



Силабус освітнього компонента Програма навчальної дисципліни



Основи криптографічного захисту

Шифр та назва спеціальності

КЗ – Національна безпека (за окремими сферами забезпечення і видами діяльності)

Спеціалізація

Освітня програма

Національна безпека у сфері кіберзахисту

Рівень освіти

Перший (бакалаврський)

Семестр

4

Інститут

ННІ комп'ютерних наук та інформаційних технологій

Кафедра

Кібербезпеки (328)

Тип дисципліни

Обов'язкова

Форма навчання

Денна

Мова викладання

Українська

Викладачі, розробники



ЄВСЄЄВ 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 статей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти. Провідний лектор з дисциплін: Математичні основи криптології, Комп'ютерні мережі, Основи криптографічного захисту, Методи криптоаналізу, Основи кібербезпеки, Сучасні проблеми постквантової криптографії, Основи наукових досліджень, Цифрова криміналістика, Етичний хакінг у студентів бакалавріата та магістратури, Методологія наукової та педагогічної діяльності в науках кіберзахисту для аспірантів.

[Детальніше про викладача на сайті кафедри](#)

Загальна інформація

Анотація

Навчальна дисципліна "Основи криптографічного захисту" є обов'язковою навчальною дисципліною. Дисципліна спрямована на вивчення симетричних та асиметричних методів шифрування інформації, їх використання; видів криптоаналізу та можливість його застосування.

Мета та цілі дисципліни

Ознайомлення з теоретичними основами криптології; придбання навичок в практичному використанні, постановці і вирішенні задач шифрування інформації; розуміння суті інформаційних процесів в криптографічних системах; застосування комп'ютерів для вирішення завдань шифрування і дешифрування; розробка і використання математичних і обчислювальних моделей процесів шифрування інформації, їх оптимізація та вироблення напрямків вдосконалення.

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.

ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

СК1. Здатність використовувати безпекові режими під час виконання службових обов'язків.

СК8. Здатність використовувати механізми забезпечення національної безпеки у її визначальних сферах.

СК11. Здатність використовувати практичні навички, тактику та прийоми роботи з людьми в інтересах службової діяльності.

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.

РН7. Вміти виявляти, ставити та вирішувати професійні завдання, вміти узагальнювати отримані результати, обробляти та аналізувати інформацію з різних джерел, оформлювати і презентувати результати досліджень відповідно до вимог.

РН8. Вміти використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективні системи інформаційно-аналітичного забезпечення підтримки прийняття рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.

РН9. Вміти використовувати безпекові режими під час виконання службових обов'язків.

РН10. Вміти аналізувати виклики та загрози національній безпеці за напрямками професійної діяльності та синтезувати інформацію щодо розроблення та реалізації стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).

РН12. Вміти застосовувати знання з основ теорії національної безпеки, зокрема: оцінювати обстановку, рівень викликів та загроз національній безпеці.

РН16. Використовувати у професійній діяльності окремі елементи механізму впливу та взаємодії у процесі забезпечення окремих складових національної безпеки.

РН17. Вміти використовувати отримані знання щодо безпекової складової зовнішньої політики України та інших держав.

РН18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.

РН19. Вміти використовувати у професійній діяльності методи та інструменти організації соціальної взаємодії, співробітництва та розв'язання конфліктів у сфері професійної діяльності,

практичні навички, тактику та прийоми, роботи з людьми в інтересах службової діяльності: працювати у команді з позицій лідера, радника (консультанта), помічника, планувати використання часу та визначати стимули і бар'єри ефективної роботи, здійснювати розподіл (делегування) функцій, повноважень і відповідальності між виконавцями.

Обсяг дисципліни

Загальний обсяг дисципліни 180 год. (6 кредитів ECTS): лекції – 32 год., лабораторні роботи – 48 год., самостійна робота – 100 год.

Передумови вивчення дисципліни (пререквізити)

Математичні основи криптології, Вища математика (спеціальні глави).

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 проекти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Теоретичні основи захисту інформації. Основні поняття. Моделі секретних систем. Основні завдання системи безпеки. Симетричні та несиметричні криптосистеми. Режими роботи симетричних криптосистем.	2
Тема 2. Протоколи автентичності. Цифровий підпис. Механізми автентичності. Класифікація цифрового підпису. Методи гешування. Механізми автентифікації на основі використання програмно-апаратних засобів. Автентифікація Kerberos.	2
Тема 3. Протоколи суворої автентифікації. Класифікація методів 2 FA. Рівні достовірності автентифікації. Загрози на 2 FA. Двофакторна автентифікація в Linux.	2
Тема 4. Система PGP. Основні функції системи. Класифікація ключів. Механізми забезпечення автентичності та конфіденційності. Система довіри.	2
Тема 5. Основи технології PKI. Основні функції та склад технології. Фізична та логічна топологія. Криптоперіод. Основні механізми технології на основі симетричних та несиметричних криптосистем.	2
Тема 6. Протоколи цілісності SSL, TLS. Взаємозв'язок об'єктів критичної інфраструктури з кіберфізичними системами. Структура протоколів SSL, TLS. Функції протоколу SSL. АТАКИ НА SSL/TLS.	2
Тема 7. Основи постквантової криптографії. Основні поняття. Основа квантових обчислень. Основні алгоритми квантового криптоаналізу.	2
Тема 8. Основи теорій інформації та кодування. Загальна структура системи зв'язку. Моделі двійкового симетричного каналу	2

без пам'яті. Ефективне кодування Хаффмана. Корекція та винахід помилок. Класифікація двійкових кодів. Основні поняття теорії перешкодостійкого кодування. Поля Галуа. Структура кінцевих полів їх властивості. Коды Боуза-Чоудхурі-Хоквінґему.

Тема 9. Основи розкодування.

2

Алгоритм Берлекемпа-Месі. Приклад.

Тема 10. Постквантові алгоритми на основі крипто-кодових конструкцій Мак-Еліса і Нідеррайтера. Гібридні системи захисту на збиткових кодах.

2

Класифікація крипто-кодових конструкцій. Еліптичні криві. Основи побудови (формування ключових матриць, формування криптограми). Оцінка стійкості. Шляхи зменшення ємності ключових даних. Формування крипто-кодових конструкцій на алгеброгеометричних (еліптичних) кодах. Основи криптографії на збиткових кодах. Формування гібридних крипто-кодових конструкцій.

Тема 11. Потоків симетричні криптосистеми.

2

Симетричні криптосистеми. Потоків шифр RC-4. Стійкість. Ініціалізація S-блоку. Потоків шифр PRC-4A. Потоків шифр STRUMOK. Потоків шифр SNOW2.0.

Тема 12. Основи криптоаналізу.

2

Класифікація аналітичних атак. Загроза-атака. Основи криптоаналізу. Атаки на асиметричні криптосистеми. Метод повного перебору. Атаки «Грубої сили». Атака «Колізій». Основні етапи лінійного криптоаналізу. Диференціальний криптоаналіз.

Тема 13. Захист застосунків.

4

Правила боя. Принципи безпеки. Класифікація небезпеки: методика STRIDE. DREAD — методика оцінка ризиків. Безпечні методи кодування. Вибір механізму контролю доступу. Небезпечні типи ACE. Тригери та дозволи SQL SERVER. Захист даних.

Тема 14. Фізичний захист об'єктів інформаційних систем.

4

Історії битв. Хакери. Вплив загроз. Сучасний центр моніторингу та управління безпекою (SOC). Фізичний захист об'єктів критичної інфраструктури. Захист інфраструктурних комунікацій.

Загальна кількість годин

32

Лабораторні заняття

Теми лабораторних занять

**Кількість
годин**

**Вагові
коефіцієнти α**

Тема 1. Найпростіші шифри. Дослідження властивостей режимів роботи блокових шифрів.

6

-

Підстановка та перестановка символів. Шифр Цезаря, афінний шифр. Шифр Віженера та його криптоаналіз. Одноразовий блокнот (One-Time Pad). Виявлення слабких місць простих шифрів. Режим ECB та його слабкі сторони. CBC (Cipher Block Chaining) – дослідження ефекту лавини. CFB та OFB режими – поточне шифрування. CTR (Counter Mode) – паралельна обробка блоків. Порівняння ефективності та безпеки різних режимів.

Тема 2. Дослідження протоколів автентичності та конфіденційності за допомогою RSA.

6

0,1

Генерація ключів RSA. Шифрування та розшифрування повідомлень. Використання RSA для автентифікації користувачів.

Дослідження стійкості RSA при малих ключах. Атаки на RSA: факторизація, підбір повідомлень.		
Тема 3. Дослідження протоколів цифрового підпису. Формування та перевірка підпису RSA. Підпис ECDSA (еліптичні криві). Використання геш-функцій у цифрових підписах. Перевірка підроблених підписів. Практика з цифровими сертифікатами (X.509).	6	0,1
Тема 4. Дослідження протоколів системи PGP. Генерація відкритих та закритих ключів. Шифрування та підпис повідомлень. Робота з «кільцем ключів» (Key Ring). Перевірка автентичності відправника. Атаки на PGP та виявлення слабких налаштувань.	6	0,1
Тема 5. Стеганографічні методи захисту інформації. Вбудовування даних у зображення (LSB-метод). Аудіостеганографія (приховання даних у звукових файлах). Використання стеганографії у текстах. Комбінування криптографії та стеганографії. Методи виявлення прихованих даних (стеганоаналіз).	6	0,1
Тема 6. Методика NIST STS оцінки статистичних властивостей криптографічних алгоритмів. Ознайомлення з пакетом тестів NIST STS. Перевірка випадковості бітових послідовностей. Тест на частоти, серії, автокореляцію. Тест довгих послідовностей (Longest Run Test). Інтерпретація результатів для криптосистем.	6	0,1
Тема 7. Побудова циклічних кодів. Основи теорії помилок та кодів. Побудова генератора та перевірного багаточлена. Код БЧХ та його властивості. Алгоритм виявлення та виправлення помилок. Практичне кодування/декодування повідомлень.	6	0,1
Тема 8. Робота з кубітами. Емуляція вимірювань. Основи квантових обчислень: стан кубіта, суперпозиція. Математичний опис операцій над кубітами (матриці Паулі, Адамара). Емуляція квантових вимірювань на класичному комп'ютері. Побудова простих квантових алгоритмів (Deutsch, Grover). Аналіз потенційних загроз класичним криптосистемам з боку квантових обчислень.	6	0,1
Загальна кількість годин	48	$\sum_{i=1}^n a_i = 0,7$
Контрольні роботи		
Теми контрольних робіт	Вагові коефіцієнти b	
Тема 1. Класичні та сучасні методи криптографії. Аналіз історичних шифрів (Цезаря, Віженера, одноразового блокнота). Основні принципи симетричної криптографії. Режим роботи блокових шифрів та їх безпека. Практичні приклади криптоаналізу простих шифрів.	0,1	
Тема 2. Сучасні протоколи захисту інформації. Алгоритм RSA: шифрування, підпис, уразливості. Цифровий підпис та роль геш-функцій. Протоколи PGP та SSL/TLS. Квантові загрози сучасним криптосистемам.	0,1	

Тема 3. Порівняльний аналіз сучасних стандартів симетричного та асиметричного шифрування (AES, RSA, ECC). Теоретичні основи роботи алгоритмів. Сильні та слабкі сторони. Области практичного застосування. Стійкість до сучасних атак.	0,1
Загалом	$\sum_{i=1}^m b_i=0,3$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Класичні методи криптографії. Історія виникнення та розвиток мов для смарт-контрактів. Порівняння синтаксису та можливостей Solidity і Vyper. Використання Rust та Go для блокчейнів нового покоління (Polkadot, Cosmos). Переваги та недоліки різних мов.	13
Тема 2. Симетрична криптографія. Архітектура EVM. Байткод та його виконання у віртуальній машині. Використання газу (gas) і вартість операцій. Роль EVM у виконанні смарт-контрактів.	13
Тема 3. Асиметрична криптографія. RSA: генерація ключів, шифрування та підпис. Алгоритм Ель-Гамала. Криптографія на еліптичних кривих (ECC).	13
Тема 4. Геш-функції та автентифікація. Криптографічні геш-функції (MD5, SHA-1, SHA-2, SHA-3). HMAC та методи перевірки цілісності. Протоколи автентифікації користувачів.	13
Тема 5. Цифровий підпис і сертифікати. Протокол DSS. Інфраструктура відкритих ключів (PKI). SSL/TLS та цифрові сертифікати.	12
Тема 6. Спеціальні методи захисту інформації. PGP та використання відкритих ключів у поштових сервісах. Стеганографія в цифрових зображеннях, аудіо та відео. Методи захисту даних у хмарних сервісах.	12
Тема 7. Криптоаналіз і стандарти оцінювання безпеки. Основи диференціального та лінійного криптоаналізу. NIST STS: тестування випадковості. Стійкість криптосистем до атак сторонніми каналами.	12
Тема 8. Квантова криптографія. Принципи роботи кубітів. Протоколи квантового розподілу ключів (BB84). Перспективи та виклики постквантової криптографії.	12
Загальна кількість годин	100

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

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

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Євсєєв С.П. Кібербезпека: сучасні технології захисту. / Євсєєв С.П, Остапов С.Е., Король О.Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: "Новий Світ- 2000", 2019. – 678. – Режим доступу: <http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnologii-zakhystu.pdf>.
2. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
<http://kist.ntu.edu.ua/textPhD/tzi.pdf>.
3. Bonaventure O. Computer Networking: Principls, Protocols and Practice. - Louvain-la-Neuve: Universite catholique de Louvain (Belgium), 2019. - 272 p.
<https://resources.saylor.org/wwwresources/archived/site/wp-content/uploads/2012/02/Computer-Networking-Principles-Bonaventure-1-30-31-OTC1.pdf>.
4. Євсєєв С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсєєв, О.В. Мілов, С.Е. Остапов, О.В. Сєверінов. – 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

6. Євсєєв С.П. КІБЕРБЕЗПЕКА: ЛАБОРАТОРНИЙ ПРАКТИКУМ З ОСНОВ КРИПТОГРАФІЧНОГО ЗАХИСТУ / С.П. Євсєєв, 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>
7. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, F. Vercauteren. Handbook of elliptic and hyperelliptic curve cryptography// Kenneth H. Rosen Ed. 2006. 843 p.
<https://blkcipher.pl/assets/pdfs/Handbook of Elliptic and Hyperelliptic Curve Cryptography.pdf>
8. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. URL: https://www.researchgate.net/publication/352013398_Synergy_of_building_cybersecurity_systems_Monograph.
9. A. Rukhin, J. Soto. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22, 2000
<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:

$$O = \Pi \cdot k_1 + K \cdot k_2 + I \cdot k_3 + \Pi_k \cdot k_4$$

де: Π – середньозважена середня оцінка за поточний контроль

I – оцінка за виконання індивідуального завдання

K – середньозважена оцінка за контрольні роботи

Π_k – оцінка за підсумковий контроль

$$\Pi = \frac{\Pi_1 \cdot a_1 + \Pi_2 \cdot a_2 + \dots + \Pi_n \cdot a_n}{\sum_{i=1}^n a_i}$$

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

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

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Шкала оцінювання

Поточні оцінки за кожну складову (Π , K , I ,...) 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 O з округленням до найближчого цілого числа в більшу сторону.

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 СВСЕЄВ

30.08.2025



Гарант ОП
Андрій ТКАЧОВ

