



Силабус освітнього компонента

Програма навчальної дисципліни



Інструментальні засоби програмування

Шифр та назва спеціальності

F5 – Кібербезпека та захист інформації

Інститут

ННІ комп'ютерних наук та інформаційних технологій (320)

Спеціалізація

-

Кафедра

Кібербезпеки (328)

Освітня програма

Кібербезпека

Тип дисципліни

Обов'язкова

Рівень освіти

Перший (бакалаврський)

Форма навчання

Денна, заочна

Семестр

4

Мова викладання

Українська, англійська

Викладачі, розробники

**ТКАЧОВ Андрій Михайлович**

andrii.tkachov@khpi.edu.ua

Кандидат технічних наук, старший науковий співробітник кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: більше 60 публікацій, 25 статей у закордонних виданнях та фахових виданнях України, 6 патентів на корисну модель, гарант освітньо-професійної програми "Національна безпека у сфері кіберзахисту" першого (бакалаврського) рівня вищої освіти.

[Детальніше про викладача на сайті кафедри](#)

Загальна інформація

Анотація

Навчальна дисципліна "Інструментальні засоби програмування" є обов'язковою навчальною дисципліною. Дисципліна спрямована на формування у студентів теоретико-практичного базису щодо сучасних підходів у сфері програмування та їх впровадження у роботу веб-орієнтованих систем. Вивчення дисципліни забезпечує професійний розвиток та спрямована на дослідження процесів виявлення знань, оволодіння сучасними технологіями та засобами програмування.

Мета та цілі дисципліни

Вивчення технологій програмування, придбання студентами знань і навиків в області розробки алгоритмів, створення, трансляції та налагодження прикладних програм, застосування бібліотек

та модулів для створення прогнаних забезпечення для вирішення задач аналізу та захисту інформаційних систем.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.

ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.

СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та систем захисту інформації.

Результати навчання

РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

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)

Алгоритми та структури даних, Основи програмування.

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. Технології кібербезпеки. Основи кібербезпеки в програмуванні. Принципи побудови безпечного коду. Інструменти захисту від шкідливого ПЗ. Управління правами доступу та автентифікацією.	4
Тема 2. Технології шифрування. Симетричне та асиметричне шифрування. Криптографічні хеш-функції та MAC.	4

Протоколи безпечного обміну ключами. Практична реалізація шифрування в мовах програмування (Python, C++).

Тема 3. Аналіз алгоритмів шифрування.

4

Критерії ефективності та безпеки алгоритмів. Виявлення вразливостей алгоритмів. Тестування криптографічних функцій. Практичні приклади оцінки стійкості алгоритмів.

Тема 4. Технології реверс-інжинірингу.

4

Основи зворотного проектування програм. Декомпілятори та дизасемблери. Аналіз виконуваних файлів та бібліотек. Виявлення логіки роботи шифрів і протоколів.

Тема 5. Аналіз шифрів.

4

Методи криптоаналізу класичних шифрів. Аналіз сучасних симетричних та асиметричних шифрів. Практичне використання інструментів для криптоаналізу. Виявлення слабких ключів та вразливих реалізацій.

Тема 6. Технології криптоаналізу.

4

Диференціальний та лінійний криптоаналіз. Використання статистичних методів у криптоаналізі. Підбір ключів та атаки на протоколи. Автоматизація криптоаналізу за допомогою програмних засобів.

Тема 7. Паралельні обчислювання.

4

Основи паралельного програмування. Використання багатопоточності та GPU. Паралельний криптоаналіз та розподілені обчислення. Практична реалізація алгоритмів шифрування на багатоядерних системах.

Тема 8. Нейронні мережі.

4

Основи штучних нейронних мереж. Використання нейромереж для аналізу даних та шифрів. Практичні приклади розпізнавання патернів у криптографічних даних. Інструментальні засоби для навчання та тестування нейронних мереж.

Загальна кількість годин

32

Лабораторні заняття

Теми лабораторних занять

Кількість годин **Вагові коефіцієнти α**

Тема 1. Використання принципів кіберзахисту при проектуванні та розробці ПЗ.

6

1

Виявлення загроз та вразливостей у проекті. Використання принципів безпечного кодування. Захист конфіденційних даних у програмі. Практичне застосування патернів безпечного програмування.

Тема 2. Технології шифрування.

6

1

Реалізація симетричного шифрування (AES, DES). Реалізація асиметричного шифрування (RSA, ECC). Використання криптографічних бібліотек (PyCrypto, OpenSSL). Шифрування та дешифрування файлів і повідомлень.

Тема 3. Аналіз алгоритмів шифрування.

6

1

Тестування стійкості шифрів до простих атак. Порівняння швидкості та ресурсомісткості різних алгоритмів. Практичне виявлення слабких місць алгоритмів.

Тема 4. Технології реверс-інжинірингу.

6

1

Використання дизасемблерів та декомпіляторів (Ghidra, IDA Pro). Аналіз виконуваних файлів на наявність прихованої логіки. Виявлення шифрувальних алгоритмів у програмному коді. Декомпіляція та інтерпретація функцій.		
Тема 5. Аналіз шифрів. Практичне застосування диференціального та лінійного криптоаналізу. Виявлення слабких S-блоків та ключових схем. Симуляція простих атак на блокові шифри. Визначення ефективності захисту алгоритмів.	6	1
Тема 6. Технології криптоаналізу. Автоматизація процесу криптоаналізу. Використання готових бібліотек для перевірки стійкості шифрів. Вимірювання складності та часу атаки. Практичне виявлення уразливих ділянок у шифрах.	6	1
Тема 7. Паралельні обчислення. Використання багатопоточності у криптографії (OpenMP, pthreads). Прискорення обчислювальних процесів на GPU (CUDA, OpenCL). Оцінка продуктивності паралельних обчислень. Розподілені обчислення для великих наборів даних.	6	1
Тема 8. Нейронні мережі. Створення простих нейронних мереж для обробки даних. Використання нейронних мереж для розпізнавання патернів у шифрованих даних. Практичні завдання на TensorFlow або PyTorch. Оцінка ефективності нейронної мережі при криптографічному аналізі.	6	1
Загальна кількість годин	48	$\sum_{i=1}^n a_i = 8$
Контрольні роботи		
<i>За наявності</i>		
Теми контрольних робіт		Вагові коефіцієнти b
Тема 1. Аналіз та оцінка стійкості алгоритмів шифрування. Перевірка ефективності симетричного та асиметричного шифрування. Виявлення вразливостей у реалізації алгоритмів.		0,5
Тема 2. Паралельні обчислення та нейронні мережі для аналізу даних. Реалізація паралельного криптоаналізу. Використання нейронних мереж для розпізнавання патернів у криптографічних даних.		1,5
Загалом		$\sum_{i=1}^m b_i = 2$
Самостійна робота		
До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу.		
Опрацювання теоретичного матеріалу		
Теми самостійного вивчення		Кількість годин
Тема 1. Основи кібербезпеки в програмуванні. Основні загрози та вразливості програмного забезпечення. Виявлення типових		13

атак на ПЗ (SQL-ін'єкції, XSS, buffer overflow). Захист програмного коду від несанкціонованого доступу.

Тема 2. Практичне застосування симетричного та асиметричного шифрування. 13

Розгляд алгоритмів AES, DES, RSA, ECC. Використання бібліотек шифрування у різних мовах програмування. Криптографічні протоколи для передачі даних.

Тема 3. Криптографічні хеш-функції та протоколи обміну ключами. 13

Принципи роботи хеш-функцій (SHA, MD5, Blake2). Використання хеш-функцій для перевірки цілісності даних. Алгоритми обміну ключами: Diffie-Hellman, ECDH.

Тема 4. Методи реверс-інжинірингу: дизасемблери та декомпілятори. 13

Аналіз виконуваних файлів та бібліотек. Використання програмних інструментів: IDA Pro, Ghidra, Radare2. Виявлення логіки роботи алгоритмів та шифрів у коді.

Тема 5. Диференціальний та лінійний криптоаналіз на прикладі симетричних шифрів. 12

Поняття диференціального та лінійного криптоаналізу. Практичне застосування на простих блокових шифрах. Аналіз слабких місць S-блоків та ключових схем.

Тема 6. Використання багатопоточності та GPU для прискорення обчислень. 12

Основи паралельного програмування (OpenMP, CUDA, OpenCL). Прискорення криптоаналізу та обчислювальних задач. Вимірювання продуктивності та ефективності паралельних алгоритмів.

Тема 7. Практичне навчання нейронних мереж на криптографічних даних. 12

Введення у машинне навчання та нейронні мережі. Використання нейронних мереж для розпізнавання патернів у шифрованих даних. Реалізація простих моделей на Python (TensorFlow, PyTorch).

Тема 8. Автоматизація аналізу алгоритмів шифрування за допомогою програмних засобів. 12

Написання скриптів для перевірки стійкості шифрів. Використання готових бібліотек для криптоаналізу. Побудова автоматизованих тестів для різних типів шифрів.

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. Онлайн-курс CISCO «C++ Adv»

<https://www.netacad.com/catalogs/learn?category=course>

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Python 3.10.2 documentation [Електронний ресурс]. – Режим доступу : <https://docs.python.org/3/>.
2. Java Platform Standard Edition 8 Documentation [Електронний ресурс]. – Режим доступу : <https://docs.oracle.com/javase/8/docs/>.
3. Microsoft C++, C, and Assembler documentation [Електронний ресурс]. – Режим доступу : <https://docs.microsoft.com/en-us/cpp/?view=msvc-170>.
4. WEB-технології [Електронний ресурс]: Навчально-довідковий посібник / С.П. Євсєєв, А.М. Ткачов, В.О. Алексієв, Ю.М. Рябуха – Харків : ХНЕУ ім. С. Кузнеця, – Львів: Видавництво «Новий Світ – 2000», 2021. – 390 с.
<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju>
5. Євсєєв С.П. КІБЕРБЕЗПЕКА: КРИПТОГРАФІЯ З PYTHON: навч. посібн. / С.П. Євсєєв, О.В. Шматко, О.Г. Король – Харків: Видавництво «Новий Світ – 2000», 2021. – 120 с.
<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju>

Додаткова література

1. Python Tutorial [Електронний ресурс]. – Режим доступу : <https://www.tutorialspoint.com/python/index.htm>.
2. Java Tutorial [Електронний ресурс]. – Режим доступу : <https://www.tutorialspoint.com/java/index.htm>.
3. C++ Tutorial [Електронний ресурс]. – Режим доступу : <https://www.tutorialspoint.com/cplusplus/index.htm>.

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
0,4	0,2		0,4

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.

Поточні оцінки за кожну складову (П, К, 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
Сергій ЄВСЕЄВ