ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету
інформаційних технологій
_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ
05 09 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Безпека та захист інформаційних систем і технологій

Галузь знань – 12 Інформаційні технології
Спеціальність – F6 Інформаційні системи і технології
Рівень вищої освіти –Другий (магістерський)
Освітньо-професійна програма – Інформаційні системи і технології
Обсяг дисципліни – 5 кредитів ЄКТС, ***Шифр дисципліни*** – ОФП.02
Мова навчання – українська
Статус дисципліни: обов'язкова, дисципліна фахової підготовки
Факультет – Інформаційних технологій
Кафедра – Комп'ютерної інженерії та інформаційних систем

Форма здобуття освіти	Курс	Семестр	Загальний обсяг		Кількість годин						Курсовий проєкт	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття					Самостійна робота, у т.ч. ІРС			Залік	Іспит
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття					
Д	1	1	5	150	50	16	34			100				+
Разом ДФН			**5**	**150**	**50**	**16**	**34**			**100**				**1**

Робоча програма складена на основі освітньо-наукової програми «Інформаційні системи і технології» за спеціальністю F6 Інформаційні системи і технології

Робоча програма складена _____ д-р. філософії Богдан САВЕНКО
Підпис автора(ів) Науковий ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

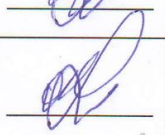
Схвалена на засіданні кафедри комп'ютерної інженерії та інформаційних систем
Протокол № 1 від 18 08 2025 р.
Зав. кафедри комп'ютерної інженерії та інформаційних систем _____ Ольга ПАВЛОВА
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена Вченою радою факультету інформаційних технологій
Протокол № 1 від 28 09 2025 р.

Голова вченої ради факультету _____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2025

ЛИСТ ПОГОДЖЕННЯ

Посада	Назва кафедри	Підпис	Ініціали, прізвище
Завідувач кафедри, д-р. філософії, доц.	Комп'ютерної інженерії та інформаційних систем		Ольга ПАВЛОВА
Гарант освітньо-професійної програми, д-р. філософії, доц.	Комп'ютерної інженерії та інформаційних систем		Ольга ПАВЛОВА

3. Пояснювальна записка

Дисципліна «***Безпека та захист інформаційних систем і технологій***» є однією із дисциплін фахової підготовки для здобувачів другого (магістерського) рівня вищої освіти, очної (денної) (далі – денної) форми здобуття вищої освіти, які навчаються за освітньо-професійною програмою «Інформаційні системи і технології» в межах спеціальності F6 Інформаційні системи і технології.

Пререквізити – вихідна.

Кореквізити – ІТ-інфраструктури (ОФП.03); технології проєктування інформаційних систем (ОФП.04); управління ІТ-проєктами (ОФП.05); кваліфікаційна робота (ОФП.07).

Відповідно до освітньої програми дисципліна сприяє забезпеченню:

***компетентностей*:** здатність розв'язувати задачі дослідницького та інноваційного характеру у сфері інформаційних систем та технологій (ІК); здатність до абстрактного мислення, аналізу та синтезу (ЗК01); здатність оцінювати та забезпечувати якість виконуваних робіт (ЗК05); здатність розробляти та застосувати ІСТ, необхідні для розв'язання стратегічних і поточних задач (ФК01); здатність управляти інформаційними ризиками на основі концепції інформаційної безпеки (ФК06); Здатність прогнозувати та оцінювати якість, надійність, живучість та безпеку інформаційних систем і технологій (УК02).

***програмних результатів навчання*:** відшуковувати необхідну інформацію в науковій і технічній літературі, базах даних, інших джерелах, аналізувати та оцінювати цю інформацію (ПРН01); вільно спілкуватись державною та іноземною мовами в науковій, виробничій та соціально-суспільній сферах діяльності (ПРН02); забезпечувати якісний кіберзахист ІСТ, планувати, організовувати, впроваджувати та контролювати функціонування систем захисту інформації (ПРН10); прогнозувати, оцінювати та забезпечувати якість, надійність, живучість та безпеку ІСТ (ПРН14).

***Мета дисципліни*:** надати студентам знання про організацію захисту інформації та безпеки інформаційних систем і технологій, а також про проєктування систем виявлення вторгнень і їх елементів.

Предмет дисципліни. Поняття захисту інформації та безпеки інформаційних систем та технологій. Системи виявлення вторгнень. Методи та технології виявлення комп'ютерних атак. Математичні аспекти безпеки та захисту комп'ютерних систем.

Завдання дисципліни: 1) формування компетентностей, необхідних для абстрактного мислення, аналізу та синтезу на відповідних рівнях забезпечення кіберзахисту в інформаційних системах та технологіях, розроблення систем захисту інформації та їх компонентів; 2) розвиток у студентів розуміння процесів, які протікають в комп'ютерних системах і мережах, з метою забезпечення безпеки та захисту інформації в них; 3) надання знань, необхідних для подальшого вивчення спеціальних дисциплін та для практичної інженерної діяльності; 4) вироблення у студентів вміння використовувати набуті знання при розробці програмних засобів спеціалізованого призначення.

Результати навчання. Після вивчення дисципліни студент повинен: досконало володіти професійною термінологією та основними поняттями об'єкту, предмету, задач, проблематики дисципліни та її основних розділів, знати понятійний апарат предметної області з інформаційної безпеки, з організації кіберзахисту в інформаційних системах і технологіях, методи проєктування програмних систем виявлення зловмисного програмного забезпечення і комп'ютерних атак; вміти використовувати методи фундаментальних і прикладних дисциплін при проєктуванні та розробленні програмних систем захисту інформації в комп'ютерних системах та мережах, виявлення несанкціонованих вторгнень та аномалій, проявів зловмисного програмного забезпечення, кібер-загроз та кібер-атак; бути здатним розв'язувати задачі із забезпечення безпеки та захисту інформаційних систем і технологій, проєктувати та створювати програмні системи захисту інформації та їх компоненти.

4. Структура залікових кредитів дисципліни

Назва теми	Кількість годин, відведених на:			
	лекції	лабораторні роботи	практичні роботи	самостійну роботу
Тема 1. Вступ. Основні поняття захисту інформації та безпеки інформаційних систем і технологій.	2	8		12
Тема 2. Організація захисту інформаційних систем в IT-інфраструктурах. Методи та технології виявлення комп'ютерних атак.	10	16		72
Тема 3. Математичні аспекти безпеки та захисту інформаційних систем і технологій.	4	10		16
Разом за 1-ий семестр:	16	34		100

5. Програма навчальної дисципліни

5.1 Зміст лекційного курсу

Номер лекції	Перелік змістових модулів, тем лекцій, їх анотації	Кількість годин
1	Тема 1. Вступ. Основні поняття захисту інформації та безпеки інформаційних систем. *Лекція 1. Вступ до інформаційної та кібер- безпеки.* Завдання навчальної дисципліни. Основна тематика курсу. Структура курсу. Проблемні завдання курсу та предметної області. Основні поняття і терміни захисту інформації та безпеки комп'ютерних систем, кіберзахисту інформаційних систем і технологій. Поняття: інформаційна безпека, кібернетична безпека (кібербезпека), захист інформації. Властивості інформаційної безпеки. Принципи забезпечення інформаційної безпеки. Крите́рії оці́нки інформаці́йної безпе́ки. Методологічна база для визначення вимог захисту комп'ютерних систем від несанкціонованого доступу, створення захисних систем та оцінки ступеня захищеності. Чотири групи вимог захисту проти певних типів загроз. Стандарт ISO/IEC 15408 «Загальні критерії оцінки безпеки інформаційних технологій». Загрози безпеці інформації. Види захисту інформації. Руйнуючі програмні впливи. Причини трудомісткості рішення задачі забезпечення безпеки програмних систем. Зловмисне програмне забезпечення та комп'ютерні атаки. Методи захисту від руйнуючих програмних впливів та їх виявлення. Покоління антивірусних програм. Типова архітектура програмних засобів антивірусного захисту. Критерії ефективності програмних засобів антивірусного захисту. ROC-аналіз в задачах виявлення зловмисного програмного забезпечення та комп'ютерних атак. Недоліки існуючих засобів захисту та перспективні методи захисту від руйнуючих програмних впливів. **Літ.: [1]-[7]; [9]-[12]; [18].**	2
2	Тема 2. Організація захисту інформаційних систем в IT-інфраструктурах. Методи та технології виявлення комп'ютерних атак. *Лекція 2. Поняття про комп'ютерні атаки. Принципи побудови систем виявлення вторгнень.* Основні поняття і терміни з предметної області «комп'ютерні атаки». Міжмережні екрани (firewall), антивіруси, системи виявлення атак (СВА) (Intrusion Detection System, IDS), системи контролю цілісності, криптографічні засоби захисту. Типи атак. Моделі атак. Класифікація комп'ютерних атак. Основні типи аномалій в IP-мережах. Етапи реалізації атак. Основні механізми реалізації атак. Вивчення оточення. Ідентифікація топології мережі. Ідентифікація вузлів. Ідентифікація сервісів або сканування портів. Ідентифікація операційної системи. Визначення ролі вузла. Визначення вразливості вузла. Реалізація атак: проникнення, встановлення контролю. Цілі реалізації атак. Завершення атаки. Засоби досягнення мети атаки. Застосування	2

	технологій безпечного програмування. **Літ.: [6]- [7]; [9]- [15]; [18]; [24].** Основні поняття про системи виявлення та попередження вторгнень. Класифікація систем виявлення атак. Системи виявлення атак рівня мережі. Класифікація систем виявлення вторгнень. Характеристики систем виявлення вторнень. Системи контролю цілісності. Монітори реєстраційних файлів. Архітектура систем виявлення вторгнень. Основні елементи локальної та глобальної архітектур систем виявлення вторгнень. **Літ.: [6]-[18]; [24].**	
3	*Лекція 3. Технології побудови систем виявлення атак.* Основні поняття про системи виявлення атак і технології виявлення. Існуючі технології систем виявлення вторгнень. Методи, які використовують сигнатури вторгнень. Продукційні (експертні) системи виявлення вторгнень. Виявлення вторгнень, що базується на моделі. Аналіз переходу системи із стану в стан. Контроль натиснення клавіш. Концепція виявлення комп'ютерних загроз. Підвищення ефективності систем виявлення атак. Фазовий простір комп'ютерних атак. Характеристика напрямків і груп методів виявлення вторгнень. Типова архітектура системи виявлення атак. Групи методів з виявлення аномалій і зловживань: з контрольованим навчанням («навчання з учителем») і з неконтрольованим навчанням («навчання без учителя»). Некомерційні системи виявлення комп’ютерних атак. Аналіз мережного трафіку і контенту. Програми аналізу та моніторингу мережного трафіку. Отримання і підготовка вихідних даних для аналізу властивостей аномалій трафіку. Аналіз зразків трафіку. Траси і їх аналіз. Тестування програмного забезпечення. Мережні атаки Portsweep, Neptune, Nmap, Mailbomb, Smurf. Типи сканування портів. **Літ.: [6]-[19]; [24].**	2
4	*Лекція 4. Статистичні методи виявлення аномальної поведінки трафіку мережі.* Застосування статичних методів в системах виявлення вторгнень. Статистичні методи виявлення аномальної поведінки. Профіль типової поведінки об'єкту. Методи математичної статистики. Класифікація методів виявлення змін. Помилки першого і другого роду в оцінці ефективності алгоритмів виявлення. Рівень значущості і потужність критерію. Статистичні тести. Критерії відповідності та однорідності. Критерій хі-квадрат. Критерії згоди. Критерій Колмогорова-Смірнова. Критерії оцінювання однорідності Вілкоксона-Манна-Уїтні. Параметричний метод реєстрації змін. Контрольні карти. Контрольні карти Шухарта, CUSUM. Виявлення DDoS-атак із застосуванням алгоритму CUSUM. Розподілене вторгнення. Три основні групи методів виявлення DDoS-атак. Виявлення DDoS-атак на основі відповідності між з'єднаннями, що встановлюються і закриваються. Вибір параметрів алгоритму CUSUM. Моніторинг різних IP-адрес у вхідному трафіку. Непараметричні багатовимірні CUSUM тести для швидкого виявлення DoS-атак в комп'ютерних	2

	мережах. Непараметричний багатовимірний CUMSUM алгоритм. Непараметричні методи. Контрольні карти EWMA. Критерії аномальної поведінки та їх практичне застосування. Відсоткове відхилення. Ентропія. Методи описової статистики. Показник активності. Розподіл активності в записах аудиту. Вимірювання категорій. Порядкові виміру. Пошук і оцінка аномалій мережного трафіку на основі циклічного аналізу. Перевірка циклів з точки зору статистичної значущості. Комбінування і проектування циклів в майбутнє. Виявлення аномалій методом головних компонент. Сингулярний спектральний аналіз. Метод головних компонент і виявлення аномалій у великих розподілених системах. Переваги та недоліки статистичних методів. Проєктування систем виявлення вторгнень із застосуванням статистичних методів виявлення аномальної поведінки мережного трафіку. **Літ.: [6]-[19]; [24-26].**	
5	*Лекція* 5. *Виявлення аномальних викидів мережного трафіку методами кратномасштабного аналізу.* Застосування методів кратномасштабного аналізу в системах виявлення вторгнень. Основи теорії вейвлетів. Неперервне вейвлет-перетворення. Дискретне вейвлет-перетворення. Алгоритм Малла. Аналіз методів виявлення аномалій мережного трафіку на основі вейвлет. Алгоритм виявлення аномалій методом дискретного вейвлет-перетворення. Алгоритм виявлення аномалій за критерієм Фішера для викидів дисперсій. Алгоритм виявлення аномалій на основі критерію Кохрана–Кокса. Алгоритм виявлення аномалій за критерієм Фішера для викидів середніх значень. Вибір порогів виявлення. Дискретне вейвлет-пакетне перетворення. Виявлення DoS- і DDoS-атак методами мультифрактального аналізу. Фрактальні властивості телекомунікаційного трафіку. Виявлення DoS- і DDoS-атак методом мультифрактального аналізу. Проєктування систем виявлення вторгнень із застосуванням методів кратномасштабного аналізу для виявлення аномальних викидів мережного трафіку. **Літ.: [6]-[12]; [14, 26].**	2
6	*Лекція* 6. *Методи інтелектуального аналізу даних в системах виявлення вторгнень.* Використання методів інтелектуального аналізу даних при проєктуванні підсистем систем виявлення вторгень. Методи Data Mining. Метод опорних векторів. Виявлення аномалій трафіку із застосуванням нейронних мереж. Виявлення аномалій мережної активності із застосуванням апарату штучних нейронних мереж. Застосування нейронних мереж в задачах виявлення вторгнень. Архітектурні рішення СВВ. Результати експериментів. Методи штучного інтелекту в задачах забезпечення безпеки комп'ютерних мереж. Багатоагентні системи. Системи аналізу захищеності. Методи штучних імунних систем і нейронних мереж для виявлення комп'ютерних атак. Побудова штучної імунної системи для виявлення комп'ютерних атак. Метод функціонування імунних нейромережних детекторів. Алгоритм функціонування системи виявлення вторгнень на основі штучних імунних систем і	2

	нейронних мереж. Візуальний аналіз даних. Аналіз методів візуалізації. **Літ.: [3]-[16]; [20-26].** Тема 3. Математичні аспекти безпеки та захисту інформаційних систем.	
7	*Лекція 7. Формальні моделі комп'ютерних вірусів, моделі поширення вірусів в комп'ютерних мережах.* Визначення комп'ютерного вірусу на основі модельного підходу. Моделі Ф. Коена. Модель Л. Адлемана. «Французька» модель. Інші формальні моделі. Модель китайських авторів Z. Zuo і M. Zhou. Векторна модель Д. Зегжди. Моделі на основі абстрактних «обчислювачів». «Екзотичні» віруси. Міфічні віруси. Batch-віруси. Віруси в початкових текстах. Графічні віруси. Віруси в інших операційних системах. Віруси в UNIX-подібних системах. Віруси для мобільних телефонів. Інша вірусна «екзотика». Поширення вірусів. Епідемії мережних worm-вірусів. Проста SI-модель експоненціального розмноження. SI-модель розмноження в умовах обмеженості ресурсів. SIS-модель примітивного протидії. SIR-модель кваліфікованої боротьби. Інші моделі епідемій. Моделювання заходів пасивної протидії. Моделювання «контр worm-вірусу». Епідемії поштових worm-вірусів, файлових і завантажувальних вірусів. Епідемії мобільних worm-вірусів. **Літ.: [9]-[10]; [13]; [20-26].**	2
8	*Лекція 8. Методи забезпечення кіберзахисту інформаційних систем і технологій від різних типів комп'ютерних вірусів.* Принципи та технології побудови і організації захисту та безпеки корпоративних мереж. Ризики інформаційної безпеки та їх оцінювання. Технології забезпечення безпеки мережної IT-інфраструктури. Надмірності в інформаційних технологіях та їх використання при створенні ІС стійких до зловмисних проявів. Виявлення комп'ютерних вірусів. Аналіз непрямих ознак. Прості сигнатури. Контрольні суми. Питання ефективності. Вибір файлових позицій. Фільтр Блума. Метод половинного ділення. Розбиття на сторінки. Використання сигнатур для детектування поліморфних вірусів. Апаратне трасування. Емуляція програм. Протидія емуляції. «Глибина» трасування і емуляції. Аналіз поліморфних вірусів і їх класифікація. Метаморфні віруси і їх детектування. Етап «виділення та збору характеристик». Етап «обробки і аналізу». Аналіз статистичних закономірностей. Евристичні методи детектування вірусів. Виділення характерних ознак. Логічні методи. Синтаксичні методи. Методи на основі формули Байеса. Методи, які використовують штучні нейронні мережі. Концепція сучасного антивірусного детектора. Боротьба з вірусами без використання антивірусів. Файлові «ревізори». Політики розмежування доступу. Криптографічні методи. Гарвардська архітектура ЕОМ. Перспективи розвитку і використання комп'ютерних вірусів. Віруси як «кіберзброя». Корисні застосування вірусів. Засоби і методи захисту від програмних закладок. Систем захисту інформації з використанням	2

	«приманок» (honeypots, honeynet). **Літ.: [6]-[12]; [18-26].**	
	Разом за 1-ий семестр:	16

5.2 Зміст лабораторних занять

№ п/п	Тема лабораторного заняття	Кількість годин
1	*Лабораторна робота 1. Системи приманок (honeypot)*	4
2*	*Лабораторна робота 2. Контроль доступу та автентифікація*	4
3	*Лабораторна робота 3. Безпека вебзастосунків, виявлення та усунення вебвразливостей*	4
4	*Лабораторна робота 4. Системи виявлення вторгнень (IDS/IPS) **	4
5	*Лабораторна робота 5. Шифрування мережевого трафіку*	4
6	*Лабораторна робота 6. Стеганографія та приховані канали*	4
7	*Лабораторна робота 7. Атаки на бездротові мережі*	4
8	*Лабораторна робота 8. Відновлення даних*	4
9	*Залікове заняття.*	2
	Разом:	**34**

Примітка: * Лабораторна робота може бути зарахована за наявності сертифікатів з проходження курсів (Cisco Networking Academy, https://www.netacad.com/ru/courses/cybersecurity/network-security та ін.).

5.3 Зміст самостійної (у т.ч. індивідуальної) роботи здобувача вищої освіти

Обсяг самостійної роботи з дисципліни в першому семестрі становить 100 годин. Він включає опрацювання лекційного матеріалу, підготовку до виконання лабораторних робіт і їх захисту, підготовку до поточного контролю.

Керівництво самостійною роботою здійснює викладач згідно з розкладом консультацій в позаурочний час.

Номер тижня	Вид самостійної роботи	К-ть годин
1	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №1. Самостійна робота над розробкою програми до лабораторної роботи №1.	6
2	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №1.	6
3	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №2. Самостійна робота над розробкою програми до лабораторної роботи №2.	6
4	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №2.	6
5	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №3. Самостійна робота над розробкою програми до лабораторної роботи №3. Самостійна робота з виконання індивідуального домашнього завдання.	6
6	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №3. Самостійне опрацювання теоретичного матеріалу. Самостійна робота з виконання індивідуального домашнього завдання.	6
7	Опрацювання лекційного матеріалу. Підготовка до лабораторної	6

	роботи №4. Самостійна робота над розробкою програми до лабораторної роботи №4. Самостійна робота з виконання індивідуального домашнього завдання.	
8	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №4. Самостійна робота з виконання індивідуального домашнього завдання.	6
9	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №5. Самостійна робота над розробкою програми до лабораторної роботи №5. Самостійна робота з виконання індивідуального домашнього завдання.	6
10	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №5. Самостійне опрацювання теоретичного матеріалу. Самостійна робота з виконання індивідуального домашнього завдання.	6
11	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №6. Самостійна робота над розробкою програми до лабораторної роботи №6. Самостійна робота з виконання індивідуального домашнього завдання.	6
12	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №6. Самостійне опрацювання теоретичного матеріалу. Самостійна робота з виконання індивідуального домашнього завдання.	6
13	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №7. Самостійна робота над розробкою програми до лабораторної роботи №7. Підготовка до захисту індивідуального домашнього завдання. Самостійна робота з виконання індивідуального домашнього завдання.	6
14	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №7. Самостійне опрацювання теоретичного матеріалу. Самостійна робота з виконання індивідуального домашнього завдання. Підготовка до тестування.	6
15	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №8. Самостійна робота над розробкою програми до лабораторної роботи №8.	6
16	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №8.	5
17	Самостійне опрацювання теоретичного матеріалу.	5
	Разом за 3-ий семестр:	100

6. Технології та методи навчання

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних технологій та методів навчання, зокрема: лекції (з використанням методів візуалізації, проблемного й інтерактивного навчання); лабораторні заняття (з використанням інструктування, демонстрування, розв'язування типових і прикладних задач, ситуаційних завдань, елементів дискусії тощо); самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання лабораторних робіт, поточного та підсумкового контролю, виконання індивідуальних та домашніх завдань), з використанням інформаційно-комп'ютерних технологій.

7. Методи контролю

Поточний контроль здійснюється під час аудиторних лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочою програмою і графіком

освітнього процесу, в т.ч. з використанням Модульного середовища для навчання. При цьому використовуються такі методи поточного контролю:

– тестовий контроль засвоєння теоретичного та практичного матеріалу;

– оцінювання результатів виконання індивідуального домашнього завдання;

– оцінювання лабораторних робіт (усне опитування перед допуском до лабораторного заняття; оцінювання результатів захисту лабораторних робіт).

При виведенні підсумкової семестрової оцінки враховуються результати як поточного контролю, так і підсумкового контролю, який проводиться з усього матеріалу дисципліни за білетами, попередньо розробленими і затвердженими на засіданні кафедри. Здобувач вищої освіти, який набрав з будь-якого виду навчальної роботи, суму балів нижчу за 60 відсотків від максимального балу, ***не допускається*** до семестрового контролю, поки не виконає обсяг роботи, передбачений Робочою програмою. Здобувач вищої освіти, який набрав позитивний середньозважений бал (60 відсотків і більше від максимального балу) з усіх видів поточного контролю і не склав іспит, вважається таким, який ***має*** академічну заборгованість. Ліквідація академічної заборгованості із семестрового контролю здійснюється у період екзаменаційної сесії або за графіком, встановленим деканатом відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ».

8. Політика дисципліни

Політика навчальної дисципліни загалом визначається системою вимог до здобувача вищої освіти, що передбачені чинними положеннями Університету про організацію і навчально-методичне забезпечення освітнього процесу. Зокрема, проходження інструктажу з техніки безпеки; відвідування занять з дисципліни є обов'язковим. За об'єктивних причин (підтверджених документально) теоретичне навчання за погодженням із лектором може відбуватись в он-лайн режимі. Успішне опанування дисципліни і формування фахових компетентностей і програмних результатів навчання передбачає необхідність підготовки до лабораторних занять (вивчення теоретичного матеріалу з теми роботи, попередню підготовку протоколу роботи, підготовку до усного опитування для допуску до заняття (наведені у Методичних рекомендаціях до лабораторних занять)), активно працювати на занятті, якісно підготувати звіт, захистити результати виконаної роботи, брати участь у дискусіях щодо прийнятих конструктивних рішень при виконанні здобувачами лабораторних робіт тощо.

Здобувачі вищої освіти мають дотримуватися встановлених термінів виконання всіх видів навчальної роботи відповідно до робочої програми навчальної дисципліни. Пропущене лабораторне заняття студент зобов'язаний відпрацювати у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за результатами опитування під час лабораторних занять, тестування й виконання індивідуального домашнього завдання. Виконання індивідуального завдання завершується його здачею на перевірку у терміни, встановлені графіком самостійної роботи.

Здобувач вищої освіти, виконуючи самостійну роботу або індивідуальну роботу з дисципліни, має дотримуватися політики доброчесності (заборонені списування, плагіат (в т.ч. із використанням мобільних девайсів)). У разі виявлення порушення політики академічної доброчесності в будь-яких видах навчальної роботи здобувач вищої освіти отримує незадовільну оцінку і має повторно виконати завдання з відповідної теми (виду роботи), що передбачені робочою програмою. Будь-які форми порушення академічної доброчесності ***не допускаються.***

У межах вивчення навчальної дисципліни здобувачам вищої освіти передбачено визнання і зарахування результатів навчання, набутих шляхом неформальної освіти, що розміщені на доступних платформах (Cisco Networking Academy,

https://www.netacad.com/ru/courses/cybersecurity/network-security), які сприяють формування компетентностей і поглибленню результатів навчання, визначених робочою програмою дисципліни, або забезпечують вивчення відповідної теми та/або виду робіт з програми навчальної дисципліни (детальніше у Положенні про порядок визнання та зарахування результатів навчання здобувачів вищої освіти у ХНУ).

9. Оцінювання результатів навчання студентів у семестрі

Оцінювання академічних досягнень здобувача вищої освіти здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». При поточному оцінюванні виконаної здобувачем роботи з кожної структурної одиниці і отриманих ним результатів викладач виставляє йому певну кількість балів із встановлених Робочою програмою для цього виду роботи. При цьому кожна структурна одиниця навчальної роботи може бути зарахована, якщо здобувач набрав не менше 60 відсотків (мінімальний рівень для позитивної оцінки) від максимально можливої суми балів, призначеної структурній одиниці.

При оцінюванні результатів навчання здобувачів вищої освіти з будь-якого виду навчальної роботи (структурної одиниці) рекомендується використовувати наведені нижче узагальнені критерії:

Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти

Оцінка та рівень досягнення здобувачем запланованих ПРН та сформованих компетентностей	**Узагальнений зміст критерія оцінювання**
Відмінно (високий)	Здобувач вищої освіти глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов’язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає логічний виклад відповіді мовою викладання (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними приладами та інструментами, прикладними програмами. Здобувач не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки, демонструє практичні навички з вирішення фахових завдань. При відповіді допустив дві–три несуттєві ***похибки***.
Добре (середній)	Здобувач вищої освіти виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання правил, закономірностей тощо. Відповідь здобувача вищої освіти будується на основі самостійного мислення. Здобувач вищої освіти у відповіді допустив дві–три ***несуттєві помилки***.
Задовільно (достатній)	Здобувач вищої освіти виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь здобувача вищої освіти будується на рівні репродуктивного мислення, здобувач вищої освіти має слабкі знання структури навчальної дисципліни, допускає неточності і ***суттєві помилки***

	у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно (недостатній)	Здобувач вищої освіти виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка «незадовільно» виставляється здобувачеві вищої освіти, який не може продовжити навчання без додаткової роботи з вивчення навчальної дисципліни.

Структурування дисципліни за видами навчальної роботи і оцінювання результатів навчання студентів денної форми здобуття освіти у семестрі

Аудиторна робота								Контрольні заходи	Самостійна робота	Семестровий контроль	Разом
Перший семестр											
Лабораторні заняття								Тестовий контроль:	ІДЗ	Іспит	Сума балів
1	2	3	4	5	6	7	8	Т 1-2			
Кількість балів за вид навчальної роботи (мінімум-максимум)											
3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5	6-10	6-10	24-40	
24-40								**6-10**	**6-10**	**24-40**	**60-100***

Примітки: *За набрану з будь-якого виду навчальної роботи з дисципліни кількість балів, нижче встановленого мінімуму, здобувач отримує незадовільну оцінку і має її перездати у встановлений викладачем (деканом) термін. Інституційна оцінка встановлюється відповідно до таблиці «**Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС»;**

Т – тема дисципліни.

Оцінювання результатів захисту лабораторної роботи.

Виконана й оформлена відповідно до встановлених Методичними рекомендаціями вимог лабораторна робота комплексно оцінюється викладачем при її захисті з урахуванням таких критеріїв: самостійність та правильність виконання; повнота відповіді та знання методики дотримання вимог при оформленні.

Результат виконання і захисту здобувачем вищої освіти кожної лабораторної роботи оцінюється відповідно до таблиці Критеріїв оцінювання навчальних досягнень здобувача вищої освіти.

У випадку виявлення здобувачем рівня знань, нижчого ніж 60 відсотків від максимального балу, встановленого Робочою програмою для кожної структурної одиниці, лабораторна робота йому ***не зараховується*** і для її захисту він має детальніше опрацювати матеріал з теми роботи, методику її виконання, виправити грубі помилки та повторно вийти на її захист у призначений для цього викладачем час.

Оцінювання результатів тестового контролю

Кожний з тестів, передбачених Робочою програмою, складається із 25 тестових завдань, кожне з яких є рівнозначним.

Відповідно до таблиці структурування видів робіт за тестовий контроль здобувач залежно від кількості правильних відповідей може отримати від 6 до 10 балів.

Розподіл балів в залежності від наданих правильних відповідей на тестові завдання

Кількість правильних відповідей	1-13	14-16	17-18	19-20	21-22	23-25
Відсоток правильних відповідей	0-59	60-65	66-72	73-82	83-89	90-100
Кількість балів	-	6	7	8	9	10

На тестування відводиться 40 хвилин. Студент проходить тестування в он-лайн режимі у Модульному середовищі для навчання. Також, студент може проходити тестування письмово, записуючи правильні відповіді у талоні відповідей. При отриманні негативної оцінки тест слід перездати до терміну ***наступного*** контролю.

Оцінювання результатів виконання індивідуального домашнього завдання (ІДЗ).

Виконане та оформлене відповідно до вимог, визначених Методичними рекомендаціями, індивідуальне домашнє завдання (ІДЗ) комплексно оцінюється викладачем з урахуванням таких критеріїв: самостійність виконання; правильність розв'язання поставлених задач; обґрунтованість вибору методів розв'язання; повнота пояснень та аргументованість відповідей; якість оформлення та дотримання вимог до структури і змісту роботи.

Результат виконання здобувачем вищої освіти кожного ІДЗ оцінюється відповідно до таблиці **Критеріїв оцінювання навчальних досягнень здобувача вищої освіти** з урахуванням рівня досягнення запланованих програмних результатів навчання та сформованих компетентностей. За підсумками захисту присвоюється відповідна сума балів (мінімальний позитивний бал – 6 бали, максимальний – 10 балів).

У разі, якщо здобувач вищої освіти виявив рівень знань і виконання ІДЗ, що нижчий ніж 60 відсотків від максимальної кількості балів, встановленої Робочою програмою для цієї структурної одиниці, завдання не зараховується. У такому випадку студент має повторно опрацювати зміст завдання, усунути помилки та здати на перевірку доопрацьоване ІДЗ у терміни, погоджені з викладачем.

Оцінювання результатів підсумкового семестрового контролю (іспит)

Освітня програма передбачає підсумковий семестровий контроль з дисципліни у формі іспиту, завданням якого є системне й об'єктивне оцінювання як теоретичної, так і практичної підготовки здобувача з навчальної дисципліни. Складання іспиту відбувається за попередньо розробленими і затвердженими на засіданні кафедри білетами. Відповідно до цього в екзаменаційному білеті пропонується поєднання питань як теоретичного (в т.ч. у тестовій формі), так і практичного характеру.

Таблиця – Оцінювання результатів підсумкового семестрового контролю здобувачів денної форми навчання (40 балів для підсумкового контролю)

Види завдань	**Для кожного окремого виду завдань**		
	Мінімальний (достатній) бал (задовільно)	**Потенційні позитивні бали* (середній бал) (добре)**	**Максимальний (високий) бал (відмінно)**
Теоретичне питання № 1	3	4	5
Теоретичне питання № 2	3	4	5
Теоретичне питання № 3	3	4	5
Практичне завдання (5 задач по 3-5 балів)	15	20	25
Разом:	**24**	**32**	**40**

Примітка. ****Позитивний бал за іспит, відмінний від мінімального (24 бали) та максимального (40 балів), знаходиться в межах 25-39 балів та розраховується як сума балів за усі структурні елементи (завдання) іспиту.***

Для кожного окремого виду завдань підсумкового семестрового контролю застосовуються критерії оцінювання навчальних досягнень здобувача вищої освіти,

наведені вище (**Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти)**.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС визначається в автоматизованому режимі після внесення викладачем результатів оцінювання у балах з усіх видів навчальної роботи до електронного журналу. Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС наведені нижче у таблиці «Співвідношення».

Семестровий іспит виставляється, якщо загальна сума балів, яку набрав студент з дисципліни за результатами поточного контролю, знаходиться у межах від 60 до 100 балів. При цьому за інституційною шкалою ставиться оцінка «відмінно/добре/задовільно», а за шкалою ЄКТС – буквене позначення оцінки, що відповідає набраній студентом сумі балів відповідно до таблиці Співвідношення.

Таблиця – **Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС**

<table>
<tr><th rowspan="2">Оцінка ЄКТС</th><th rowspan="2">Рейтингова шкала балів</th><th colspan="2">Інституційна оцінка (рівень досягнення здобувачем вищої освіти запланованих результатів навчання з навчальної дисципліни)</th></tr>
<tr><th>Залік</th><th>Іспит/диференційований залік</th></tr>
<tr><td>A</td><td>90-100</td><td rowspan="5">Зараховано</td><td>Відмінно/Excellent – високий рівень досягнення запланованих результатів навчання з навчальної дисципліни, що свідчить про безумовну готовність здобувача до подальшого навчання та/або професійної діяльності за фахом</td></tr>
<tr><td>B</td><td>83-89</td><td rowspan="3">Добре/Good – середній (максимально достатній) рівень досягнення запланованих результатів навчання з навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом
Задовільно/Satisfactory – Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни</td></tr>
<tr><td>C</td><td>73-82</td></tr>
<tr><td>D</td><td>66-72</td></tr>
<tr><td>E</td><td>60-65</td></tr>
<tr><td>FX</td><td>40-59</td><td rowspan="2">Незараховано</td><td>Незадовільно/Fail – Низка запланованих результатів навчання з навчальної дисципліни відсутня. Рівень набутих результатів навчання є недостатнім для подальшого навчання та/або професійної діяльності за фахом</td></tr>
<tr><td>F</td><td>0-39</td><td>Незадовільно/Fail – Результати навчання відсутні</td></tr>
</table>

10. Питання для самоконтролю результатів навчання

1. Основні поняття і терміни захисту інформації та безпеки інформаційних систем та технологій. Поняття: інформаційна безпека, кібербезпека, захист інформації.
2. Властивості інформаційної безпеки. Принципи забезпечення інформаційної безпеки. Крите́рії оці́нки інформаці́йної безпе́ки.
3. Методологічна база для визначення вимог захисту інформаційних систем від несанкціонованого доступу, створення захисних систем та оцінки ступеня захищеності. Чотири групи вимог захисту проти певних типів загроз. Стандарт ISO/IEC 15408 «Загальні критерії оцінки безпеки інформаційних технологій».
4. Загрози безпеці інформації. Види захисту інформації. Руйнуючі програмні впливи. Причини трудомісткості рішення задачі забезпечення безпеки програмних систем. Зловмисне програмне забезпечення та комп'ютерні атаки.
5. Методи захисту від руйнуючих програмних впливів та їх виявлення. Покоління антивірусних програм. Типова архітектура програмних засобів антивірусного захисту.

Недоліки існуючих засобів захисту та перспективні методи захисту від руйнуючих програмних впливів.
6. Критерії ефективності програмних засобів антивірусного захисту. ROC-аналіз в задачах виявлення зловмисного програмного забезпечення та комп'ютерних атак.
7. Поняття про комп'ютерні атаки.
8. Міжмережні екрани (firewall), антивіруси, системи виявлення атак (СВА) (Intrusion Detection System, IDS), системи попередження атак, системи контролю цілісності, криптографічні засоби захисту.
9. Типи атак. Моделі атак. Класифікація комп'ютерних атак. Основні типи аномалій в IP-мережах. Етапи реалізації атак.
10. Основні механізми реалізації атак. Вивчення оточення. Ідентифікація топології мережі. Ідентифікація вузлів. Ідентифікація сервісів або сканування портів. Ідентифікація операційної системи. Визначення ролі вузла. Визначення вразливості вузла. Реалізація атак: проникнення, встановлення контролю. Цілі реалізації атак. Завершення атаки. Засоби досягнення мети атаки.
11. Застосування технологій безпечного програмування.
12. Принципи побудови систем виявлення вторгнень.
13. Основні поняття про системи виявлення вторгнень. Класифікація систем виявлення атак.
14. Системи виявлення атак рівня мережі. Класифікація систем виявлення вторгнень.
15. Характеристики систем виявлення вторгнень. Системи контролю цілісності. Монітори реєстраційних файлів.
16. Архітектура систем виявлення вторгнень. Основні елементи локальної та глобальної архітектур систем виявлення вторгнень.
17. Технології побудови систем виявлення атак.
18. Основні поняття про системи виявлення атак і технології виявлення. Існуючі технології систем виявлення вторгнень.
19. Методи, які використовують сигнатури вторгнень. Продукційні (експертні) системи виявлення вторгнень. Виявлення вторгнень, що базується на моделі. Аналіз переходу системи із стану в стан. Контроль натиснення клавіш.
20. Концепція виявлення комп'ютерних загроз. Підвищення ефективності систем виявлення атак.
21. Фазовий простір комп'ютерних атак.
22. Характеристика напрямків і груп методів виявлення вторгнень. Типова архітектура системи виявлення атак.
23. Групи методів з виявлення аномалій і зловживань: з контрольованим навчанням («навчання з учителем») і з неконтрольованим навчанням («навчання без учителя»).
24. Некомерційні системи виявлення комп'ютерних атак.
25. Аналіз мережного трафіку і контенту. Програми аналізу та моніторингу мережного трафіку. Отримання і підготовка вихідних даних для аналізу властивостей аномалій трафіку. Аналіз зразків трафіку. Траси і їх аналіз.
26. Тестування програмного забезпечення. Мережні атаки Portsweep, Neptune, Nmap, Mailbomb, Smurf. Типи сканування портів.
27. Застосування статичних методів в системах виявлення вторгнень. Статистичні методи виявлення аномальної поведінки. Профіль типової поведінки об'єкту.
28. Методи математичної статистики. Класифікація методів виявлення змін.
29. Помилки першого і другого роду в оцінці ефективності алгоритмів виявлення.
30. Рівень значущості і потужність критерію.
31. Статистичні тести. Критерії відповідності та однорідності. Критерій хі-квадрат. Критерії згоди.
32. Критерій Колмогорова-Смірнова.
33. Критерії оцінювання однорідності Вілкоксона-Манна-Уїтні.

34. Параметричний метод реєстрації змін.
35. Контрольні карти. Контрольні карти Шухарта, CUSUM.
36. Виявлення DDoS-атак із застосуванням алгоритму CUSUM.
37. Розподілене вторгнення. Три основні групи методів виявлення DDoS-атак. Виявлення DDoS-атак на основі відповідності між з'єднаннями, що встановлюються і закриваються. Вибір параметрів алгоритму CUSUM. Моніторинг різних IP-адрес у вхідному трафіку.
38. Непараметричні багатовимірні CUSUM тести для швидкого виявлення DoS-атак в комп'ютерних мережах. Непараметричний багатовимірний CUMSUM алгоритм.
39. Непараметричні методи. Контрольні карти EWMA.
40. Критерії аномальної поведінки та їх практичне застосування. Відсоткове відхилення. Ентропія. Методи описової статистики. Показник активності. Розподіл активності в записах аудиту. Вимірювання категорій. Порядкові виміру. Пошук і оцінка аномалій мережного трафіку на основі циклічного аналізу. Перевірка циклів з точки зору статистичної значущості. Комбінування і проектування циклів в майбутнє.
41. Виявлення аномалій методом головних компонент.
42. Сингулярний спектральний аналіз.
43. Метод головних компонент і виявлення аномалій у великих розподілених системах.
44. Переваги та недоліки статистичних методів.
45. Проєктування систем виявлення вторгнень із застосуванням статистичних методів виявлення аномальної поведінки мережного трафіку.
46. Застосування методів кратномасштабного аналізу в системах виявлення вторгнень.
47. Основи теорії вейвлетів. Неперервне вейвлет-перетворення. Дискретне вейвлет-перетворення. Алгоритм Малла.
48. Аналіз методів виявлення аномалій мережного трафіку на основі вейвлет.
49. Алгоритм виявлення аномалій методом дискретного вейвлет-перетворення.
50. Алгоритм виявлення аномалій за критерієм Фішера для викидів дисперсій.
51. Алгоритм виявлення аномалій на основі критерію Кохрана–Кокса.
52. Алгоритм виявлення аномалій за критерієм Фішера для викидів середніх значень. Вибір порогів виявлення.
53. Дискретне вейвлет-пакетне перетворення.
54. Виявлення DoS- і DDoS-атак методами мультифрактального аналізу. Фрактальні властивості телекомунікаційного трафіку.
55. Використання методів інтелектуального аналізу даних при проєктуванні підсистем систем виявлення вторгень. Методи Data Mining. Метод опорних векторів.
56. Виявлення аномалій трафіку із застосуванням нейронних мереж. Виявлення аномалій мережної активності із застосуванням апарату штучних нейронних мереж. Застосування нейронних мереж в задачах виявлення вторгнень. Архітектурні рішення СВВ. Результати експериментів.
57. Методи штучного інтелекту в задачах забезпечення безпеки комп'ютерних мереж.
58. Багатоагентні системи. Системи аналізу захищеності.
59. Методи штучних імунних систем і нейронних мереж для виявлення комп'ютерних атак. Побудова штучної імунної системи для виявлення комп'ютерних атак. Метод функціонування імунних нейромережних детекторів. Алгоритм функціонування системи виявлення вторгнень на основі штучних імунних систем і нейронних мереж.
60. Візуальний аналіз даних. Аналіз методів візуалізації.
61. Математичні аспекти безпеки та захисту інформаційних систем.
62. Формальні моделі комп’ютерних вірусів. Визначення комп’ютерного вірусу на основі модельного підходу. Моделі Ф. Коена. Модель Л. Адлемана. «Французька» модель. Інші формальні моделі. Модель китайських авторів Z. Zuo і M. Zhou. Векторна модель Д. Зегжди. Моделі на основі абстрактних «обчислювачів».
63. Моделі поширення вірусів в комп’ютерних мережах. Проста SI-модель експоненціального розмноження. SI-модель розмноження в умовах обмеженості ресурсів.

SIS-модель примітивного протидії. SIR-модель кваліфікованої боротьби. Інші моделі епідемій.
64. «Екзотичні» віруси. Міфічні віруси. Batch-віруси. Віруси в початкових текстах. Графічні віруси. Віруси в інших операційних системах. Віруси в UNIX-подібних системах. Віруси для мобільних телефонів. Інші типи вірусів.
65. Поширення вірусів. Епідемії мережних worm-вірусів Моделювання заходів пасивної протидії. Моделювання «контр worm-вірусу». Епідемії поштових worm-вірусів, файлових і завантажувальних вірусів. Епідемії мобільних worm-вірусів.
66. Методи забезпечення безпеки та захисту комп'ютерних систем від різних типів комп'ютерних вірусів.
67. Виявлення комп'ютерних вірусів. Аналіз непрямих ознак. Прості сигнатури. Контрольні суми. Питання ефективності. Вибір файлових позицій. Фільтр Блума. Метод половинного ділення. Розбиття на сторінки. Використання сигнатур для детектування поліморфних вірусів. Апаратне трасування. Емуляція програм. Протидія емуляції. «Глибина» трасування і емуляції.
68. Типи поліморфних вірусів та їх внутрішня будова.
69. Метаморфні віруси і їх детектування.
70. Етап «виділення та збору характеристик». Етап «обробки і аналізу». Аналіз статистичних закономірностей. Евристичні методи детектування вірусів. Виділення характерних ознак.
71. Логічні методи. Синтаксичні методи. Методи на основі формули Байеса. Методи, які використовують штучні нейронні мережі.
72. Концепція сучасного антивірусного детектора. Боротьба з вірусами без використання антивірусів. Файлові «ревізори».
73. Політики розмежування доступу. Криптографічні методи. Гарвардська архітектура ЕОМ. Перспективи розвитку і використання комп'ютерних вірусів. Віруси як «кіберзброя». Корисні застосування вірусів.
74. Засоби і методи захисту від програмних закладок. Проєктування систем захисту інформації з використанням «приманок» (honeypots, honeynet).
75. Принципи та технології побудови і організації захисту та безпеки корпоративних мереж.
75. Ризики інформаційної безпеки та їх оцінювання.
76. Технології забезпечення безпеки мережної IT-інфраструктури.
77. Надмірності в інформаційних технологіях та їх використання при створенні ІС стійких до зловмисних проявів.

11. Навчально-методичне забезпечення

Освітній процес з дисципліни повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою. Зокрема, викладачами кафедри підготовлені і видані такі роботи:
1. ***Безпека та захист інформаційних систем і технологій*** : лабораторний практикум з дисципліни для здобувачів другого (магістерського) рівня вищої освіти спеціальності F6 «Інформаційні системи та технології» / О. С. Савенко, А. О. Нічепорук, М. В. Капустян, Б. О. Савенко, А. І. Дрозд. Хмельницький : ХНУ, 2025. 70 с.

12. Матеріально-технічне та програмне забезпечення дисципліни (за потреби)

Інформаційна та комп'ютерна підтримка: ПК, планшет, смартфон або інший мобільний пристрій, проєктор. Програмне забезпечення: програми Microsoft Office або аналогічні, доступ до мережі Інтернет, робота з презентаціями.

13. Рекомендована література:

Основна

1. Стратегія кібербезпеки України: Затверджено Указом Президента України від 15.03.2016 р. № 96/2016 // Офіційний вісник України. – 2016. – № 23. – С. 69. – Ст. 899.
2. ЗАКОН УКРАЇНИ Про основні засади забезпечення кібербезпеки України (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) {Із змінами, внесеними згідно із Законом № 2469-VIII від 21.06.2018, ВВР, 2018, № 31, ст.241}
3. Міжнародний стандарт ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity: [Електронний ресурс]. – Режим доступу: https://webstore.iec.ch/preview/info_isoiec27032%7Bed1.0%7Den.pdf.
4. National Institute of Standards and Technology (NIST). (2010a). Guide to Aplying the Risk Management Framework to Federal Information Systems, NIST Special Publication 800-37.
5. National Institute of Standards and Technology (NIST). (2010b). Security and Privacy Controls for Federal Information Systems and Organizations, Building Effective Security Assessment Plans, NIST Special Publication 800-53A.
6. Богуш В.М., Довидьков О.А., Кривуца В. Г. Теоретичні основи захищених інформаційних технологій. Навч. посібник. – К.: ДУІКТ, 2010. – 454 с. ISBN 978-966-2970-49-4.
7. Лукова-Чуйко Н.В. Методологічні основи забезпечення функціональної стійкості розподілених інформаційних систем до кібернетичних загроз / Дис. на здобуття наук. ступеня докт. техн. наук за спеціальністю 05.13.06 інформаційні технології. - Київ. Державний університет телекомунікацій. – 2018.
8. S. Lysenko, O. Savenko, K. Bobrovnikova, A. Kryshchuk. Self-adaptive system for the corporate area network resilience in the presence of botnet cyberattacks / Communications in Computer and Information Science, 2018.- 860, - Pp. 385-401.
9. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник] / В.Л. Бурячок, С.В. Толюпа, В.В. Семко, Л.В. Бурячок, П.М. Складанний, Н.В. Лукова-Чуйко. –К.: ДУТ-КНУ, 2016. –178 с. ISBN 978–617–7092–78–9.
10. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В. Толюпа, А.О. Аносов, В.А. Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с. ISBN № 978–966–2970–81–4.
11. Основи криптографічного захисту інформації: підручник / Г.М. Гулак, В.А. Мухачов, В.О. Хорошко, Ю.Є. Яремчук / Вінниця: ВНТУ, 2011. – 199 с. ISBN 978-966-641-430-7.
12. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М. Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с. ISBN 978–617–7092–64–2.
13. Sergii Lysenko. Detection of the botnets' low-rate DDoS attacks based on self-similarity / Lysenko, S., Bobrovnikova, K., Matiukh, S., Hurman, I., Savenko, O. // International Journal of Electrical and Computer Engineering. – 2020. – Vol. 10., №4 – PP.-3651-3659, ISSN: 2088-8708.
14. Markowsky G. The technique for metamorphic viruses' detection based on its obfuscation features analysis / G. Markowsky, O. Savenko, S. Lysenko, A. Nicheporuk // CEUR-WS, ISSN: 1613–0073. – 2018. – Vol. 2104. – Pp. 680–687.
15. R. C. Joshi, A. Sardana. Honeypots A New Paradigm to Information Security. USA: Science Publishers. - 2011. - 339 p. ISBN 978-1-57808-708-2.
16. Савенко О.С. Теорія та практика створення розподілених систем виявлення зловмисного програмного забезпечення в локальних комп'ютерних мережах / Дис. на здобуття наук. ступеня докт. техн. наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти. – Львів. Національний університет «Львівська політехніка». – 2019.

Додаткова

17. Center for Strategic & International Studies (CSIS). (2012). Twenty Critical Scurity Controls for Effective Cyber Defense: Consensus Audit Guidelines. Retrieved from SANS.org website January 24, 2013 at http://www.sans.org/critical-security-controls/
18. McAfee, Inc. (2009). Virtual Criminology Report – Cybercrime: The Next Wave. Santa Clara, CA. Retrieved February 2, 2010 from the McAfee websitehttp://www.mcafee.com/us/research/criminology _ report/default.html
19. Carlin D. Dynamic Analysis of Malware Using Run-Time Opcodes/ D. Carlin, P. O'Kane, S.Sezer // Data Analytics and Decision Support for Cybersecurity. – 2017. – Pp. 99-125.
20. Kashtalian, A., Lysenko, S., Sachenko, A., Savenko, B., Savenko, O., & Nicheporuk, A. (2025). Evaluation criteria of centralization options in the architecture of multicomputer systems with traps and baits. *Radioelectronic and Computer Systems*, *2025*(1), 264-297. doi:https://doi.org/10.32620/reks.2025.1.18

21. Sochor T. Analysis of attackers against windows emulating honeypots in various types of networks and regions/ T. Sochor, M. Zuzcak, P. Bujok// 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN). – Vienna (Austria), July 5-8, 2016. – Pp. 863-868.
22. Дудикевич В. Б. Квінтесенція інформаційної безпеки кіберфізичної системи / В. Б. Дудикевич, Г. В. Микитин, А. І. Ребець // Вісник Національного університету «Львівська політехніка». Інформаційні системи та мережі. — Львів: Видавництво Львівської політехніки, 2018. – № 887. – С. 58–68.
24. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
25. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.
26. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
27. НД ТЗІ 2.5-008-02. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.
28. НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.
29. НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.
30. Kashtalian, A., Lysenko, S., Savenko, O., Nicheporuk, A., Sochor, T., & Avsiyevych, V. (2024). Multi-computer malware detection systems with metamorphic functionality. Radioelectronic and Computer Systems, 2024(1), 152-175. doi:https://doi.org/10.32620/reks.2024.1.13

14. Інформаційні ресурси

1. Модульне середовище для навчання. URL : **https://msn.khmnu.edu.ua/course/view.php?id=8787**
2. Електронна бібліотека ХНУ. URL: http://library.khmnu.edu.ua/
3. Інституційний репозитарій ХНУ. URL : https://elar.khmnu.edu.ua/home

Електронні ресурси:

1. AV-TEST | Antivirus & Security Software & AntiMalware Reviews. https://www.av-test.org/en/
2. Avast! [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: https://www.avast.com/index (Viewed on April 2, 2019). – Title from the screen.
3. AVG [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: http://www.avg.com (Viewed on April 2, 2019). – Title from the screen.

4. Avira [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: http://www.avira.com (Viewed on April 2, 2019). – Title from the screen.
5. ClamAV [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: https://www.clamav.net/ (Viewed on April 2, 2019). – Title from the screen.
6. DAMBALLA. Botnet communication topologies. Understanding the intricacies of botnet command-and-control [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: https://www.damballa.com/downloads/r_pubs /WP_Botnet_Communications_Primer.pdf (Viewed on April 2, 2019). – Title from the screen.
7. DAMBALLA. Botnet detection for communications service providers [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: https:// www.damballa.com/ downloads/r_pubs/WP_Botnet_Detection_for_CSPs. pdf (Viewed on April 2, 2019). – Title from the screen.
8. https://www.virusbulletin.com/
9. ESET Endpoint Security [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: http://www.eset.com/ (Viewed on April 2, 2019). – Title from the screen.
10. Symantec Endpoint Protection [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: https://www.anti-malware.ru/reviews/ Symantec_Endpoint_Protection (Viewed on April 2, 2019). – Title from the screen.

Анотація дисципліни

Безпека та захист інформаційних систем і технологій

Тип дисципліни	Обов'язкова
Рівень вищої освіти	Другий (магістерський)
Мова викладання	Українська
Семестр	3
Кількість встановлених кредитів ЄКТС	5,0
Форми навчання, для яких викладається дисципліна	Очна (денна)

Результати навчання:

Після вивчення дисципліни студент повинен: досконало володіти професійною термінологією та основними поняттями об'єкту, предмету, задач, проблематики дисципліни та її основних розділів, знати понятійний апарат предметної області з інформаційної безпеки, з організації кіберзахисту в інформаційних системах і технологіях, методи проєктування програмних систем виявлення зловмисного програмного забезпечення і комп'ютерних атак; вміти використовувати методи фундаментальних і прикладних дисциплін при проєктуванні та розробленні програмних систем захисту інформації в комп'ютерних системах та мережах, виявлення несанкціонованих вторгнень та аномалій, проявів зловмисного програмного забезпечення, кібер-загроз та кібер-атак; бути здатним розв'язувати задачі із забезпечення безпеки та захисту інформаційних систем і технологій, проєктувати та створювати програмні системи захисту інформації та їх компоненти.

Зміст навчальної дисципліни. Поняття інформаційної безпеки, кібербезпеки та захисту інформації. Стохастична комп'ютерна вірусологія. Тенденції розвитку загроз інформаційної безпеки. Класифікація атак. Організація заходів безпеки в комп'ютерних системах. Критерії ефективності антивірусних засобів. Принципи побудови систем виявлення вторгнень. Технології побудови систем виявлення атак. Перспективні методи протидії зловмисним програмам. Методи виявлення аномалій. Засоби і методи захисту від програмних закладок. Системи захисту інформації з використанням «приманок» (honeypots, honeynet). Методи інтелектуального аналізу даних в системах виявлення вторгнень. Технології безпечного програмування. Організація захисту інформаційних систем в IT-інфраструктурах. Математичні аспекти безпеки та захисту інформаційних систем і технологій. Принципи та технології побудови і організації захисту та безпеки корпоративних мереж. Ризики інформаційної безпеки та їх оцінювання. Технології забезпечення безпеки мережної IT-інфраструктури. Надмірності в інформаційних технологіях та їх використання при створенні ІС стійких до зловмисних проявів.

Пререквізити – вихідна.

Кореквізити – IT-інфраструктури (ОФП.03); технології проєктування інформаційних систем (ОФП.04); управління IT-проєктами (ОФП.05); кваліфікаційна робота (ОФП.07).

Відповідно до освітньої програми дисципліна сприяє забезпеченню:

Запланована навчальна діяльність: лекції - 16 год., лабораторні заняття – 34 год., самостійна робота - 100 год.; разом – 150 год.

Методи навчання: словесні, проблемного й інтерактивного навчання, інтерактивні, пояснювально-ілюстративні

Форми оцінювання результатів навчання: усне опитування; захисти лабораторних робіт; тестовий контроль; перевірка виконання індивідуального домашнього завдання

Вид семестрового контролю: іспит

Навчальні ресурси:

1. ЗАКОН УКРАЇНИ Про основні засади забезпечення кібербезпеки України (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) {Із змінами, внесеними згідно із Законом № 2469-VIII від 21.06.2018, ВВР, 2018, № 31, ст.241}
2. Міжнародний стандарт ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity: [Електронний ресурс]. – Режим доступу: https://webstore.iec.ch/preview/info_isoiec27032%7Bed1.0%7Den.pdf.
3. Богуш В.М., Довидьков О.А., Кривуца В. Г. Теоретичні основи захищених інформаційних технологій. Навч. посібник. – К.: ДУІКТ, 2010. – 454 с. ISBN 978-966-2970-49-4.
4. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник] / В.Л. Бурячок, С.В. Толюпа, В.В. Семко, Л.В. Бурячок, П.М. Складанний, Н.В. Лукова-Чуйко. –К.: ДУТ-КНУ, 2016. –178 с. ISBN 978–617–7092–78–9.
5. R. C. Joshi, A. Sardana. Honeypots A New Paradigm to Information Security. USA: Science Publishers. - 2011. - 339 p. ISBN 978-1-57808-708-2.
6. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.

Викладач: **д-ф. Б. Савенко**