ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан ФІТ _____
Тетяна ГОВОРУЩЕНКО
_5_ _____09_____ 2024 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Безпека та захист інформаційних систем і технологій

Галузь знань 12 Інформаційні технології
(шифр) (назва)
Спеціальність 126 Інформаційні системи та технології очна денна форма здобуття освіти
(шифр) (назва)
Освітня програма **Інформаційні системи та технології**
Шифр дисципліни ОПП.02
Статус дисципліни: обов'язкова, дисципліна професійної підготовки
(назва)
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

форма здобуття освіти	Курс	Семестр	Загальне навантаження		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, в т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття					Залік	Іспит
Д	1	1	5	150	51	17	34			99				+

Робоча програма складена на основі стандарту вищої освіти зі спеціальності 126 Інформаційні системи та технології, освітньо-професійної програми та навчального плану

Програма складена _____ _____Богдан САВЕНКО_____
Підпис Ім'я, прізвище викладача

Схвалена на засіданні кафедри комп'ютерної інженерії та інформаційних систем
Протокол № _2_ від _30_ ____08____2024 р.
Зав. кафедри комп'ютерної інженерії та інформаційних систем _____ Ірина ЗАСОРНОВА
Підпис Ім'я, прізвище

Робоча програма розглянута та схвалена Вченою радою факультету інформаційних технологій
Протокол № _1_ від _05_ ____09____2024 р.

Голова Вченої ради _____ _____Тетяна ГОВОРУЩЕНКО _____
Підпис Ім'я, прізвище

Хмельницький 2024

ВСТУП

Мета викладання дисципліни. Дисципліна є однією з фундаментальних дисциплін і тому займає провідне місце у підготовці магістрів.

Метою дисципліни є: 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.

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.

Пререквізити: іноземна мова за професійним спрямуванням, методологічні основи створення інформаційних систем і технологій; ***кореквізити***: технології проєктування інформаційних систем; ІТ-інфраструктури; науково-дослідна практика.

Завдання дисципліни. Надати студентам знання про організацію захисту інформації та безпеки інформаційних систем і технологій, а також про проєктування систем виявлення вторгнень і їх елементів.

Після вивчення дисципліни студент має досягти таких результатів навчання (сукупність знань, умінь, навичок, компетентностей):

знати: об'єкт, предмет, задачі, проблематику дисципліни та її основні розділи, понятійний апарат предметної області з інформаційної безпеки, 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.

Програмні компетентності:

Інтегральна - здатність розв'язувати задачі дослідницького та інноваційного характеру у сфері інформаційних систем та технологій.

ЗК01. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК05. Здатність оцінювати та забезпечувати якість виконуваних робіт.

ФК01. Здатність розробляти та застосувати ІСТ, необхідні для розв'язання стратегічних і поточних задач.

ФК06. Здатність управляти інформаційними ризиками на основі концепції інформаційної безпеки.

ФК08. Здатність виконувати захист ІСТ від зловмисного програмного забезпечення, кібер-загроз та кібер-атак.

ФК09. Здатність до забезпечення якості, надійності, живучості та безпеки ІСТ.

Програмні результати навчання:
ПРН01. Відшуковувати необхідну інформацію в науковій і технічній літературі, базах даних, інших джерелах, аналізувати та оцінювати цю інформацію.
ПРН02. Вільно спілкуватись державною та іноземною мовами в науковій, виробничій та соціально-суспільній сферах діяльності.
ПРН10. Забезпечувати якісний кіберзахист ІСТ, планувати, організовувати, впроваджувати та контролювати функціонування систем захисту інформації.
ПРН14. Вміти прогнозувати, оцінювати та забезпечувати якість, надійність, живучість та безпеку ІСТ.

Анотація дисципліни

Безпека та захист інформаційних систем і технологій

Тип дисципліни	Обов'язкова
Рівень вищої освіти	Другий (магістерський)
Мова викладання	Українська
Семестр	1
Кількість встановлених кредитів ЄКТС	5,0
Форми здобуття освіти	Очна денна

Результати навчання:

ПРН01. Відшуковувати необхідну інформацію в науковій і технічній літературі, базах даних, інших джерелах, аналізувати та оцінювати цю інформацію.

ПРН02. Вільно спілкуватись державною та іноземною мовами в науковій, виробничій та соціально-суспільній сферах діяльності.

ПРН10. Забезпечувати якісний кіберзахист ІСТ, планувати, організовувати, впроваджувати та контролювати функціонування систем захисту інформації.

ПРН14. Вміти прогнозувати, оцінювати та забезпечувати якість, надійність, живучість та безпеку ІСТ.

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 ІТ-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 ІТ-інфраструктури. Надмірності в інформаційних технологіях та їх використання при створенні ІС стійких до зловмисних проявів.

Пререквізити: іноземна мова за професійним спрямуванням, методологічні основи створення інформаційних систем і технологій; ***кореквізити***: технології проєктування інформаційних систем; ІТ-інфраструктури; науково-дослідна практика.

Запланована навчальна діяльність: лекції - 17 год., лабораторні заняття – 34 год., самостійна робота - 99 год.; разом – 150 год.

Методи навчання: словесні, проблемного навчання і візуалізації, інтерактивні, пояснювально-ілюстративні

Форми оцінювання результатів навчання: усне опитування, захисти лабораторних робіт

Вид семестрового контролю: іспит

Навчальні ресурси:

1. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів/ Козачок В.А., Гайдур Г.І., Гахов С.О., Хмелевський Р.М., Чумак Н.С. Київ: ДУТ ННІЗІ, 2020. 167 с.
2. Технології забезпечення безпеки мережевої інфраструктури/ В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. К.: КУБГ, 2019. 218 с.
3. Fundamentals of Information Systems Security/ Editors : David Kim, Michael G. Solomon. Burlington, Massachusetts: Jones & Bartlett Learning, 2018. 548 p.
4. Information Security. Foundations, technologies and applications/ Editors: Ali Ismail Awad, Michael Fairhurst. The Institution of Engineering and Technology, 2018. 418 p.
5. Браіловський М.М. Аналіз кіберзахищеності інформаційних систем: монографія. / Браіловський М. М., Зибін С. В., Кобозева А. А., Хорошко В. О., Хохлачова Ю. Є. – К.: ФОП Ямчинський О.В., 2021. – 360 с.
6. О. Г. Корченко, С. В. Казмірчук, Б. Б. Ахметов. Прикладні системи оцінювання ризиків інформаційної безпеки: монографія. Київ, ЦП «Компринт», 2017 – 435 с.
7. А. О. Корченко, В. М. Гребенюк. Технології виявлення та попередження кібератак. – К. : Вид. НАУ, 2021. – 109 с.
8. Методи та засоби захисту інформації [Навчальний посібник] / В. А. Лахно, Є. В. Васіліу, В. М. Гладких, В. М. Домрачев, Н. М. Сивкова. – К. : ЦП «Компринт» О.В., 2021. – 444 с.
9. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.

Викладач: **д. ф. Б. Савенко**

1. Структура залікових кредитів дисципліни

Назва теми	Кількість годин, відведених на:			
	лекції	лабораторні роботи	практичні роботи	самостійну роботу
Перший семестр				
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.	12	16		72
Тема 3. Математичні аспекти безпеки та захисту інформаційних систем і технологій.	4	10		15
Разом за 1-ий семестр:	18/16	34		99

2. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

2.1 Зміст лекційного курсу

Номер лекції	Перелік змістових модулів, тем лекцій, їх анотації	Кількість годин
	Перший семестр	
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.* 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].**	
3	*Лекція* 3. *Принципи побудови систем виявлення вторгнень*. 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].**	2
4	*Лекція 4. 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
5	*Лекція 5. 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	2

	різних IP-адрес у вхідному трафіку. Непараметричні багатовимірні CUSUM тести для швидкого виявлення DoS-атак в комп'ютерних 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].**	
6	*Лекція* 6. *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
7	*Лекція* 7. *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	2

	нейромережних детекторів. Алгоритм функціонування системи виявлення вторгнень на основі штучних імунних систем і нейронних мереж. Візуальний аналіз даних. Аналіз методів візуалізації. **Літ.: [3]-[16]; [20-26].** Тема 3. Математичні аспекти безпеки та захисту інформаційних систем.	
8	*Лекція 8. 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
9	*Лекція 9. 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».	2

	Корисні застосування вірусів. Засоби і методи захисту від програмних закладок. Систем захисту інформації з використанням «приманок» (honeypots, honeynet). **Літ.: [6]-[12]; [18-26].**	
	Разом за 1-ий семестр:	18/16

2.2 Зміст лабораторних занять

№ п/п	Тема лабораторного заняття	Кількість годин
Перший семестр		
1	*Лабораторна робота 1. Планування, оцінювання ризиків та організація кіберзахисту ІСТ.* Комплексні системи захисту інформації ІС. Оцінювання ризиків інформаційної та кібер- безпеки в корпоративних мережах та ІТ-інфраструктурах.	
2*	*Лабораторна робота 2. Налаштування та адміністрування систем захисту інформації в корпоративних мережах.* Організація кіберзахисту ІСТ в корпоративній мережі, ІТ-інфраструктурі. Аналіз, проєктування, планування, впровадження та контроль функціонування систем захисту інформації. Налаштування фаєрвола, створення правил, із використанням існуючих засобів. Налаштування систем виявлення та попередження вторгнень, антивірусних програм.	4
3	*Лабораторна робота 3. Розробка правил в YARA для виявлення зловмисного програмного забезпечення.* Забезпечення безпеки ІС на основі створення правил в YARA для виявлення зловмисного програмного забезпечення.	4
4	*Лабораторна робота 4. Ознайомлення з методами емуляції виконуваних файлів PE.* Використання модулів аналізу виконуваних файлів PE та емуляції виконання Cuckoo для YARA.	4
5	*Лабораторна робота 5. Розподілені системи виявлення та аналізу мережного трафіку.* Ознайомлення з мережними системами попередження та виявлення вторгнень. Реалізація аналізатора мережного трафіку з використанням розподіленої системи виявлення.	4
6	*Лабораторна робота 6. Розподілені системи виявлення зловмисного програмного забезпечення.* Забезпечення безпеки інформаційно-комунікаційної системи. Проєктування та реалізація розподіленої системи для виявлення зловмисного програмного забезпечення	4
7	*Лабораторна робота 7. Сигнатурний аналіз в розподіленій системі виявлення зловмисного програмного забезпечення.* Реалізація функції сигнатурного аналізу для виявлення зловмисного програмного забезпечення із використанням розподіленої системи.	4
8	Лабораторна робота 8. *Евристичний аналіз в розподіленій системі виявлення зловмисного програмного забезпечення.* Реалізація функції евристичного аналізу для виявлення зловмисного програмного забезпечення і з використанням розподіленої системи.	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.).

2.3 Зміст самостійної (індивідуальної) роботи

Обсяг самостійної роботи з дисципліни в 1 семестрі становить 99 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
	Перший семестр	
1	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №1. Самостійна робота над виконанням завдань 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 виконанням завдань 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 виконанням завдань до лабораторної роботи №3.	6
6	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №3. Самостійне опрацювання теоретичного матеріалу.	6
7	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №4. Самостійна робота над виконанням завдань до лабораторної роботи №4.	6
8	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №4.	6
9	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №5. Самостійна робота над виконанням завдань до лабораторної роботи №5.	6
10	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №5. Самостійне опрацювання теоретичного матеріалу.	6
11	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №6. Самостійна робота над виконанням завдань до лабораторної роботи №6.	6
12	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №6. Самостійне опрацювання теоретичного матеріалу.	6
13	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №7. Самостійна робота над виконанням завдань до лабораторної роботи №7.	6
14	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №7. Самостійне опрацювання теоретичного матеріалу.	6

15	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №8. Самостійна робота над виконанням завдань до лабораторної роботи №8	5
16	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №8.	5
17	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу.	5
	Разом за 3-ий семестр:	99

3. МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції проводяться в основному словесними методами, методами проблемного навчання і візуалізації, інтерактивними та пояснювально-ілюстративними методами, а лабораторні заняття проводяться з використанням інформаційних технологій і мають за мету – набуття студентами практичних навичок з розуміння кіберзагроз для інформації, інформаційних систем та їх компонентів, а також забезпечення кіберзахисту та організації безпеки в інформаційних системах існуючими спеціалізованими засобами та організаційними заходами.

4. ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ

Поточний контроль здійснюється під час лекційних та лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочим планом дисципліни. Семестровий контроль проводиться у формі іспиту. При цьому при виведенні остаточної оцінки враховуються результати поточного контролю.

При викладанні дисципліни використовуються такі види навчальних занять, як лекції, лабораторні роботи, індивідуальне консультування і керівництво самостійною роботою студента.

Кожний вид роботи з дисципліни оцінюється за *чотирибальною* шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих *позитивно* з врахуванням коефіцієнта вагомості. Студент, який набрав позитивний середньозважений бал за поточну роботу і не здав підсумковий контрольний захід (іспит), вважається невстигаючим.

При оцінюванні знань студентів використовуються різні засоби контролю, зокрема: усне опитування перед допуском до виконання лабораторної роботи – здійснюється на її початку; якість виконання, набуття теоретичних знань і практичних навичок перевіряється шляхом захисту кожної лабораторної роботи згідно з робочою програмою дисципліни.

Оцінка, яка виставляється за *лабораторне заняття*, складається з таких елементів: усне опитування студентів перед допуском до виконання лабораторної роботи; знання теоретичного матеріалу з теми; якість оформлення звіту і графічної частини; вміння студента обґрунтувати прийняті конструктивні рішення; своєчасний захист лабораторної роботи. Для виконання програми дисципліни студент повинен отримати 8 позитивних оцінок за лабораторні роботи в семестрі.

Пропущене лабораторне заняття студент повинен відпрацювати в лабораторіях кафедри у встановлений викладачем термін з реєстрацією у відповідному журналі кафедри, але не пізніше, ніж за тиждень до завершення теоретичних занять у семестрі.

При *оцінюванні знань* студентів викладач керується такими критеріями.

Оцінку „відмінно”, за шкалою ECTS – A (див. шкалу оцінок), отримує студент за глибоке і повне опанування змісту навчального матеріалу, в якому він легко орієнтується, понятійного апарату, за уміння зв’язувати теорію з практикою, вирішувати практичні завдання, висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає

грамотний, логічний виклад відповіді (як в усній, так і в письмовій формі), якісне зовнішнє оформлення. Студент повинен набути практичних навичок із складання різних алгоритмів та розробки програм за цими алгоритмами. Оцінка "відмінно" виставляється студенту, який глибоко засвоїв предметну область та вміє застосовувати її на практиці. Студент не повинен вагатися при видозміні запитання, повинен робити детальні та узагальнюючі висновки.

Оцінку „добре”, за шкалою ECTS – B, отримує студент за повне засвоєння навчального матеріалу, володіння понятійним апаратом, орієнтування в вивченому матеріалі, свідоме використання знань для вирішення практичних завдань, грамотний виклад відповіді, але у змісті і формі відповіді мали місце окремі неточності (похибки), нечіткі формулювання закономірностей тощо. Відповідь студента повинна будуватись на основі самостійного мислення.

Оцінку „добре”, за шкалою ECTS – C, отримує студент за правильну відповідь з однією суттєвою помилкою.

Оцінки "задовільно", за шкалою ECTS – D, заслуговує студент, який виявив знання основного навчально-програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, що справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент слабо знає структуру курсу, допускає помилки у відповіді, засвоїв і набув практичних навичок, але допустив неточності. Вагається при відповіді на видозмінене запитання, разом з тим студент володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.

Оцінки "задовільно", за шкалою ECTS – E, заслуговує студент за неповне опанування програмного матеріалу, але отримані знання і набуті практичні навички.

Оцінка „незадовільно”, за шкалою ECTS – FX, виставляється, коли студент має 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 студенту, який не може продовжити навчання без додаткових знань з курсу.

Оцінка „незадовільно”, за шкалою ECTS – F, виставляється студенту за повне незнання і нерозуміння навчального матеріалу або відмову від відповіді і передбачає повторне навчання студента з дисципліни.

Кожний вид роботи оцінюється за чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів робіт.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів у семестрі за ваговими коефіцієнтами

<table>
<tr><td colspan="10">Аудиторна робота</td><td colspan="3">Самостійна, індивідуальна робота</td><td>Форма семестрового контролю</td></tr>
<tr><td colspan="14">1 семестр</td></tr>
<tr><td colspan="8">Лабораторні роботи №:</td><td colspan="6">Практичні роботи №</td><td>Тестовий контроль:</td><td colspan="2">КР</td><td></td><td>Іспит</td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="8">ВК: 0,6</td><td colspan="6"></td><td></td><td colspan="2"></td><td></td><td>0,4</td></tr>
</table>

Примітка: Т – тема дисципліни; ВК – ваговий коефіцієнт;

Якщо студент отримав негативну оцінку, то він повинен перездати її в установленому порядку, але обов’язково до терміну наступного контролю.

Підсумкова семестрова оцінка за національною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення усіх оцінок до електронного журналу. Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС наведені у наступній таблиці.

Для переходу від вітчизняної оцінки до оцінки за шкалою ECTS необхідно знайти середньоарифметичну оцінку за вітчизняною шкалою, помножити її на відповідний ваговий коефіцієнт і, додавши всі складові, отримаємо суму балів, які визначать конкретну оцінку ECTS.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ECTS	Бали	Вітчизняна оцінка	
A	4,75-5,00	5	ВІДМІННО – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25-4,74	4	ДОБРЕ – повне знання навчального матеріалу з кількома незначними помилками
C	3,75-4,24	4	ДОБРЕ – в загальному правильна відповідь з однією суттєвою помилкою
D	3,25-3,74	3	ЗАДОВІЛЬНО – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00-3,24	3	ЗАДОВІЛЬНО – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00 -2,99	2	НЕЗАДОВІЛЬНО – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00-1, 99	2	НЕЗАДОВІЛЬНО – необхідна серйозна подальша робота і повторне вивчення дисципліни

5. ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ СТУДЕНТІВ

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.

6. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни повністю і в достатній кількості забезпечений необхідними навчально-методичними посібниками в модульному середовищі.

1. **Безпека та захист комп'ютерних систем**: методичні вказівки до виконання лабораторних робіт для студентів спеціальності "Комп'ютерна інженерія"/ О. С. Савенко, А. О. Нічепорук, Д. М. Медзатий. – Хмельницький: ХНУ, 2021. – 86 с.

7. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна література.

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 Законами № 2469-VIII від 21.06.2018, ВВР, 2018, № 31, ст.241, № 720-IX від 17.06.2020, ВВР, 2020, № 47, ст.408, № 912-IX від 17.09.2020, № 1591-IX від 30.06.2021 - вводиться в дію з 01.08.2022, № 1882-IX від 16.11.2021, № 1907-IX від 18.11.2021, № 2130-IX від 15.03.2022 , № 2470-IX від 28.07.2022}
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. Інформаційна безпека держави. Навчальний посібник / Т.М. Мужанова. Київ, 2019. 131 с.
5. Основи управління інформаційною безпекою: навч. посібник/ А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 144 с.
6. 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.
7. 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.
8. 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.

9. 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.

10. Основи інформаційної безпеки: навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.

11. Основи кібербезпеки та кібероборони: підручник/ Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. Одеса.: ОНАЗ ім. О.С. Попова, 2019. 320 с.

12. 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.

13. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів/ Козачок В.А., Гайдур Г.І., Гахов С.О., Хмелевський Р.М., Чумак Н.С. Київ: ДУТ ННІЗІ, 2020. 167 с.

14. Технології забезпечення безпеки мережевої інфраструктури/ В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. К.: КУБГ, 2019. 218 с.

15. Аналіз використання програмних приманок як засобу забезпечення інформаційної безпеки/ І.Р. Опірський, С.І. Василишин, А.З. Піскозуб// Кібербезпеки: освіта, наука, техніка, №2 (10), 2020. С. 88-97.

16. Honeypot. To bee or not to bee: A study of attacks on ICS/SCADA systems.- Mälardalen University. 2021. p. 39.

17. A novel honeypot based security approach for real-time intrusion detection and prevention systems/ Muhammet Baykara, Resul Das. Journal of Information Security and Applications, Volume 41, August 2018. pp. 103-116. https://doi.org/10.1016/j.jisa.2018.06.004

18. Fundamentals of Information Systems Security/ Editors : David Kim, Michael G. Solomon. Burlington, Massachusetts: Jones & Bartlett Learning, 2018. 548 p.

19. Information Security. Foundations, technologies and applications/ Editors: Ali Ismail Awad, Michael Fairhurst. The Institution of Engineering and Technology, 2018. 418 p.

20. 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.

21. Стецюк М. В. Методи та засоби забезпечення відмовостійкості та живучості спеціалізованих інформаційних технологій в умовах впливів зловмисного програмного забезпечення / Дис. на здобуття ступеня доктора філософії за спеціальністю 123 комп'ютерна інженерія. – Хмельницький. Хмельницький національний університет. – 2022.

22. А. Корченко, Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія, Київ, ЦП «Компринт», 2019 – 361 с.

23. Браіловський М.М. Аналіз кіберзахищеності інформаційних систем: монографія. / Браіловський М. М., Зибін С. В., Кобозева А. А., Хорошко В. О., Хохлачова Ю. Є. – К.: ФОП Ямчинський О.В., 2021. – 360 с.

24. О. Г. Корченко, С. В. Казмірчук, Б. Б. Ахметов. Прикладні системи оцінювання ризиків інформаційної безпеки: монографія. Київ, ЦП «Компринт», 2017 – 435 с.

25. А. О. Корченко, В. М. Гребенюк. Технології виявлення та попередження кібератак. – К. : Вид. НАУ, 2021. – 109 с.

26. Методи та засоби захисту інформації [Навчальний посібник] / В. А. Лахно, Є. В. Василіу, В. М. Гладких, В. М. Домрачев, Н. М. Сивкова. – К. : ЦП «Компринт» О.В., 2021. – 444 с.

Додаткова література.

27. 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.

28. 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.

29. 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.

30. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних *системах від несанкціонованого доступу.*

31. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.

32. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

33. НД ТЗІ 2.5-008-02. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.

34. НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

35. 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.

Інформаційні ресурси

Електронний університет:

1. Модульне середовище для навчання (розміщені усі необхідні навчальні матеріали з дисципліни).
2. Електронна бібліотека університету.

Електронні ресурси:

3. AV-TEST | Antivirus & Security Software & AntiMalware Reviews. https://www.av-test.org/en/
4. Avast! [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: https://www.avast.com/index (Viewed on April 28, 2023). – Title from the screen.
5. AVG [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: http://www.avg.com (Viewed on April 28, 2023). – Title from the screen.
6. Avira [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: http://www.avira.com (Viewed on April 28, 2023). – Title from the screen.
7. ClamAV [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: https://www.clamav.net/ (Viewed on April 28, 2023). – Title from the screen.
8. 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 Communicationsrimer.pdf (Viewed on April 28, 2023). – Title from the screen.
9. 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 28, 2023). – Title from the screen.
10. https://www.virusbulletin.com/
11. ESET Endpoint Security [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: http://www.eset.com/ (Viewed on April 28, 2023). – Title from the screen.

12. Symantec Endpoint Protection [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: https://www.anti-malware.ru/reviews/ Symantec_Endpoint_Protection (Viewed on April 28, 2023). – Title from the screen.