

## СИЛАБУС

### Кафедра автоматизованого управління технологічними процесами

<b>Назва курсу</b>	Захист інформації в комп'ютерних системах
<b>Мова викладання</b>	Українська
<b>Викладач (-і)</b>	Юсипів Т. В., старший викладач кафедри загальноінженерних дисциплін та теплоенергетики
<b>Профайл викладача</b>	E-mail: yusypiv.taras@tnu.edu.ua ORCID: <a href="http://orcid.org/0000-0003-2798-9472">http://orcid.org/0000-0003-2798-9472</a>
<b>Контакти викладача</b>	E-mail: yusypiv.taras@tnu.edu.ua

#### 1. Анотація курсу

Навчальна дисципліна «Захист інформації в комп'ютерних системах» є складовою циклу професійної підготовки фахівців освітньо-кваліфікаційного рівня «бакалавр».

Курс підпорядковано вирішенню таких основних задач, як з'ясування концептуальних принципів аналізу побудови надійних комп'ютерних систем з точки зору їх інформаційної безпеки.

Короткий зміст курсу:

**Змістовий модуль 1. Основні напрямки захисту інформації в комп'ютерних системах**

**Тема 1. Концепція захисту інформації та інформаційних технологій.**

Категорії комп'ютерної безпеки. Огляд найбільш поширених методів комп'ютерного «злому». Концепція і концептуальна модель інформаційної безпеки. Класифікація загроз комп'ютерним системам.

**Тема 2. Основні методи захисту програмного забезпечення.**

Опис руйнуючих програмних засобів. Поняття комп'ютерних вірусів та їх класифікація. Захист операційних систем від програм-закладок. «Клавіатурні шпигуни» та їх класифікація. Налаштування антишпигунів.

**Тема 3. Захист баз даних.**

Загальна концепція захисту бази даних. Налаштування системи захисту СУБД. Захист СУБД від SQL-ін'єкцій. Цілісність бази даних та системи резервного копіювання. Проблема спільного доступу. Технічні (в тому числі, апаратні) засоби захисту даних від витоків.

**Тема 4. Організація захисту інформації в мережах.**

Типи засобів забезпечення захисту даних в розподілених обчислювальних середовищах та мережах. Системи аналізу глобальних та локальних вразливостей. Принципи побудови системи виявлення вторгнень. Вразливості протоколів мережі Internet. Методи розпізнавання спаму: чорні та білі списки, байєсовський підхід.

#### **Тема 5. Антивірусні програми та засоби.**

Механізми виявлення шкідливих та небезпечних програм. Засоби для профілактики та захисту комп'ютерних систем від вірусів. Антивірусні монітори та сканери. Налаштування антивірусів.

### **Змістовий модуль 2. Криптографічні засоби захисту інформації в комп'ютерних системах**

#### **Тема 1. Математичні основи сучасної криптології.**

Визначення криптології та сфери її застосування. Криптографічні інструменти та засоби. Ймовірнісні тести: Соловея-Штрассена та Міллера-Рабіна. Факторизація. Поняття ядра функції. Предикат з секретом та ймовірнісне криптування.

#### **Тема 2. Криптосистеми з відкритим ключем.**

Концепція відкритих систем. Система RSA. Система Рабіна. Пакет захисту PGP.

#### **Тема 3. Системи генерування, зберігання та обміну ключів. Цифровий підпис.**

Генератори псевдовипадкових бітів. Протоколи обміну ключами. Ідентифікація за допомогою симетричної криптосистеми, на основі цифрового підпису.

#### **Тема 4. Криптографічні засоби захисту інформації.**

Реалізація криптографічного захисту інформації на ПК, серверах та в мережах. Стеганографічні методи захисту інформації. Використання особливостей структури файлу. Використання особливостей візуалізації даних.

#### **Тема 5. Організація системи захисту інформації.**

Політика безпеки та методи захисту даних. Програми тестування та діагностики. Оптимізація дисків. Методи стискання й резервного зберігання інформації. Ідентифікація, верифікація та аутентифікація користувачів. Міжнародні сертифікати забезпечення захисту комп'ютерних систем.

## **2. Мета та цілі курсу**

Метою вивчення дисципліни «Захист інформації в комп'ютерних системах» є необхідність формування у студентів бази для подальшого засвоєння навиків роботи з комп'ютерними системами. Значення дисципліни для реалізації вимог кваліфікаційної характеристики фахівця та вивчення наступних дисциплін полягає в тому, що дисципліна сприяє формуванню відповідного мислення майбутнього фахівця, створює базу, яка необхідна при вивченні наступних дисциплін. Виходячи з цього викладання дисципліни «Захист інформації в комп'ютерних системах» підпорядковане вирішенню

таких основних задач, як з'ясування концептуальних принципів аналізу комп'ютерних систем з точки зору їх безпеки та захисту інформації, що ними зберігається чи обробляється. Розглядаються питання присвячені практичних аспектам використання набутих знань.

### 3. Результати навчання

Використовувати знання сучасних комп'ютерних наук, навички програмування та застосування програмних засобів, безпечної роботи в комп'ютерних мережах, уміння створювати бази даних, використовувати інтернет-ресурси та демонструвати уміння розробляти алгоритми та комп'ютерні програми на мовах високого рівня та технологій об'єктно-орієнтованого програмування для реалізації прикладних задач.

Володіти мовами системного програмування та методами розробки програм, що взаємодіють з компонентами комп'ютерних систем, демонструвати знання мережних технологій, архітектури комп'ютерних мереж і практичні навички технології адміністрування комп'ютерних мереж та їх програмного забезпечення.

### 4. Обсяг курсу

Вид заняття	Загальна к-сть годин
лекції	34/16*
лабораторні заняття	0/0*
практичні заняття	36/18*
самостійна робота (реферат, РГР, КР, КП, тощо)	82/116*

Символом «\*» позначена відповідна кількість годин для заочної ф.н.

### 5. Пререквізити

Дисципліна «Захист інформації в комп'ютерних системах» є базовою для опанування технологіями проектування комп'ютерних систем.

В результаті вивчення дисципліни «Захист інформації в комп'ютерних системах» студенти здобувають навички кваліфікованих спеціалістів з комп'ютерних систем та їх захисту.

### 6. Система оцінювання та вимоги

<b>Загальна система оцінювання курсу</b>	Підсумкова оцінка з дисципліни є сумою оцінок з відповідною вагою за кожен з таких видів робіт: активна робота на лабораторних та практичних заняттях, тести та підсумковий контроль (екзамен). Підсумкова оцінка визначається відповідно до поданої нижче таблиці оцінювання за різними шкалами (100-бальна, ECTS, національна).
--	---

<b>Розрахункова графічна-робота</b>	В рамках курсу не передбачено виконання РГР.
<b>Лабораторні та практичні роботи</b>	<b>Критерії оцінювання лабораторних та практичних робіт:</b> 1. Підготовленість до лабораторних/практичних занять 2. Самостійність виконання лабораторних/практичних робіт. 3. Повнота виконання завдань 4. Своєчасність виконання та захисту лабораторних/практичних робіт Максимальний бал за кожну лабораторну/практичну роботу – 5 балів
<b>Тест</b>	Проміжний тест проводиться у кожному модулі з курсу та оцінюється максимально в 10 балів.
<b>Іспит</b>	Іспит проводиться в кінці курсу, включає два теоретичних питання і одне практичне завдання. Максимально оцінюється в 40 балів.
<b>Умови допуску до підсумкового контролю</b>	Позитивна оцінка за всіма обов'язковими видами робіт (лабораторні та практичні роботи)

## 7. Політики курсу

*Політика щодо академічної доброчесності:* списування під час тесту, іспиту заборонені.

Жодні форми порушення академічної доброчесності не толеруються. У випадку таких подій – реагування відповідно до Методичних рекомендацій для закладів вищої освіти з підтримки принципів академічної доброчесності.

*Правила перезарахування кредитів у випадку мобільності, правила перескладання або відпрацювання пропущених занять тощо:* відбувається згідно з Положення про організацію освітнього процесу у Таврійському національному університет ім. В.І. Вернадського.

*Політика щодо дедлайнів та перескладання:* роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (до -50% від можливої максимальної кількості балів за вид діяльності).

*Перескладання тесту* відбувається за наявності поважних причин (наприклад, лікарняний).

*Політика щодо відвідування:* відвідування занять є обов'язковим компонентом. За об'єктивних причин (наприклад, хвороба, працевлаштування, міжнародне стажування) навчання може відбуватись в онлайн-формі за погодженням.

## 8. Рекомендована література

### Основна

1. Величко В.В. Передача даних в сетях мобільної зв'язи третього покоління / В.В.Величко. – М.: Радио и связь, Горячая линия-Телеком, 2005. – 332с.
2. Горбенко І.Д., Горбенко Ю.І., Прикладна криптологія. Теорія. Практика. Застосування: монографія. – Х.:Видавництво «Форт», 2012. – 870с.
3. Захист інформації в комп'ютерних системах та мережах : навч. посіб. / С.Г.Семенов, А.О.Подорожняк, О.І.Баленко, С.Ю.Гавриленко – Х.: НТУ «ХПІ», 2014.– 251с.
4. Єжова Л.Ф. Алгоритмізація і програмування процедур обробки інформації. – К.: КНЕУ, 2000. – 152с.
5. Хорошко В.А., Чекатков А.А. Захист інформації в комп'ютерних системах та мережах. Підручник. К.: ВНУ, 2005.

### Додаткова

6. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. – К.: Укр. НДІССІ, 1997. – 11с.
7. Гуржій А.М., Коряк С.Ф., Самсонов В.В., Склярів О.Я. Контроль та керування корпоративними комп'ютерними мережами: Інструментальні засоби та технології: Навч. посібник. – Харків: СМІТ, 2004 – 544с.
8. Єжова Л.Ф. Алгоритмізація і програмування процедур обробки інформації. – К.: КНЕУ, 2000. – 152с.
9. Жураковський Ю.П., Полтораки В.П. Теорія інформації та кодування: Підручник. – Київ: Вищ. шк., 2001. – 255с.
10. Новиков О.М., Грайворонський М.В., Основи захисту інформації в автоматизованих системах. Навч. пос. – К.: Академія, 2003.

### Інформаційні ресурси

Система дистанційного навчання GOOGLE CLASSROOM Курс: Захист інформації в комп'ютерних системах. [Електронний ресурс]. – Режим доступу: [Захист інформації в комп'ютерних системах Денне 4 курс, КІ, КН \(google.com\)](#)