КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015

Кафедра інженерії програмного забезпечення та кібербезпеки

ЗАТВЕРДЖЕНО
Вченою радою
(прот. № 6 від «07» 05 2021 р.)
Ректор
_____ А.А. Мазаракі

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ /
CRYPTOGRAPHIC METHODS OF INFORMATION PROTECTION

ПРОГРАМА /
COURSE SUMMARY

Київ 2021

Автори: Н.В. ЛУКОВА-ЧУЙКО, доктор технічних наук, професор кафедриінженерії програмного забезпечення та кібербезпеки,
А.О. ФЕСЕНКО, кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки,
Т.В. САВЧЕНКО, кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Л.О. ВЛАСЕНКО, кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки
М.В. САШНЬОВА, кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Ю.В. КОСТЮК, асистент кафедри інженерії програмного забезпечення та кібербезпеки

Програму розглянуто і затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки «20» квітня 2021 р., протокол №8.

Рецензенти: С.Л. РЗАЄВА, кандидат технічних наук, доцент
О.О. РУДЕНКО, Front-endTeamLeadatAstoundCommerce
В.Ф. ГАМАЛІЙ, доктор фіз.-мат. наук, професор

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ /
CRYPTOGRAPHIC METHODS OF INFORMATION PROTECTION
ПРОГРАМА /
COURSE SUMMARY

ВСТУП

Дисципліна «Криптографічні методи захисту інформації» призначена для здобувачів другого рівня вищої освіти «Магістр» галузі знань 12 «Інформаційні технології», спеціальності 124 «Системний аналіз», спеціалізації «Інформаційні технології та бізнес-аналітика (Data Science)».

Програму підготовлено відповідно до Стандартів вищої освіти України із зазначених спеціальностей та відповідних освітньо-професійних програм підготовки бакалаврів КНТЕУ.

Програма складається з таких частин:

1. Мета, завдання та предмет дисципліни.
2. Передумови вивчення дисципліни як вибіркової компоненти освітньої програми.
3. Результати вивчення дисципліни.
4. Зміст дисципліни.
5. Список рекомендованих джерел.

1. МЕТА, ЗАВДАННЯ ТА ПРЕДМЕТ ДИСЦИПЛІНИ

Метоювивчення дисципліни «Криптографічні методи захисту інформації» є формування у майбутніх фахівців сучасного рівня культури з інформаційної безпеки; набуття практичних навичок з основ застосування сучасних методів забезпечення криптографічного захисту інформації в комп'ютерних системах, а також надання студентам системних знань з принципів побудови систем криптографічного захисту інформації в КС.

Завданнями вивчення дисципліни «Криптографічні методи захисту інформації» є:

- розгляд основних етапів історичного розвитку криптографії;
- оволодіння теоретичними знаннями про основні методи криптографічного захисту інформації;
- розгляд математичних моделей симетричних шифрів та їх властивостей;
- оволодіння основними способами шифрування даних;
- вивчення методів асиметричної криптографії;
- дослідження особливостей криптографічних алгоритмів та криптографічних протоколів;
- ознайомлення з основними положеннями нормативно-правового регулювання у галузі криптографічного захисту інформації;
- розгляд основних напрямків розвитку сучасних систем

криптографічного захисту інформації.

Предметом вивчення навчальної дисципліни «Криптографічні методи та засоби захисту інформації» є забезпечення формування знань та вмінь, визначених освітньо-кваліфікаційною характеристикою, за сукупністю й рівнями їхньої сформованості, необхідними для вирішення професійних завдань.

2. ПЕРЕДУМОВИ ВИВЧЕННЯ ДИСЦИПЛІНИ ЯК ВИБІРКОВОЇ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ

знання:

- безпека баз даних;
- безпека операційних систем;
- основи кіберпезпеки;
- правове забезпечення інформаційної безпеки держави;
- теорії чисел;
- теорії ймовірностей та математичної статистики;
- математичного аналізу;
- комп'ютерної дискретної математики;
- економічної інформатики (стандартне програмне забезпечення персональних комп'ютерів);
- архітектури комп'ютера;
- захист систем електронних комунікацій;
- об'єктно-орієнтованого програмування;
- іноземної мови за професійним спрямуванням;

вміння: вільно працювати:

- з офісними додатками Microsoft;
- з хмарними сервісами Office 365;
- з технологіями розробки та тестуванням ПЗ;
- з пошуковою системою Google.

3. РЕЗУЛЬТАТИ ВИВЧЕННЯ ДИСЦИПЛІНИ

Дисципліна «Криптографічні методи захисту інформації», як обов'язкова компонента освітньої програми, забезпечує оволодіння студентами загальними та фаховими компетентностями і досягнення ними програмних результатів навчання за відповідними освітньо-професійними програмами:

Спеціальність 124 «Системний аналіз», спеціалізації «Інформаційні технології та бізнес-аналітика (Data Science)» (ОС магістр)

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Загальні компетентності за освітньою програмою		
ЗК3	Здатність до пошуку, оброблення та аналізу інформації з різних джерел.	1 – 7
Фахові компетентності за освітньою програмою		
СК2	Здатність проєктувати архітектуру інформаційних систем.	1 – 7
СК3	Здатність розробляти системи підтримки прийняття рішень та рекомендаційні системи.	1-7
СК7	Здатність управляти робочими процесами у сфері інформаційних технологій, які є складними, непередбачуваними та потребують нових стратегічних підходів.	2-5
СК13	Здатність розробляти і впроваджувати моделі задач інтелектуального аналізу даних засобами комп'ютерного моделювання.	1-4
Програмні результати навчання за освітньою програмою		
1	Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері системного аналізу та інформаційних технологій і є основою для оригінального мислення та проведення досліджень.	1-7
4	Розробляти та застосовувати методи, алгоритми та інструменти прогнозування розвитку складних систем і процесів різної природи.	1-7
5	Використовувати міри оцінювання ризиків та застосовувати їх при аналізі багатофакторних ризиків в складних системах	1-7
8	Здійснювати ідентифікацію та оцінювання параметрів математичних моделей об'єктів керування.	1-7

4. ЗМІСТ ДИСЦИПЛІНИ

Тема 1. Історичний огляд криптографічних методів захисту інформації

Історія криптографії. Базові поняття криптографії. Роль криптографії у захисті даних. Поняття шифру. Шифр простої замінитайого аналіз. Шифри перестановки таїх аналіз. Варіанти ускладнення шифру простої заміни. Шифр багатоалфавітної замінитайого аналіз. Вимогидо шифрів - принцип Керхгоффса. Шифрувальні машинита підходидоїх аналізу. Ідеальний шифр і класи стійкості шифрів.

Список рекомендованих джерел:
Основний: 1, 3, 4
Додатковий: 10, 14, 15
Internet-ресурси:

Тема 2.Сучасні криптографічні методи захисту інформації

Вимоги до сучасних криптографічних систем. Шифри на основімережі Фейстеля. Мережа Фейстеля. Американський шифр DES. Шифр «Магма». Шифри на основі SP-мережі. Стандарт AES. Асиметричні системи шифрування. Концепція асиметричного шифрування. Протокол Діффі-Хеллмана. Криптосистема RSA. Схемиелектронного цифрового підпису. Надійність цифрового підпису.Хеш-функції, призначення та їх основні властивості. Класифікація функцій хешування.

Список рекомендованих джерел:
Основний: 1, 2, 5
Додатковий: 12, 17, 18
Internet-ресурси:

Тема 3. Криптографія та криптоаналіз. Симетричні та асиметричні криптографічні перетворення

Криптографічне перетворення. Симетричні криптографічні перетворення. Структура алгоритму DES. Операції алгоритму IDEA. Сімейство алгоритмів RC. Основні методи криптоаналізу. Методи генерації псевдовипадкових числових послідовностей. Модулярна арифметика. Односторонні функції та їх властивості. Отримання великих простих чисел. Сучасні асиметричні криптосистеми.Опискриптосистеми RSA. Криптосистеми Рабіна та Ель-Гамаля. Перспективи розвитку криптографії. Вплив криптографії на суспільство. Створення комбінованих криптографічних засобів та нові підходи до побудови шифрів. Реалізація технології квантової криптографії.

Список рекомендованих джерел:
Основний: 1, 2, 5
Додатковий: 12, 17, 18
Internet-ресурси:19

Тема 4. Криптографічні протоколи

Поняття криптографічних протоколів. Їх опис. Класифікація криптографічних протоколів. Властивості, що визначають безпеку криптографічних протоколів. Атаки на протоколи. Аналіз та моделювання криптографічних протоколів. Протоколи електронного цифрового підпису. Протоколи, що ґрунтуються на симетричних криптосистемах. Протоколи, що ґрунтуються на асиметричних криптосистемах. Протоколи обміну ключами. Квантовий розподіл ключів. Протокол розподілу ключів за допомогою еліптичних кривих.

Список рекомендованих джерел:
Основний: 2 –4
Додатковий: 6 – 8, 13, 15, 17
Internet-ресурси:19

Тема 5. Протоколи аутентифікації (ідентифікації)

Основні етапи аутентифікації та авторизації. Чинники аутентифікації. Аутентифікація суб'єктів доступа. Аутентифікація на основі знань. Аутентифікація на основі володіння. Аутентифікація на основі ознак та дій. Парольна аутентифікація. Аутентифікація на основі коректної обробки алгоритмів. Аутентифікація на основі електронних і фізичних ключів. Протокол ідентифікації/аутентифікації на основі шифрування з відкритим ключем. Біометрична аутентифікація. Авторизація. Реєстрація подій у системі. Розмежування доступу. Дискреційна модель розмежування доступу. Мандатна модель розмежування доступу. Рольова модель розмежування доступу.

Список рекомендованих джерел:
Основний: 3, 4
Додатковий: 7 – 9, 14, 15, 17
Internet-ресурси:19

Тема 6. Управління криптографічними ключами

Сутність управління ключами. Принцип Керкгоффса. Стандарти генерації ключів. Накопичення, розподілення, оновлення, зберігання, резервування ключів. Генерація ключів. Модифікація ключа. Зберігання ключів. Розподіл ключів. Трирівнева ієрархія розподілу ключів: головний

ключ; ключ шифрування ключів; ключ шифрування даних (сеансовий ключ). Децентралізований та централізований розподіл ключів. Протоколи обміну ключами. Протокол Kerberos. ПротоколШаміра. Алгоритм Діффі-Хеллмана.

Список рекомендованих джерел:

Основний: 1, 3, 4
Додатковий: 7 – 9, 14, 15 – 18
Internet-ресурси:19

Тема 7.Стеганографічний захист інформації

Історичний оглядстеганографії. Основні поняття стеганографії. Стеганографічна система. Стеганографічний контейнер. Стеганографічний канал. Основнізагрози безпекистеганографічних систем. Виявлення стеганографічного каналу. Типипорушників безпекистеганографічних систем. Три класи порушників: пасивний, активний та зловмисник. Типи атак на стеганографічні системи. Атака з відомим контейнером. Атака з вибором контейнера. Атака з відомим повідомленням. Атака з вибором повідомлення. Атака, що направлена на руйнування повідомлення. Комп'ютерна та цифрова стеганографія. Сфера використання методів стеганографічного захистуінформації.

Список рекомендованих джерел:

Основний: 1 – 5
Додатковий: 6 – 9, 11, 13 – 17
Internet-ресурси: 19 – 22

5. СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

1. Бабак В. П. Теоретичні основи захисту інформації : підручник // Бабак В. П. – Книжкове видавництво НАУ, 2008. – 752 с.
2. *Основи криптографічного захисту інформації : підручник / авт.: Г.М. Гулак, В.А. Мухачов, В.О. Хорошко, Ю.Є. Яремчук. – Вінниця : ВНТУ, 2011. – 94 с.*
3. Основи захисту інформації : навч. посібн. / О. А. Смірнов, Л. Г. Віхрова, С. І. Осадчий та ін. – Кіровоград, 2010. – 322 с.
4. Основи інформаційної безпеки / С. В. Кавун, О. А. Смірнов, В. Ф. Столбов – Кіровоград : Вид. КНТУ, 2012. – 414 с.
5. Фаль О. М. Криптографія : основні ідеї та застосування / О. М. Фаль. – К. : ІВЦ Видавництво «Політехніка», 2003. – 28 с.

Додатковий

6. Блінцов В. С. Захист програмних продуктів : навчальний посібник / В. С. Блінцов, С. С. Козирев. – Миколаїв : НУК, 2010. – 146 с.
7. Голубєв В. О. Інформаційна безпека : проблеми боротьби з кіберзлочинами : монографія / В. О. Голубєв. – Запоріжжя : ГУ «ЗІДМУ», 2003. – 250 с.
8. Гулак Г. Н. Основыкриптографическойзащитыинформации / Г. Н. Гулак. – К. : Вид. ГУІКТ, 2009. – 228 с.
9. Довгий С. О. Сучасні телекомунікації : Мережі, технології, безпека, економіка, регулювання: монографія / С. О. Довгий, П. П. Воробієнко, К. Д. Гуляєв; За загальною ред. С. О. Довгого. – [2-ге видання (доповнене)]. – К. : Аимут-Україна, 2013. – 608 с.
10. Защитакомпьютернойинформации. Эффективныеметоды и средства / Шаньгин В. Ф. – К. : ДМК Пресс, 2008. – 544 с.
11. Інформаційний та кіберпростори : проблеми безпеки, методи та засоби боротьби : посібник / В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін. – К. : ДУТ – КНУ, 2016. – 178 с.
12. Кавун С. В. Інформаційна безпека : підручник / С. В. Кавун. – Харків: Вид. ХНЕУ, 2009. – 368 с.
13. Конахович Г. Ф. Захист інформації в мережах передачі даних : підручник / Г. Ф. Конахович. – К. : Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 714 с.
14. Криптографія [Електронний ресурс]. – Режим доступу : http://uk.wikipedia.org/wiki/Криптографія.

15. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 512 с.
16. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. Правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с.
17. Смит Р. Є. Аутентификация: от паролей до открытых ключем / Р. Є. Смит. – К. : Видавничий дім «Вільямс», 2002. – 432 с.
18. Столлингс В. Криптография и защитасетей : принципы и практика / В. Столлингс. – К. : Видавничий дім «Вільямс», 2001. – 672 с.

Internet-ресурси

19. http://www.dsszzi.gov.ua/dsszzi/control/uk/index
20. http://jrnl.nau.edu.ua/index.php/ZI
21. www.bsm.com.ua
22. http://www.rada.gov.ua

**Курсивом зазначені джерела, що є в наявності в бібліотеці КНТЕУ*