КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
Кафедра інженерії програмного забезпечення та кібербезпеки

СИЛАБУС

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ / CRYPTOGRAPHIC METHODS OF INFORMATION PROTECTION

SYLLABUS

ОП 2018

освітній ступінь	**бакалавр**	**/**	bachelor
галузь знань	**12 Інформаційні технології**	/	Information technologies
спеціальність	**125 Кібербезпека**	/	Cybersecurity
спеціалізація	**Безпека інформаційних і комунікаційних систем в економіці**	/	Security of information and communication systems in the economy

Київ 2021

Автори: А.О. ФЕСЕНКО, кандидат технічних наук, доцент

Силабус розглянуто і затверджено на засіданні кафедри програмної інженерії та інформаційних технологій 27 серпня 2021 протокол № 1.

СИЛАБУС

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ / CRYPTOGRAPHIC METHODS OF INFORMATION PROTECTION

SYLLABUS

освітній ступінь	**бакалавр**	**/**	bachelor
галузь знань	**12 Інформаційні технології**	/	Information technologies
спеціальність	**125 Кібербезпека**	/	Cybersecurity
спеціалізація	**Безпека інформаційних і комунікаційних систем в економіці**	/	Security of information and communication systems in the economy

1. **Викладач**:

1.1. **Лектор**: Фесенко Андрій Олексійович,

- *вчене звання та посада*: кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки;
- *педагогічний стаж* – 5 років;
- *e-mail:*a.fesenko@knute.edu.ua;
- *наукові інтереси*: системи біометричної ідентифікації, квантова криптографія, криптографічні механізми захисту інформації
- *стажування та підвищення кваліфікації*:
  - "Методи та засоби реалізації інформаційної безпеки у технологіях віртуального навчання. Linkos Group «Інформаційні технології в економіці: інноваційні рішення захисту даних підприємства» в обсязі 180 академічних годин)

2. **Дисципліна**: **«Криптографічні методи захисту інформації»**,
   - рік навчання: 4;
   - семестр навчання: 7;
   - кількість кредитів: 6;
   - кількість годин за семестр: 180 год.
     - лекційних: 24 год.
     - лабораторних: 56 год.
     - на самостійне опрацювання: 96 год.
   - кількість аудиторних годин на тиждень:
     - лекційних: 2 год.
     - лабораторних: 4 год.

3. **Час та місце проведення:**
   - аудиторні заняття - відповідно до розкладу КНТЕУ з врахуванням специфіки дисципліни передбачено в аудиторіях: 510;
   - поза аудиторна робота - самостійна робота студента, результат виконання якої висвітлено засобами Office 365;
   - всі лабораторні завдання виконуються на основі інтерактивних методів навчання у електронному середовищі. Передбачається можливість проведення практичних та лекційних занять на базах підприємств-партнерів.
   - під час карантинних обмежень усі заняття проводяться у Microsoft Teams, події плануються заздалегідь, повідомлення про заплановані події надсилається на корпоративну пошту, відображається у календарі та у команді БПЗ, лекції.

4. **Пререквізити та постреквізити навчальної дисципліни:**
   - **пререквізити:** дисципліна базується на знаннях та компетентностях,що набуває здобувач вищої освіти під час вивчення дисциплін «Комп'ютерна дискретна математика», «Теорія ймовірності та математична статистика», «Теорія чисел».
   - **постреквізити:** Дисципліна надає студентам необхідні знання та навички, які будуть корисні при проходженні виробничої практики, підготовці до випускного кваліфікаційного проекту та у подальшій професійній діяльності.

- **програмні результати навчання та компетенції:** Відображені в освітній програмі та програмі дисципліни.

5. Результати вивчення дисципліни:

«Безпека інформаційних і комунікаційних систем в економіці» (ОС бакалавр 2018 р.)

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Загальні компетентності за освітньою програмою		
КЗ1	Здатність застосовувати знання у практичних ситуаціях	1-10
КЗ2	Знання та розуміння предметної області та розуміння професії.	1-10
КЗ4	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.	1-10
Фахові компетентності за освітньою програмою		
КФ10	Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.	1-10
Програмні результати навчання за освітньою програмою		
44	Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.	1-10
47	Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.	1-10
48	Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.	1-10

6. Характеристика дисципліни:

6.1. Призначення навчальної дисципліни:є забезпечення формування знань та вмінь, визначених освітньо-кваліфікаційною характеристикою, за сукупністю й рівнями їхньої сформованості, необхідними для вирішення професійних завдань.

6.2. Мета вивчення 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.

6.3. Зміст навчальної дисципліни: відповідає навчальній та робочій програмі, яка відповідає запитам стейкхолдерів.

Назва теми	Кількість годин				Форми контролю
	Усього год/кредитів	Лекції	Лабораторні заняття	Самостійна робота студ.	
Тема1. Історичний огляд криптографічних методів захисту інформації	18	2	8	8	УО, ЛР,
Тема 2. Сучасні криптографічні методи захисту інформації	20	2	8	10	УО, ЛР
Тема 3. Основні принципи роботи блокових шифрів.	34	4	20	10	УО, ЛР,
Тема 4. Криптографія та криптоаналіз. Симетричні та асиметричні криптографічні перетворення	10	2		8	УО, ЛР
Тема 5. Основні Алгоритми (Діфі-Хелмана, Ель-Гамаля, RSA, та інші)	22	2	10	10	УО, ЛР
Тема 6. Криптосистеми з відкритим ключем на основі еліптичних кривих	22	2	10	10	УО, ЛР
Тема 7. Криптографічні протоколи	14	4		10	УО, ЛР
Тема 8.Протоколи аутентифікації (ідентифікації)	12	2		10	УО, ЛР
Тема 9. Управління криптографічними ключами	14	4		10	УО, ЛР
Тема 10. Стеганографічний захист інформації	14	4		10	УО, ЛР, Т
Разом	**180/6**	**28**	**56**	**96**	
Підсумковий контроль – екзамен					

УО – усне опитування; ЛР – захист лабораторних робіт; Т – тестування.

6.4. План вивчення дисципліни:

ТЕОРЕТИЧНИЙ БЛОК:

Навчальна діяльність	Робочий час студента (год.)
1	2
Тема 1. Історичний огляд криптографічних методів захисту інформації *План лекції* 1. Історія криптографії. 2. Базові поняття криптографії. 3. Роль криптографії у захисті даних. 4. Поняття та види шифрів. 5. Вимогидо шифрів - принцип Керхгоффса. 6. Шифрувальні машинита підходидоїх аналізу. 7. Ідеальний шифр і класи стійкості шифрів.	2

1	2
Список рекомендованих джерел: *Основний: 1, 3, 4* *Додатковий: 10, 14, 15*.	
Тема 2. Сучасні криптографічні методи захисту інформації *План лекції* 1. Основні види криптографічних методів 2. Реалізація криптографічних методів 3. Симетричні і асиметричні методи шифрування 4. Шифри на основі мережі Фейстеля. Мережа Фейстеля. 5. Американський шифр DES. 6. Шифри на основі SP-мережі. **Список рекомендованих джерел:** *Основний: 1, 2, 5* *Додатковий: 12, 17, 18* *Internet-ресурси: 19*	2
Тема 3. Основні принципи роботи блокових шифрів *План лекції* 1. Сучасні блокові шифри 2. Компоненти сучасного блокового шифру 3. Розгляд відомих блокових шифрів (ГОСТ 28147, DES, AES, ДСТУ 7624 і т.д.). Переваги недоліки. 4. Складені шифри 5. Режими роботи блокових шифрів **Список рекомендованих джерел:** *Основний: 1, 2, 5* *Додатковий: 12, 17, 18* *Інтернет-ресурси:* 19, 21.	4
Тема 4. Криптографія та криптоаналіз. Симетричні та асиметричні криптографічні перетворення *План лекції* 1. Криптографічне перетворення. 2. Симетричні криптографічні перетворення. 3. Методи генерації псевдовипадкових числових послідовностей. Модулярна арифметика. 4. Перспективи розвитку криптографії. Вплив криптографії на суспільство. 5. Створення комбінованих криптографічних засобів та нові підходи до побудови шифрів. **Список рекомендованих джерел:** *Основний:* 1, 2, 3. *Додатковий:* 8-10. *Інтернет-ресурси:* 19, 20, 21.	2
Тема 5. Основні Алгоритми (Діфі-Хелмана, Ель-Гамаля, RSA, та інші) *План лекції* 1. Криптосистема Ель–Гамаля. 2. Шифрування та розшифрування в криптосистемі Ель–Гамаля. 3. Коректність, ефективність та надійність криптосистем Рабіна та Ель-Гамаля. 4. Криптосистема Діфі-Хелмана. 5. Шифрування та розшифрування в криптосистемі Діфі-Хелмана. 6. Коректність, ефективність та надійність криптосистем Діфі-Хелмана.	2

1	2
Список рекомендованих джерел: *Основний:* 1, 2, 3. *Додатковий:*6-7. *Інтернет-ресурси:*20, 21	
Тема 6. Криптосистеми з відкритим ключем на основі еліптичних кривих *План лекції* 1. Принципи еліптичної криптографії. 2. Методи шифрування в еліптичній криптографії. 3. Алгебраїчні операції в скінчених полях. 1. Особливості програмної реалізації операції над точками еліптичної кривої. **Список рекомендованих джерел:** *Основний: 1, 2, 5* *Додатковий: 12, 17, 18* *Internet-ресурси:19*	2
Тема 7. Криптографічні протоколи *План лекції* 1. Поняття криптографічних протоколів. Їх опис. 2. Класифікація криптографічних протоколів. Властивості, що визначають безпеку криптографічних протоколів. 3. Атаки на протоколи. 4. Аналіз та моделювання криптографічних протоколів. 5. Протоколи електронного цифрового підпису. **Список рекомендованих джерел:** *Основний: 2 –4* *Додатковий: 6 – 8, 13, 15, 17* *Internet-ресурси:19*	4
Тема 8. Протоколи аутентифікації (ідентифікації) *План лекції* 6. Основні етапи аутентифікації та авторизації. 7. Чинники аутентифікації. 8. Класифікація видів аутентифікації 9. Розмежування доступу. 10. Моделі розмежування доступу. **Список рекомендованих джерел:** *Основний: 3, 4* *Додатковий: 7 – 9, 14, 15, 17* *Internet-ресурси:19*	2
Тема 9. Управління криптографічними ключами *План лекції* 1. Сутність управління ключами. Принцип Керкгоффса. 2. Стандарти генерації ключів. Накопичення, розподілення, оновлення, зберігання, резервування ключів. 3. Генерація та модифікація ключа. 4. Зберігання тарозподіл ключів. 5. Протоколи обміну ключами. 6. Протоколів, що ґрунтуються на симетричних криптосистемах 7. Протоколи, що ґрунтуються на асиметричних криптосистемах	4

1	2
Список рекомендованих джерел: *Основний: 1, 3, 4* *Додатковий: 7 – 9, 14, 15 – 18* *Internet-ресурси:19, 22*.	
Тема 10. Стеганографічний захист інформації *План лекції* 1. Історичний огляд стеганографії. 2. Стеганографічна система. Стеганографічний контейнер. Стеганографічний канал. 3. Виявлення стеганографічного каналу. 4. Типи та класи порушників безпеки стеганографічних систем. 5. 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. 6. Комп'ютерна та цифрова стеганографія. **Список рекомендованих джерел:** *Основний: 1 – 5* *Додатковий: 6 – 9, 11, 13 – 17* *Internet-ресурси: 19 – 22*	4

ЛАБОРАТОРНІ ЗАНЯТТЯ:

Навчальна діяльність	Робочий час студента (год.)	Бали

1	2	
Тема 1. Історичний огляд криптографічних методів захисту інформації ***Список рекомендованих джерел:*** *Основний: 1, 3, 4* *Додатковий: 10, 14, 15*. Лабораторне заняття № 1 **"Шифр Цезаря"** **Мета:** оволодіння практичними навичками із застосування методів частотного аналізу до шифру Віженера. **Завдання:** Написати програму для шифрування тексту за допомогою методу «Шифр Цезаря». Необхідно реалізувати як шифрування, так і дешифрування текстів українською та англійською мовами. Знайти ключ, використовуючи оцінку логарифмічної функції правдоподібності та розшифрувати текст, зашифрований на українській мові за алгоритмом Цезаря **Результати навчання.** проводити шифрування і дешифрування тексту, написаного кирилицею і латиницею, «методом Цезаря»	8	15
Тема 2. Сучасні криптографічні методи захисту інформації ***Список рекомендованих джерел:*** *Основний: 1, 2, 5*	8	15

1	2	
Додатковий: 12, 17, 18 *Internet-ресурси: 19* Лабораторне заняття № 2 **Криптоаналіз шифру Віженера** **Мета:**оволодіння практичними навичками із застосування методів частотного аналізу до шифру Віженера. **Завдання:** Знайти ключ, довжина якого відома та розшифрувати криптограму, яка зашифрована шифром Віженера (алфавіт – український із пропуском). Для криптоаналізу використовувати таблицю частот. Визначити довжину ключа, ключ та розшифрувати криптограму, яка зашифрована шифром Віженера (алфавіт — український із пропуском). **Результати навчання.** проводити шифрування і дешифрування тексту, написаного кирилицею і латиницею, «методом Віженера» (метод Казискі, Перший метод Фрідмана)		
Тема 3. Основні принципи роботи блокових шифрів ***Список рекомендованих джерел:*** *Основний: 1, 2, 5* *Додатковий: 12, 17, 18* *Інтернет-ресурси:* 19, 21. Лабораторне заняття № 3 **Криптоаналіз шифрів стовпцевої перестановки та подвійної перестановки** **Мета**: вивчення елементів частотного аналізу криптограми: частоти біграм, сполучність букв. **Завдання:** Розшифрувати вислів, зашифрований стовпцевою перестановкою (текст українською мовою). Для криптоаналізу використовуються таблиці біграм та сполучність букв. Розшифрувати вислів, зашифрований подвійною перестановкою (спочатку були переставлені стовпці, потім рядки; текст українською мовою). **Результати навчання** проводити шифрування і дешифрування українського тексту, зашифрованого стовпцевою перестановкою та подвійною перестановкою, а також за допомогою шифру S-DES. Лабораторне заняття № 4 **Алгоритми шифрування S-DES** **Мета:** вивчення структури DES – для шифрування і дешифрування з використанням блокових шифрів. **Завдання:** написати програму, що реалізує процес шифрування та дешифрування даних за допомогою шифру S-DES в режимі Electronic Code Book (ECB). **Результати навчання** проводити шифрування і дешифрування українського тексту, зашифрованого за допомогою шифру S-DES	10 10	15 15
Тема 5. Основні Алгоритми (Діфі-Хелмана, Ель-Гамаля, RSA, та інші) ***Список рекомендованих джерел:***	10	15

1	2	
Основний: 1, 2, 3. *Додатковий:*6-7. *Інтернет-ресурси:* 20, 21 Лабораторне заняття № 5 **Алгоритм блочного шифрування даних ДСТУ ГОСТ 28147:2009** **Мета:**отримати навички у реалізації на вибраній мові програмування алгоритму блочного шифрування даних ДСТУ ГОСТ 28147:2009. **Завдання:** розробити на обраній мові програмування консольний або віконний додаток, що реалізує алгоритм ДСТУ ГОСТ 28147:2009 за такими режимами шифрування: режим простої заміни (з доповненням блоків);режим гамування;режим гамування зі зворотним зв'язком. Вхідні дані: вхідний текст у вигляді символів або байтів, ключ, вектор ініціалізації (синхропосилка), режим роботи (шифрування або дешифрування), режим шифрування. Вихідні дані: для шифрування – послідовність байтів зашифрованого **Результати навчання** проводити шифрування і дешифрування українського тексту на основі алгоритмів блочного шифрування.		
Тема 6. Криптосистеми з відкритим ключем на основі еліптичних кривих ***Список рекомендованих джерел:*** *Основний: 1, 2, 5* *Додатковий: 12, 17, 18* *Internet-ресурси:19* Лабораторне заняття № 6 **Потокове шифрування на базі РЗЛЗЗ** **Мета:** отримати навички у створенні програмної реалізації алгоритму потокового шифрування на базі регістра зсуву з лінійним зворотним зв'язком (РЗЛЗЗ). **Завдання:** розробити на обраній мові програмування консольний або віконний додаток, що реалізує описаний алгоритм потокового шифрування на базі РЗЛЗЗ для шифрування вмісту текстового або виконуваного файлу. Програма повинна запитувати ім'я вхідного і вихідного файлів, представлення утворюваного многочлена та ініціалізуюче значення. Розрядність РЗЛЗЗ повинна бути меншою або дорівнювати максимальній розрядності стандартних цілочисельних типів даних (64 біт). **Результати навчання** *проводити шифрування і дешифрування українського тексту на основі алгоритмів потокового шифрування*	10	15

** всі лабораторні завдання виконуються на основі інтерактивних методів навчання у комп'ютерному середовищі*

САМОСТІЙНА РОБОТА:

Навчальна діяльність	Робочий час студента (год.)	Бали
1	2	3
Тема 1. Історичний огляд криптографічних методів захисту інформації ***Список рекомендованих джерел:*** *Основний: 1, 3, 4* *Додатковий: 10, 14, 15*. **Самостійна робота:** Вивчення матеріалів лекції на основі самостійного опрацювання основних літературних джерел, зазначених у списку та електронних матеріалів, які надаються викладачем. Ознайомлення і оволодіння понятійним апаратом. Вивчення різних видів шифрів та особливостей їх використання.	8	1
Тема 2. Сучасні криптографічні методи захисту інформації ***Список рекомендованих джерел:*** *Основний: 1, 2, 5* *Додатковий: 12, 17, 18* *Internet-ресурси: 19* **Самостійна робота:** Вивчення матеріалів лекції на основі самостійного опрацювання основних літературних джерел, зазначених у списку та електронних матеріалів, які надаються викладачем. Визначити різницю між закритими і відкритими ключами. Ознайомитись з особливостями шифрування і дешифрування шифрами на основі мережі Фейстеля та її модифікацій, SP-мережі та DataEncryption Standard	10	1
Тема 3. Основні принципи роботи блокових шифрів ***Список рекомендованих джерел:*** *Основний: 1, 2, 5* *Додатковий: 12, 17, 18* *Інтернет-ресурси:* 19, 21. **Самостійна робота:** Вивчення матеріалів лекції на основі самостійного опрацювання основних літературних джерел, зазначених у списку та електронних матеріалів, які надаються викладачем. Вивчити особливості відомих блокових шифрів (ГОСТ 28147, DES, AES, ДСТУ 7624 і т.д.), їх переваги та недоліки. Засвоїти режими роботи блокових шифрів.	10	1
Тема 4. Криптографія та криптоаналіз. Симетричні та асиметричні криптографічні перетворення ***Список рекомендованих джерел:*** *Основний:* 1, 2, 3. *Додатковий:* 8-10. *Інтернет-ресурси:* 19, 20, 21. **Самостійна робота:** Вивчення матеріалів лекції на основі самостійного опрацювання основних літературних джерел, зазначених у списку та електронних матеріалів, які надаються викладачем. Ознайомлення з основами медулярної арифметики. Розглянути перспективи розвитку криптографії, підходи до створення комбінованих криптографічних підходів	8	1

Навчальна діяльність	Робочий час студента (год.)	Бали
1	2	3
до шифрування.		
Тема 5. Основні Алгоритми (Діфі-Хелмана, Ель-Гамаля, RSA, та інші) ***Список рекомендованих джерел:*** *Основний:* 1, 2, 3. *Додатковий:*6-7. ***Інтернет-ресурси: 20, 21*** **Самостійна робота:** Вивчення матеріалів лекції на основі самостійного опрацювання основних літературних джерел, зазначених у списку та електронних матеріалів, які надаються викладачем. Вивчення основ функціонування алгоритмів шифрування Ель-Гамаля та Діфі-Хелмана. Визначення коректності та проведення оцінки ефективності та надійності криптосистем, що функціонують на основі алгоритмів Ель-Гамаля та Діфі-Хелмана.	10	1
Тема 6. Криптосистеми з відкритим ключем на основі еліптичних кривих ***Список рекомендованих джерел:*** *Основний: 1, 2, 5* *Додатковий: 12, 17, 18* ***Internet-ресурси: 19*** **Самостійна робота**: Вивчення матеріалів лекції на основі самостійного опрацювання основних літературних джерел, зазначених у списку та електронних матеріалів, які надаються викладачем. Знати алгоритми, які використовуються для конкретних кінцевих груп переписуються для використання груп раціональних точок еліптичних кривих	10	1
Тема 7. Криптографічні протоколи ***Список рекомендованих джерел:*** *Основний: 2 –4* *Додатковий: 6 – 8, 13, 15, 17* *Internet-ресурси:19* **Самостійна робота:** Вивчення матеріалів лекції на основі самостійного опрацювання основних літературних джерел, зазначених у списку та електронних матеріалів, які надаються викладачем. 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.	10	1
Тема 8. Протоколи аутентифікації (ідентифікації) ***Список рекомендованих джерел:*** *Основний: 3, 4* *Додатковий: 7 – 9, 14, 15, 17* *Internet-ресурси:19* **Самостійна робота:** Вивчення матеріалів лекції на основі самостійного опрацювання основних літературних джерел, зазначених у списку та електронних матеріалів, які надаються	10	1

Навчальна діяльність	Робочий час студента (год.)	Бали
1	2	3
викладачем: 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. Дискреційна, мандатна та рольова моделі розмежування доступу		
Тема 9. Управління криптографічними ключами ***Список рекомендованих джерел:*** *Основний: 1, 3, 4* *Додатковий: 7 – 9, 14, 15 – 18* *Internet-ресурси:19, 22* **Самостійна робота:** Вивчення матеріалів лекції на основі самостійного опрацювання основних літературних джерел, зазначених у списку та електронних матеріалів, які надаються викладачем. Трирівнева ієрархія розподілу ключів: головний ключ; ключ шифрування ключів; ключ шифрування даних (сеансовий ключ). Децентралізований та централізований розподіл ключів. Протокол Kerberos. Протокол Шаміра. Алгоритм Діффі-Хеллмана.	10	1
Тема 10. Стеганографічний захист інформації ***Список рекомендованих джерел:*** *Основний: 1 – 5* *Додатковий: 6 – 9, 11, 13 – 17* *Internet-ресурси: 19 – 22* **Самостійна робота:** Вивчення матеріалів лекції на основі самостійного опрацювання основних літературних джерел, зазначених у списку та електронних матеріалів, які надаються викладачем. Основи стенографії, поняття стенагрофічної системи, контейнеру, каналу; 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.	10	1

7. 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. Основы криптографической защиты информации / 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. Защита компьютерной информации. Эффективные методы 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. Державна служба спеціального зв'язку та захисту інформації України http://www.dsszzi.gov.ua/dsszzi/control/uk/index
20. Захист інформації http://jrnl.nau.edu.ua/index.php/ZI
21. Бизнес и безопасностьwww.bsm.com.ua
22. Офіційний вебпортал парламенту Україниhttp://www.rada.gov.ua

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

8. Контроль та оцінювання результатів навчання:

Положення про оцінювання результатів навчання студентів і аспірантів наказ КНТЕУ №2891 від 16.09.2019р. (Електронний ресурс. Точка доступу: https://knute.edu.ua/file/NzU4MQ==/69da3a261374f213990591e6e9a812cd.pdf)

Під час вивчення дисципліни викладачем здійснюється поточний та підсумковий контроль. Поточний контроль та оцінювання передбачає:

- перевірку рівня засвоєння теоретичного матеріалу (тестування за матеріалами лекції, який здійснюється з використанням 365 Office);
- захист лабораторних робіт (проходить під час кожної лабораторної роботи);
- перевірка ходу виконання індивідуального завдання (фінальний проект);
- перевірка засвоєння матеріалу, що винесений на самостійне опрацювання під час фронтального опитування на лекції та заслуховування доповідей на обрані студентами теми;
- перевірка знань отриманих у ході неформальної освіти (додаткові рекомендовані курси).

9. Політика навчальної дисципліни:

9.1. Відвідування лекційних та лабораторних занять: відвідування лекційних та лабораторних занять є обов'язковим. Допускаються пропуски занять з таких поважних причин, як хвороба (викладачу надається копія довідки від медичного закладу), участь в олімпіаді, творчому конкурсі тощо за попередньою домовленістю та згодою викладача за умови дозволу деканату (надаються документи чи інші матеріали, які підтверджують заявлену участь у діяльності студента).

9.2. Відпрацювання пропущених занять: відпрацювання пропущених занять є обов'язковим незалежно від причини пропущеного заняття. Лекційне заняття має бути відпрацьоване до наступної лекції на консультації викладача з використанням ПЗ 365 OfficeTeams. Відпрацювання лекційного матеріалу передбачає вивчення пропущеного теоретичного матеріалу та складання тесту за цим матеріалом. Лабораторне заняття відпрацьовується під час консультації викладача (розклад консультацій на сайті).

9.3. Правила поведінки під час занять: обов'язковим є дотримання техніки безпеки в комп'ютерних лабораторіях. Студенти повинні приймати активну участь в обговоренні навчального матеріалу ознайомившись з ним напередодні (навчальний матеріал надається викладачем). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки практичних завдань в процесі заняття. Задля зручності, дозволяється використання ноутбуків та інших електронних пристроїв під час навчання в комп'ютерних аудиторіях (за взаємною згодою всіх учасників освітнього процесу)

9.4. За порушення академічної доброчесності студенти будуть притягнені до академічної відповідальності у відповідності до положення про дотримання академічної доброчесності педагогічними, науково-педагогічними, науковими працівниками та здобувачами вищої освіти КНТЕУ (Наказ КНТЕУ від 02.02.2018 №377. (Електронний ресурс. Точка доступу: https://knute.edu.ua/file/MTEyNDI=/f78c64a74cbbe5b4238729782d707efa.pdf)