Силабус освітнього компонента
Програма навчальної дисципліни

Інструментальні засоби програмування

Шифр та назва спеціальності
К4 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320)

Спеціалізація
-

Кафедра
Кібербезпеки (328)

Освітня програма
Управління інформаційною безпекою

Тип дисципліни
Обов'язкова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
4

Мова викладання
Українська

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 програних забезпечення для вирішення задач аналізу та захисту інформаційних систем.

Формат занять

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

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.
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 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 проєкти, 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. Протоколи безпечного обміну ключами. Практична реалізація шифрування в мовах програмування (Python, C++).	4
Тема 3. Аналіз алгоритмів шифрування. Критерії ефективності та безпеки алгоритмів. Виявлення вразливостей алгоритмів. Тестування криптографічних функцій. Практичні приклади оцінки стійкості алгоритмів.	4
Тема 4. Технології реверс-інжинірингу. Основи зворотного проектування програм. Декомпілятори та дизасемблери. Аналіз виконуваних файлів та бібліотек. Виявлення логіки роботи шифрів і протоколів.	4

Тема 5. Аналіз шифрів. Методи криптоаналізу класичних шифрів. Аналіз сучасних симетричних та асиметричних шифрів. Практичне використання інструментів для криптоаналізу. Виявлення слабких ключів та вразливих реалізацій.	4
Тема 6. Технології криптоаналізу. Диференціальний та лінійний криптоаналіз. Використання статистичних методів у криптоаналізі. Підбір ключів та атаки на протоколи. Автоматизація криптоаналізу за допомогою програмних засобів.	4
Тема 7. Паралельні обчислювання. Основи паралельного програмування. Використання багатопоточності та GPU. Паралельний криптоаналіз та розподілені обчислення. Практична реалізація алгоритмів шифрування на багатоядерних системах.	4
Тема 8. Нейронні мережі. 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.	4
Загальна кількість годин	**32**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Використання принципів кіберзахисту при проектуванні та розробці ПЗ. Виявлення загроз та вразливостей у проекті. Використання принципів безпечного кодування. Захист конфіденційних даних у програмі. Практичне застосування патернів безпечного програмування.	6	1
Тема 2. Технології шифрування. Реалізація симетричного шифрування (AES, DES). Реалізація асиметричного шифрування (RSA, ECC). Використання криптографічних бібліотек (PyCrypto, OpenSSL). Шифрування та дешифрування файлів і повідомлень.	6	1
Тема 3. Аналіз алгоритмів шифрування. Тестування стійкості шифрів до простих атак. Порівняння швидкості та ресурсомісткості різних алгоритмів. Практичне виявлення слабких місць алгоритмів.	6	1
Тема 4. Технології реверс-інжинірингу. Використання дизасемблерів та декомпіляторів (Ghidra, IDA Pro). Аналіз виконуваних файлів на наявність прихованої логіки. Виявлення шифрувальних алгоритмів у програмному коді. Декомпіляція та інтерпретація функцій.	6	1
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.	6	1

Автоматизація процесу криптоаналізу. Використання готових бібліотек для перевірки стійкості шифрів. Вимірювання складності та часу атаки. Практичне виявлення уразливих ділянок у шифрах.		
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

За наявності

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 атак на ПЗ (SQL-ін'єкції, XSS, buffer overflow). Захист програмного коду від несанкціонованого доступу.	13
Тема 2. Практичне застосування симетричного та асиметричного шифрування. Розгляд алгоритмів AES, DES, RSA, ECC. Використання бібліотек шифрування у різних мовах програмування. Криптографічні протоколи для передачі даних.	13
Тема 3. Криптографічні хеш-функції та протоколи обміну ключами. Принципи роботи хеш-функцій (SHA, MD5, Blake2). Використання хеш-функцій для перевірки цілісності даних. Алгоритми обміну ключами: Diffie-Hellman, ECDH.	13

Тема 4. Методи реверс-інжинірингу: дизасемблери та декомпілятори. Аналіз виконуваних файлів та бібліотек. Використання програмних інструментів: IDA Pro, Ghidra, Radare2. Виявлення логіки роботи алгоритмів та шифрів у коді.	13
Тема 5. Диференціальний та лінійний криптоаналіз на прикладі симетричних шифрів. Поняття диференціального та лінійного криптоаналізу. Практичне застосування на простих блокових шифрах. Аналіз слабких місць S-блоків та ключових схем.	12
Тема 6. Використання багатопоточності та GPU для прискорення обчислень. Основи паралельного програмування (OpenMP, CUDA, OpenCL). Прискорення криптоаналізу та обчислювальних задач. Вимірювання продуктивності та ефективності паралельних алгоритмів.	12
Тема 7. Практичне навчання нейронних мереж на криптографічних даних. Введення у машинне навчання та нейронні мережі. Використання нейронних мереж для розпізнавання патернів у шифрованих даних. Реалізація простих моделей на Python (TensorFlow, PyTorch).	12
Тема 8. Автоматизація аналізу алгоритмів шифрування за допомогою програмних засобів. Написання скриптів для перевірки стійкості шифрів. Використання готових бібліотек для криптоаналізу. Побудова автоматизованих тестів для різних типів шифрів.	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. 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. Євсеєв, 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. Євсеєв С.П. КІБЕРБЕЗПЕКА: КРИПТОГРАФІЯ З PYTHON: навч. посібн. / С.П. Євсеєв, 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:

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

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