | |
| **Тема 2. Злам блокового шифру.**<br>Блокові шифри. Класифікація зловмисника за силою потужності. Складність атак. Атаки на блокові шифри. | 2 |
| **Тема 3. Диференціальний криптоаналіз шифру DES. Лінійний криптоаналіз шифру DES.**<br>Принципи диференціального криптоналізу. Проходження через цикли des різниць (XOR) текстів.<br>Принципи лінійного криптоаналізу. Сутність методу лінійного криптоаналізу. Побудова лінійних апроксимаційних таблиць. Лінійні апроксимаційні характеристики в атаках Мацуї. | 2 |
| **Тема 4. Диференціальний криптоаналіз шифрів, побудованих на основі структур SPN.**<br>Принципи диференціального криптоаналізу. Шифри структури SPN. Аналіз властивостей нелінійного перетворення. Побудова диференціальної характеристики. Вилучення ключових бітів. Складність атаки. | 2 |
| **Тема 5. Прискорений метод криптоаналізу на основі використання зменшених моделей шифрів. Метод оцінки стійкості БСШ на основі оцінки ентропії.**<br>Сутність прискореного методу криптоаналізу. Результати обчислювальних експериментів по визначенню повних диференціалів зменшених моделей сучасних шифрів. Лінійні властивості зменшених моделей шифрів.<br>Сутність ентропійної оцінки стійкості сучасних шифрів. | 2 |
| **Тема 6. Характеристика та аналіз роботи методики оцінки на основі пакету НІСТ 822-STS. Характеристика та аналіз роботи мобільних мереж четвертого покоління.**<br>Загальні принципи оцінки стійкості на основі пакету НІСТ 822-STS. Методи оцінки.<br>Архітектура мобільних мереж 4G (LTE). Моделі загроз у мобільних мережах 4G. Механізми автентифікації та управління доступом. Методи захисту сигнального та користувацького трафіку. | 2 |
| **Загальна кількість годин** | **12** |

## Лабораторні заняття

| Теми лабораторних занять | Кількість годин | Вагові коефіцієнти $a$ |
|---|---|---|
| **Тема 1. Засвоєння й дослідження методики виконання атак диференціального криптоаналізу на симетричні блокові шифри.**<br>Основні принципи диференціального криптоаналізу. Побудова таблиць різницевих характеристик для S-блоків. Приклади атак на спрощені блокові шифри (SPN, Feistel-мережі). Використання відомих відкритих текстів і шифротекстів. Практичні межі застосування диференціального криптоаналізу. | 4 | 1 |
| **Тема 2. Вивчення методики виконання атак лінійного** | 4 | 1 |

| | | |
|---|---|---|
| **криптоаналізу на блочні симетричні шифри.**<br>Теоретичні основи лінійного криптоаналізу. Побудова лінійних апроксимацій для S-блоків. Обчислення ймовірностей відхилення від випадкового розподілу. Використання великої кількості відомих пар «відкритий текст – шифротекст». Порівняння ефективності лінійного та диференціального криптоаналізу. | | |
| **Тема 3. Знаходження ключових бітів на основі використання відомих вхідних пар та вихідних XORів S-блоків.**<br>Використання властивостей S-блоків у криптоаналізі. Алгоритм обчислення XOR-виходів S-блоків. Виявлення залежностей між входами та виходами S-блоків. Приклади пошуку ключових бітів у DES/спрощених DES. Обмеження та складність методу. | 4 | 1 |
| **Тема 4. Аналіз вимог до відбору S-блоків, що використані розробниками стандарту DES.**<br>Історія створення DES і вибір S-блоків. Основні критерії криптостійкості S-блоків. Роль S-блоків у забезпеченні нелінійності та лавинного ефекту. Устойчивість S-блоків до диференціального криптоаналізу. Аналіз опублікованих досліджень і критика S-блоків DES. | 4 | 1 |
| **Тема 5. Дослідження алгоритмів на основі ентропійного методу.**<br>Основи ентропії та її застосування у криптографії. Оцінка рівня випадковості шифротекстів. Ентропійний підхід для оцінки стійкості шифрів. Приклади використання ентропії для виявлення слабких ключів. Порівняння ентропійного аналізу з іншими методами криптоаналізу. | 4 | 1 |
| **Тема 6. Дослідження алгоритмів на основі пакету HICT 822-STS.**<br>Призначення пакету NIST SP 800-22 Statistical Test Suite (STS). Огляд основних статистичних тестів: частотний тест, серійний тест, тест довгих послідовностей тощо. Використання NIST STS для оцінки генераторів випадкових чисел. Тестування криптографічних алгоритмів на випадковість. Інтерпретація результатів STS і визначення придатності алгоритму. | 4 | 1 |
| **Загальна кількість годин** | **24** | $\sum_{i=1}^{n} a_i = 6$ |

## Контрольні роботи

| Теми контрольних робіт | Вагові коефіцієнти $b$ |
|---|---|
| **Тема 1. Диференціальний та лінійний криптоаналіз: методологія, застосування та порівняльна ефективність.**<br>Аналіз основних етапів атак. Приклади застосування до класичних симетричних блокових шифрів. Оцінка складності та практичних обмежень. | 1 |
| **Тема 2. S-блоки в симетричних шифрах: властивості, вимоги та стійкість до криптоаналітичних атак.**<br>Критерії відбору S-блоків (на прикладі DES). Їхня роль у забезпеченні | 1 |

| | |
|---|---|
| нелінійності. Стійкість до диференціального та лінійного криптоаналізу. | |
| **Тема 3. Методи криптоаналізу та їх застосування в сучасних системах шифрування.** Класифікація методів криптоаналізу (повний перебір, частотний аналіз, диференційний та лінійний криптоаналіз). Особливості криптоаналізу симетричних алгоритмів (DES, AES). Методи криптоаналізу асиметричних алгоритмів (RSA, ECC). Роль квантових обчислень у криптоаналізі (Shor's algorithm, Grover's algorithm). Практичні приклади атак на сучасні криптосистеми. | 1 |
| **Загалом** | $\sum_{i=1}^{m} b_i$=3 |

## Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

### Опрацювання теоретичного матеріалу

| Теми для самостійного вивчення | Кількість годин |
|---|---|
| **Тема 1. Історичний розвиток криптоаналізу та його вплив на сучасну криптографію.** Класичні приклади криптоаналізу: «Енігма», шифр Цезаря, Віженера. Роль криптоаналізу у військових конфліктах. Перехід від класичних методів до математичних моделей. Внесок криптоаналізу в розвиток сучасних стандартів шифрування. | 12 |
| **Тема 2. Методи алгебраїчного криптоаналізу симетричних шифрів.** Основи алгебраїчного підходу: системи рівнянь для опису шифру. Атаки на основі багаточленів та їх спрощення. Алгебраїчний криптоаналіз AES. Переваги та недоліки цього методу в практичному застосуванні. | 12 |
| **Тема 3. Атаки на основі побічних каналів (side-channel attacks).** Теоретичні засади побічних каналів. Атаки за часом виконання (Timing attacks). Аналіз споживання енергії (DPA, SPA). Електромагнітний аналіз (EMA). Методи захисту від побічних атак. | 12 |
| **Тема 4. Методи диференціально-лінійного криптоаналізу.** Основи диференціального криптоаналізу. Основи лінійного криптоаналізу. Поєднання методів: диференціально-лінійні атаки. Практичні приклади застосування до DES та AES. Вплив цих методів на проектування сучасних шифрів. | 12 |
| **Тема 5. Криптоаналіз сучасних потокових шифрів.** Загальна характеристика потокових шифрів. Вразливості RC4 та практичні атаки. Безпека Salsa20 та ChaCha у сучасних протоколах. Методи атак на LFSR-шифри. Роль потокових шифрів у VPN та TLS. | 12 |
| **Тема 6. Аналіз стійкості криптографічних геш-функцій.** Властивості криптографічних геш-функцій. Колізії, предобрази та другі предобрази. Атаки на MD5 і SHA-1: приклади та наслідки. Стійкість сучасних алгоритмів SHA-2 та SHA-3. Роль геш-функцій у цифрових підписах та блокчейні. | 12 |
| **Тема 7. Квантові алгоритми криптоаналізу.** Основи квантових обчислень для криптоаналізу. Алгоритм Шора та його вплив на RSA та ECC. Алгоритм Гровера та атаки на симетричні шифри. Потенціал квантових атак у майбутньому. Постквантова криптографія як відповідь на нові | 12 |

виклики.

| | |
|---|---|
| **Загальна кількість годин** | **84** |

## Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості.

### Рекомендовані курси, тренінги, стажування

За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

## Література, навчальні матеріали та інформаційні ресурси

### Основна література

1. Основи криптографії: навчальний посібник /. С. Е. Остапов, Л. О. Валь. – Чернівці: Книги–ХХІ, 2008. – 188 с.
https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/36505/1/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D0%B7.%20%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%87%D0%BD%D1%96%20%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D0%B8.pdf
2. Євсеєв С.П. КІБЕРБЕЗПЕКА: ЛАБОРАТОРНИЙ ПРАКТИКУМ З ОСНОВ КРИПОГРАФІЧНОГО ЗАХИСТУ / С.П. Євсеєв, О.В. Мілов, О.Г. Король – Львів: «Новий Світ- 2000», 2020 . – 241 с.
http://library.hneu.edu.ua/storage/new-arrivals-books/December2020/Yevseiev.pdf.
3. Онацький О. В., Йона Л. Г. Криптографічні системи : навчальний посібник з дисциплін "Криптографія та криптоаналіз" для освітньо-професійної підготовки бакалаврів в галузі знань 12 "Інформаційні технології" за спеціальністю 125 "Кібербезпека" / О. В. Онацький, Л. Г. Йона. – Одеса : Міжнародний гуманітарний університет, 2023. – 156 с.
https://dspace.onua.edu.ua/server/api/core/bitstreams/7d8fb278-794c-4b0d-9254-64acb7892ed1/content
4. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
http://monograph.com.ua/pctc/catalog/view/64/52/231-1.
5. Євсєев С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. “Новий Світ-2000”, 2023. – 657 с.
https://acrobat.adobe.com/id/urn%3Aaaid%3Asc%3AEU%3A3c427761-01ab-4365-88f6-37f76ca508c5/?x_api_client_id=chrome_extension_viewer&bookmarkAcrobat=true&x_api_client_location=bookmark&filetype=application%2Fpdf&viewer%21megaVerb=group-discover.

### Додаткова література

1. A. Rukhin, and J. Soto. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22, 09.2000, 164 p.
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf.

## Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників $k$:

| Поточний контроль (практичні, семінарські, лабораторні заняття), $k_1$ | Контрольні роботи (за наявності), $k_2$ | Індивідуальне завдання (за наявності), $k_3$ | Підсумковий контроль (для ОК з іспитом), $k_4$ |
|---|---|---|---|
| 0,7 | 0,3 | | |

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
$K$ – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: $a_i$ - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: $b_i$ - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, $K$, І,... ) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

**Шкала оцінювання**

| Сума балів | Національна оцінка | ECTS |
|---|---|---|
| 90–100 | Відмінно | A |
| 82–89 | Добре | B |
| 75–81 | Добре | C |
| 64–74 | Задовільно | D |
| 60–63 | Задовільно | E |
| 35–59 | Незадовільно (потрібне додаткове вивчення) | FX |
| 1–34 | Незадовільно (потрібне повторне вивчення) | F |

## Норми академічної етики і політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.
Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

## Погодження

Силабус погоджено 30.08.2025 **Завідувач кафедри**

Сергій ЄВСЕЄВ

30.08.2025 

**Гарант ОП**
Роман КОРОЛЬОВ