

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

Навчально-науковий інститут автоматики та електротехніки
Кафедра комп'ютерних технологій та інформаційної безпеки

Код за ОПІ
ПІІ3



ЗАТВЕРДЖУЮ

Проректор з науково-педагогічної
роботи, к.т.н., доцент

С.О. Слободян

2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Program of the Discipline

**БЕЗПЕКА ІНФОРМАЦІЙНИХ ТА КОМУНІКАЦІЙНИХ
СИСТЕМ**

Information and communication systems security

Рівень вищої освіти перший (бакалаврський)
Тип дисципліни обов'язкова
Мова викладання українська

Миколаїв 2023 рік

Робоча програма навчальної дисципліни «Безпека інформаційних та комунікаційних систем» є однією із складових комплексної підготовки фахівців галузі знань 12 «Інформаційні технології», спеціальності 125 «Кібербезпека та захист інформації», освітня програма «Системи технічного захисту інформації, автоматизація її обробки»

«___» _____ 2023 р. – с.

Розробник: Турти М.В., доцент кафедри Комп'ютерних технологій та інформаційної безпеки, канд. техн. наук, доцент

Проект робочої програми навчальної дисципліни «Безпека інформаційних та комунікаційних систем» узгоджено з гарантом освітньої програми

Гарант освітньої програми «Системи технічного захисту інформації, автоматизація її обробки»

Нужний С.М., канд. техн. наук, доцент



Проект робочої програми навчальної дисципліни «Безпека інформаційних та комунікаційних систем» розглянуто на засіданні кафедри КТІБ.

Протокол від «13» _____ 06 2023 р. № 12.

Завідувач кафедри КТІБ, к.т.н., доцент _____ С.М. Нужний



Проект робочої програми навчальної дисципліни «Безпека інформаційних та комунікаційних систем» розглянуто методичною радою Навчально-наукового інституту автоматики та електротехніки.

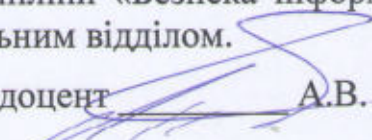
Протокол від «30» _____ 08 2023 р. № 1.

Голова, к.т.н., доц. _____ Д.О.Жук



Проект робочої програми навчальної дисципліни «Безпека інформаційних та комунікаційних систем» погоджено з навчальним відділом.

Начальник навчального відділу, к.т.н., доцент _____ А.В. Лабарткава

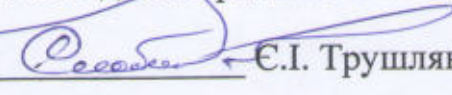


Робочу програму навчальної дисципліни «Безпека інформаційних та комунікаційних систем» затверджено Навчально-методичною радою НУК ім. адм. Макарова.

Протокол від «7» _____ 09 2023 р. № 6.

Голова Навчально-методичної ради НУК ім. адм. Макарова,

д.т.н., професор _____ Є.І. Трушляков



ЗМІСТ

Вступ.....	4
1. Опис навчальної дисципліни	5
2. Мета навчальної дисципліни	6
3. Передумови для вивчення навчальної дисципліни	6
4. Очікувані результати навчання	7
5. Програма навчальної дисципліни	8
6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування.....	27
7. Форми поточного та підсумкового контролю	28
8. Критерії оцінювання результатів навчання.....	30
9. Засоби навчання	36
10. Рекомендовані джерела інформації.....	37

ВСТУП

Анотація

Навчальна дисципліна «Безпека інформаційних та комунікаційних систем» є дисципліною професійної підготовки бакалаврів зі спеціальності 125 «Кібербезпека та захист інформації». Дана дисципліна є обов'язковим компонентом освітньої програми, який забезпечує здобуття студентами теоретичних відомостей про принципи побудови і формування практичних умінь створення захищених інформаційних та комунікаційних систем. Отримані слухачами курсу теоретичні знання та практичні навички є базовим програмним результатом навчання та формують фахову компетентність.

Ключові слова: інформаційно-комунікаційні системи, типові вразливості, віддалена атака, захист на рівні операційних систем, захист розподілених мереж

Abstract

The educational discipline " Information and communication systems security " is a discipline of professional training of bachelors in the specialty 125 "Cybersecurity and information protection". This discipline is a mandatory component of the educational program, which ensures that students acquire theoretical information about the principles of construction and formation of practical skills for creating protected information and communication systems. The theoretical knowledge and practical skills acquired by the course participants are the basic program learning outcome and form professional competence.

Keywords: information and communication systems, typical vulnerabilities, remote attack, protection at the level of operating systems, protection of distributed networks

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів – 12	Галузь знань 12 Інформаційні технології Спеціальність: 125 Кібербезпека та захист інформації	Обов’язкова	
Модулів – 4	Освітня програма «Системи технічного захисту інформації, автоматизація її обробки»	Рік підготовки	
Змістових модулів – 6		2-й, 3-й	2-й, 3-й
Курсова робота “Захищена телекомунікаційна система”		Семестр	
Загальна кількість годин – 360		4-й, 5-й, 6-й	4-й, 5-й, 6-й
		Індивідуальне науково-дослідне завдання – курсова робота	
Тижневих годин для денної форми навчання: 4-й семестр: Аудиторних – 2; Самостійної роботи: – 4. 5-й семестр: Аудиторних – 4; Самостійної роботи: – 4. 6-ий семестр: Аудиторних – 2; Самостійної роботи: – 8.	Рівень вищої освіти: перший (бакалаврський)	Лекції, год	
		45 год.	14 год.
		Лабораторні роботи, год	
		75 год.	29 год.
		Практичні роботи, год	
		-	-
		Самостійна робота, год	
		240	317
		Вид контролю: 4-й семестр – екзамен 5-й семестр - екзамен 6-й семестр - курсова робота, екзамен	
	Форма контролю: усна, письмова		

2. Мета навчальної дисципліни

Метою вивчення навчальної дисципліни «Безпека інформаційних та комунікаційних систем» є ознайомлення студентів із теоретичними методами побудови захищених інформаційних і комунікаційних систем та здобуття практичних навичок налагодження ефективних систем захисту з врахуванням особливостей їх апаратної та програмної реалізації.

Завданнями дисципліни є теоретична та практична підготовка студентів для вирішення конкретних фахових питань, зокрема: обґрунтування прийняття проектних рішень в галузі захисту інформації в телекомунікаційних мережах і системах на основі аналізу загроз і моделі порушника; здобуття практичних навичок застосування спеціалізованого програмного і апаратного забезпечення для захисту інформації в телекомунікаційних мережах і системах для формування наступних компетентностей.

- (ЗК1) - Здатність застосовувати знання у практичних ситуаціях;
- (ФК6) - Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження;
- (ФК9) - Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою;
- (ФК11) - Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки;
- (ФК12) - Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

3. Передумови для вивчення навчальної дисципліни

Для ефективного вивчення дисципліни «Безпека інформаційних та комунікаційних систем», студенти повинні засвоїти матеріал з дисциплін:

- Інформаційні технології систем управління та захисту інформації;
- Бази даних;
- Системи і мережі передачі даних.

4. Очікувані результати навчання

Основними (програмними) результатами навчання з дисципліни «Безпека інформаційних та комунікаційних систем» є:

- (PH13) аналізувати проекти інформаційно-комунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;
- (PH15) використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;
- (PH17) – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;
- (PH18) – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;
- (PH19) – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
- (PH21) вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-комунікаційних (автоматизованих) системах;
- (PH22) вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;
- (PH23) – Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
- (PH25) Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в' інформаційних та інформаційно-комунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;
- (PH26) – Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;

- (PH27) – Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;
- (PH28) – Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки;
- (PH29) – Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;
- (PH30) – Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;
- (PH31) – Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
- (PH32) – Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;
- (PH41) – Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;
- (PH45) – Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;
- (PH46) – Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;
- (PH50) – Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);
- (PH51) – Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;
- (PH52) – Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

5. Програма навчальної дисципліни

Модуль 1

Змістовий модуль 1. Основні принципи побудови захищених інформаційно-телекомунікаційних систем.

Тема 1. Базові поняття в галузі захисту інформаційно-телекомунікаційних систем. [1] – с.12-21; [3] – с.7-16, 57-61, 64-70, 74-80; [4] – с.18-26, 32-34, 62-75, 142-187, 316-332; [5] – с.26-31; [7-11]; [18]; [21] – с.71-84.

Перелік питань, що виносяться на вивчення за темою:

Кіберпростір, кібербезпека та кібертероризм: поняття і визначення. Інформаційне протиборство, інформаційна війна, інформаційна зброя. Способи та методи ведення розвідки ІТ-систем. Системи, в яких здійснюється захист інформації. Об'єкти захисту. Завдання захисту інформації. Політика інформаційної безпеки. Профіль захищеності автоматизованої системи. Загрози і вразливості. Захищена комп'ютерна система, комплекс засобів захисту, ідентифікація, автентифікація, авторизація, правила розмежування доступу. Моделі інформаційної безпеки: модель загроз, модель порушника, Cyber Kill Chain, , моделі доступу (дискреційна, мандатна, рольова, безпека потоків даних, ізольоване програмне середовище), моделі цілісності, теорія інформаційної безпеки. Критерії оцінювання захищеності інформаційно-комунікаційних систем.

Тема 2. Вразливості і загрози інформаційно-комунікаційних систем [1] – с.27-30; [3] – с.24-29; [4] – с.27-30, 31-32, 78-97, 329-339; [5] – с.18-26; [21] - с.64-71; [30].

Перелік питань, що виносяться на вивчення за темою:

Класифікація загроз. Типові загрози безпеці. Узагальнена схема загроз комп'ютерній системі. Методика класифікації загроз STRIDE. Класифікація кібернетичних втручань і загроз за схемою, запропонованою Конвенцією Ради Європи (2001 р.) Передумови виникнення вразливостей в комп'ютерних системах. Класифікація джерел інцидентів, а також способів, об'єктів та результатів їхнього впливу. Класифікація мережевих аномалій. К л а с и ф і к а ц і я і н д и к а т о р і в к о м п р о м е т а ц і ї. Класифікація вад захисту. Класифікація помилок програмної реалізації системи. Помилки переповнення буферу. Помилки обробки рядків тексту. Загрози інформації в комп'ютерних мережах. Стеки протоколів відкритих систем. Сервіси і механізми безпеки.

Тема 3. Типові віддалені атаки [1] – с.648-667; [3] – с.44-53; [4] – с.30-31; [20].

Перелік питань, що виносяться на вивчення за темою:

Класифікація атак: віддалене проникнення, локальне проникнення, віддалена відмова в обслуговуванні, локальна відмова в обслуговуванні, сканування мережі, сканування вразливостей, злам паролів, пасивне прослуховування трафіку. Загальна структура кібернетичної атаки. Класифікація типових віддалених атак за базовими ознаками несанкціонованого доступу. Класифікація кібернетичних атак П.Ноймана. Особливості найбільш поширених атак (DoS: Flood, ICMP flood, Identification flood, TCP SYN flood, Ping of Death, Tribe Flood Network, Trinco, Stacheldracht, Trinity; DDoS: TCP SYN flood, TCP flood, SYN flooding, UDP flood, ICMP flood; сніфер пакетів; IP-спуфінг; паролльні атаки, логічні бомби; троянські коні; вірусні атаки; ін'єкції).

Тема 4. Шкідливі програмні засоби [1] – с.667-670; [3] – с.53, 80-84, 112-136; [4] – с.99-135; [5] – с.112-121.

Перелік питань, що виносяться на вивчення за темою:

Класифікація шкідливого програмного забезпечення. Програми-шпигуни. Класифікація вірусів за середовищем розповсюдження, способам маскуванню в середовищі, інфікованим об'єктам, способу інфікування об'єктів, способу розміщення в інфікованому об'єкті, руйнівним впливам, здатності до змін, стилю написання, типу кода. Програмні закладки. Хробак Морріса. Класифікація троянських вірусів. Соціальна інженерія. Фшинг, бейтинг, вішинг, фармінг. Методи боротьби з ШПЗ: методи виявлення ШПЗ, технології боротьби з ШПЗ, методи усунення наслідків зараження ШПЗ. Захист від комп'ютерних вірусів: структура системи антивірусного захисту, сучасні антивірусні програми.

Змістовий модуль 2. Базові засоби захисту інформації в інформаційно-телекомунікаційних системах

Тема 5. Організація захисту інформації в інформаційно-комунікаційних системах [1] – с.671-677; [2] – с.20-37; [3] – с.35-42, [4] – с.37-49, 333-340; [5] – с.7-17; [7-15]; [21] – с.38-54; [29]; [30].

Перелік питань, що виносяться на вивчення за темою:

Структура інформаційно-комунікаційних систем та їх рівні. Зонування мережевої безпеки. Підходи до забезпечення захисту інформації в ІТС. Моделі управління мережевими ресурсами. Несанкціонований доступ на різних рівнях інформаційно-комунікаційних систем. Функціональні сервіси безпеки і механізми, що їх реалізують. Класифікація засобів захисту від НСД. Базові вимоги до засобів захисту. Класифікація засобів захисту програмного забезпечення. Структура комплексу засобів захисту. Рекомендації американської ІТ-компанії SANS щодо заходів забезпечення кібербезпеки комп'ютерних систем і мереж. Рекомендації CERT-UA щодо захисту інформації в інформаційно-комунікаційних системах.

Тема 6. Захист інформації в операційних системах [4] – с.189-312; [5] – с.73-82, 206-210

Перелік питань, що виносяться на вивчення за темою:

Апаратне забезпечення засобів захисту. Функції захисту інформації в процесорах Intel. Керування оперативною пам'яттю. Керування задачами. Загрози безпеці операційних систем. Побудова захищених операційних систем. Засоби захисту в операційних системах Windows, Unix, Linux, Solaris, Фенікс. PGP.

Тема 7. Міжмережевий екран [1] – с.694-711; [2] – с.63-66; [4] – с.465-474; [5] - с.62-95

Перелік питань, що виносяться на вивчення за темою:

Архітектура захищених мереж. Функції міжмережевих екранів. Структура міжмережевих екранів. Рівні реалізації міжмережевих екранів. Схеми підключення міжмережевих екранів. Особливості персональних брандмауерів. Екрануючий шлюз прикладного рівня (пакетний фільтр). Екрануючий шлюз сеансового рівня. Недоліки міжмережевих екранів. Політика міжмережевої взаємодії: політика доступу до мережесервісів, політика роботи міжмережевого екрану. Налаштування параметрів міжмережевих екранів.

Тема 8. Безпека мережесервісів Інтернет-протоколів [4] – с.343-408, 500-508; [5] – с.170-174, 178-206

Перелік питань, що виносяться на вивчення за темою:

Ієрархія протоколів. Протоколи прикладного рівня: Telnet, FTP, мережні служби Unix. Протоколи транспортного рівня: UDP, TCP. Протоколи мережного рівня: IP. Протокол маршрутизації BGP. Протоколи керування мережею: ICMP, SNMP. Архітектура засобів захисту IPsec. Протокол AH. Протокол ESP. Робота AH і ESP в транспортному режимі і в режимі тунелювання. Протокол IKE. Протокол ISAKMP. Протоколи створення криптозахисених віртуальних каналів на канальному рівні. Протокол PPP. Протокол PPTP. Протокол L2TP. Протокол SSL/TLS. П р о т о к о л SSH.

Модуль 2

Змістовий модуль 3. Завадостійкі системи передавання інформації

Тема 9. Інформаційні системи передачі даних [1] – с.14-19, 335—351, 406-423

Перелік питань, що виносяться на вивчення за темою:

Узагальнена схема передавання даних. Показники якості дискретних каналів зв'язку. Завадостійкість. Електромагнітна сумісність. Методи забезпечення енергетичної і структурної секретності. Класифікація інформаційних каналів за природою сигналів. Класифікація інформаційних каналів за частотними діапазонами. Особливості радіоканалу. Класифікація інформаційних каналів за структурою. Інформаційно-комунікаційні мережі: структура, апаратне забезпечення, організація доступу, використовувані протоколи на різних рівнях моделі OSI.

Тема 10. Характеристики інформаційних каналів [1] – с.351-373

Перелік питань, що виносяться на вивчення за темою:

Час передавання сигналу. Ширина частотного спектру. Середня потужність сигналу. Динамічний діапазон інформаційного каналу. Обсяг сигналу. Ємність каналу. Загальна умова узгодженості сигналу і каналу передавання інформації. Достатня умова узгодженості сигналу і каналу передавання інформації. Швидкість передавання інформації. Пропускна здатність каналу передавання інформації. Швидкість введення інформації. Завади в неперервному каналі передавання інформації. Характеристики дискретного каналу передавання інформації. Моделі дискретних каналів передавання інформації: двійковий несиметричний канал без пам'яті, двійковий симетричний канал без пам'яті, симетричний канал без пам'яті із стиранням. Основна задача прийняття дискретних сигналів. Зворотна задача прийняття дискретних сигналів. Швидкість передавання інформації і пропускна здатність дискретного каналу без завад. Швидкість передавання інформації і пропускна здатність дискретного каналу із завадами. Швидкість передавання інформації і пропускна здатність неперервного каналу із завадами.

Тема 11. Синтез елементів інформаційних систем [1] – с.373-387

Перелік питань, що виносяться на вивчення за темою:

Оптимальний приймач. Задачі аналізу. Задачі синтезу. Виявлення інформаційного сигналу на фоні завад. Розпізнавання сигналу на фоні завад. Визначення параметрів сигналу на фоні завад. Виділення сигналу на фоні завад. Синтез приймачів неперервних сигналів. Ідеальний приймач Котельникова. Оптимальні приймачі з активною і пасивною паузами.

Тема 12. Багатоканальні мережі передачі [1] – с.387–396.

Перелік питань, що виносяться на вивчення за темою:

Розподіл інформаційних каналів. Класифікація розподілів інформаційних каналів, з просторовим розділенням, з диференціальним розділенням, з частотним розділенням, з часовим розділенням, з фазовим розділенням, з просторовим розділенням, з розділенням за формою, з кореляційним

розділенням. Схема розділення каналів на фоні ортогональних функцій. Багатоканальні системи зв'язку з комбінованими схемами розділення каналів.

Змістовий модуль 4. Принципи забезпечення інформаційної безпеки в системах передавання інформації

Тема 13. Завадостійкість систем передачі інформації [1] – с.396-404; [3] – с.136-142; [4] – с.413-459; [6] – с.33-40

Перелік питань, що виносяться на вивчення за темою:

Завадостійкість систем передавання інформації. Критерії оцінювання завадостійкості систем передавання інформації. Потенційна завадостійкість прийняття дискретних сигналів. Потенційна завадостійкість прийняття інформаційних сигналів за Котельниковим. Оптимальний приймач Котельникова з системою прийняття рішень на базі визначених порогів на фоні завад. Схема кореляційного приймача із визначеним порогом прийняття рішень на фоні завад. Безпека електронної пошти. Безпека web-ресурсів. SQL-ін'єкції. Міжсайтовий скринінг. Модель безпеки технології Java. Порівняльний аналіз можливостей реалізації телекомунікаційних послуг на основі різних протоколів. Показники якості надання послуг в авіаційній телекомунікаційній мережі

Тема 14. Системи бездротової передачі інформації та захист інформаційних ресурсів [1] – с.434-460

Перелік питань, що виносяться на вивчення за темою:

Переваги бездротових мереж. Технології розширення спектру: частотне розширення спектру, розширення спектру з прямою послідовністю. Коди Баркера. Модуляція в каналах без провідникового зв'язку. Кодування в каналах без провідникового зв'язку. Розділення каналів у багатоканальних системах безпровідного зв'язку: ортогональне частотне розділення каналів (частотне розділення каналів із мультиплексуванням, запобігання між символної інтерференції за допомогою охоронних інтервалів, метод пакетного згорткового кодування. Мережеві пристрої і точки доступу систем бездротового зв'язку. Робочі режими систем і мереж бездротового зв'язку: режими, які визначаються на МАС-рівні (локальні бездротові мережі, інфраструктурні мережі); режими, які визначаються на каналному рівні (функція розподіленої координації, функція централізованої координації). Вибір конфігурації бездротової мережі. Режим мультиплексорного моста для об'єднання територіально рознесених сегментів провідникових мереж. Інтеграція безпровідних сегментів до стандартної провідникової мережі. Ширококутний маршрутизатор. Ширококутний шлюз. Системи супутникового зв'язку: принципи функціонування, переваги, архітектура, групові тракти і групові канали передачі станцій супутникового зв'язку, класифікація методів і засобів побудови інтегрованих інформаційно-комунікаційних систем супутникового зв'язку, методи кодування в системах супутникового зв'язку.

Тема 15. Множинний доступ до інформаційних ресурсів [1] – с.460-481; [2] – с. 174-213; [3] – с.142-144; [5] – с.165-210.

Перелік питань, що виносяться на вивчення за темою:

Множинний доступ з частотним розподіленням в супутникових системах. Множинний доступ з часовим розділенням (ущільнення). Багатоканальний розподіл ресурсу зв'язку. Швидкість передачі в системах FDMA та TDMA. Затримка повідомлень в системах FDMA та TDMA. Множинний доступ з кодовим розділенням: розширення спектра методом прямої послідовності, розширення спектра методом стрибкоподібного перестроювання частоти, конфіденційність передачі інформаційних потоків. Канали із завмираннями. Управління множинним доступом. Множинний доступ з наданням каналів за вимогою. Порівняння ширини смуги для фіксованого і динамічного розподілу каналів. Супутникова комутація. Системи зв'язку множинного доступу та їх архітектура. Безпека телефонного зв'язку. Класифікація VPN. Сервіси безпеки VPN. Створення гостьової VLAN з обмеженими правами.

Модуль 3

Змістовий модуль 5. Утіліти в системах захисту інформації

Тема 16. Kali Linux. Інсталяція, вбудовані засоби захисту інформації. [33].

Перелік питань, що виносяться на вивчення за темою:

Віртуалізація операційних систем. VirtualBox. Засоби Kali Linux для тестування на проникнення: Armitage (графічний інструмент управління кібератаками), Nmap (сканер портів), Wireshark (аналізатор трафіку), John the Ripper (зломщик паролів), Aircrack-ng (набір програмного забезпечення для проникнення у бездротові локальні мережі), Burp suite, OWASP ZAP (сканер безпеки веб-додатків), Pentbox, PenTest, Docker (Docker Engine, Docker Compose)

Тема 17. Використання утиліт моніторингу трафіку для захисту інформації в локальних мережах [2] – с.161-174; [4] – с.484-489; [5] - с.31-61.

Перелік питань, що виносяться на вивчення за темою:

Методи виявлення атак в комп'ютерних мережах (метод виявлення аномалій в мережевому трафіку, метод виявлення зловживань у мережевому трафіку, поведінкові методи, методи штучного інтелекту). Сканери безпеки комп'ютерних мереж/ Методи та методики мережевого сканування: відкриті методи сканування (TCP SYN scanning за допомогою функції connect, сканування TCP-портів методом reverse-ident (зворотної ідентифікації)), напіввідкриті методи сканування (SYN scan), приховані методи сканування, АСК-сканування. Мережеві аналізатори: принципи функціонування, схема застосування, tcpdump, wireshark. Класифікація засобів моніторингу та аналізу мереж. Система моніторингу мережі Zabbix. Системи глибокого аналізу пакетів DPI. Системи аналізу мережевого трафіку NTA. Функції контролю підключення вузлів до портів комутатора: Port Security, IP-MAC-Port Binding. Проведення автентифікації користувачів за стандартом IEEE 802.1X: ролі пристроїв, протокол EAP, алгоритм, налаштування комутатора. Network Monitor: призначення, принцип дії, вихідні дані, налаштування фільтру. eEye Iris: призначення, принцип дії, вихідні дані, налаштування фільтру.

Тема 18. Використання утиліт виявлення вразливостей для захисту інформації в локальних мережах [4] – с.484-489, [5] – с.42-44

Перелік питань, що виносяться на вивчення за темою:

Система виявлення вразливостей і реагування на кіберінциденти та кібератаки в Україні. «Програма виявлення вразливостей» в інформаційно-комунікаційних системах, НКЦК при РНБО України за підтримки міжнародних партнерів. Порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератак. Aigerplay-ng. Airgeddon. WiFite. Scapy. Zulu. HiJackThis Fork. Kamerka. Утіліта APS: призначення, переваги, налаштування системи імітації сервісів, користувацька база портів та відповідні протоколи, динамічні елементи «банера» TCPView: призначення, налаштування, період відновлення. Сканер nmap. Евристичні методи пошуку вразливостей. XSpider: призначення, принцип дії, перевантаження каналу (причини і способи подолання), створення і активація розкладу, типи вразливостей, що визначаються, доступні для сканування мережеві служби, перевизначення вразливостей, файл портів, налаштування, автоматизація роботи утиліти.

Змістовий модуль 6. Системи захисту інформації

Тема 19. Засоби виявлення вторгнень і системи запобігання вторгненням [2] – с.99-131; [4] – с.474-484; [5] – с. 95-111, 121-127.

Перелік питань, що виносяться на вивчення за темою:

Технології виявлення вторгнень. Функціональні можливості систем виявлення вторгнень.

Архітектура систем виявлення атак. Класифікація систем виявлення вторгнень. Системи виявлення атак рівня мережі, вузла, прикладних програм. Варіанти розташування сенсорів систем виявлення вторгнень мережного рівня. Інформаційні джерела для систем виявлення вторгнень. Обробка подій в системах виявлення вторгнень. Реакція на події систем виявлення вторгнень. Додаткові засоби систем виявлення вторгнень. Системи виявлення вразливостей. Функціональні можливості систем запобігання вторгненням. IDS/IPS Suricata. Інтелектуальні системи виявлення і запобігання вторгненням. Технології виявлення та блокування кібератак на кінцевих пристроях: EDR, UBA, UEBA. Технології протидії витокам інформації (DLP). SATAN. Internet Scanner. Nessus.

Тема 20. Використання технологій обману (Deception Technology) і технології безпечного виконання програм (Sandbox) в захисті ІТС [5] – с.128-142; [35]

Перелік питань, що виносяться на вивчення за темою:

Призначення і принципи Deception Technology. Класифікація існуючих типів Deception Technology. Складові частини Deception Technology: honeypot, honeynet, honeytokens, honeywall. Класифікація honeypot. Honeypot в ієрархії політик. Особливості використання honeypot із різним ступенем взаємодії зі зловмисником, виробничих honeypot, дослідницьких honeypot. Розташування honeypot. Розгортання honeypot в мережі. Розгортання Deception Technology. Переваги honeypot. Недоліки honeypot. SNARE. Conpot. Ринок honeypot. Проекти honeypot. Sandbox: принципи функціонування, класифікація пісочниць.

Тема 21. Пентестинг [3] – с.190-197, [19]; [31].

Перелік питань, що виносяться на вивчення за темою:

Білий хакінг. Пентести. Експлойти. Методи проведення пентестінгу. Black-Box пентест. White-Box пентест. Grey-Box пентест. Glass Box пентест. Black Hat. White Hat. Технічні методи тестування на проникнення. Пристрої для проведення пентестінгу. Методики оцінки безпеки мережевого та прикладного рівнів: Open Source Security Testing Methodology Manual (OSSTMM), Information Systems Security Assessment Framework (ISSAF), Open Web Application Security Project (OWASP) Top Ten, Web Application Security Consortium Threat Classification (WASC-TC). Платформа BackTrack. Соціоінженерні методи тестування на проникнення. Сканери безпеки. Бази вразливостей. Сучасні підходи щодо проведення пентестінгу.

Тема 22. SIEM системи [5] – с.142-164

Перелік питань, що виносяться на вивчення за темою:

Технології SIEM. Функції SIEM. Переваги SIEM. Використання методів кореляції в реагуванні на кібератаки. Рівні роботи SIEM. Структура та схема роботи SIEM. Джерела інформації SIEM. Стек ELK як система централізованого зберігання журналів: Beats, Logstash, Elasticsearch, Kibana, Scirius Community Edition, Узагальнена схема роботи стека, налагодження конфігурації, порівняння Elasticsearch і SQL. Система управління інформацією та подіями безпеки SIEM SPLUNK: призначення, архітектура, файли конфігурації, пересилання даних на сервер, конвеєр даних, Search Processing Language (типи пошуків, типи команд, алгоритм виконання пошуку, запит SPL)

Модуль 4

Індивідуальне науково-дослідне завдання (ІНДЗ):

курсова робота на тему "Розробка захищеної телекомунікаційної система для
" _____ " .
(назва об'єкта інформаційної діяльності)

Тематичний план навчальної дисципліни

Назви змістових модулів і тем	Кількість годин							
	денна форма				заочна форма			
	усього	у тому числі			усього	у тому числі		
		л	лаб	с.р.		л	лаб	с.р.
Модуль 1 (М1)								
Змістовий модуль 1. Основні принципи побудови захищених інформаційно-телекомунікаційних систем								
Тема 1. Базові поняття в галузі захисту інформаційно-телекомунікаційних систем	10	2	2	6	10	2	-	8
Тема 2. Вразливості і загрози інформаційно-комунікаційних систем	6	2	-	4	6		-	6
Тема 3. Типові віддалені атаки	6	2	-	4	6		-	6
Тема 4. Шкідливі програмні засоби	8	2	1	5	8		2	6
Разом за змістовим модулем 1	30	8	3	19	30	2	2	26
Змістовий модуль 2. Базові засоби захисту інформації в інформаційно-телекомунікаційних системах								
Тема 5. Організація захисту інформації в інформаційно-комунікаційних системах	6	2	-	4	6	2	-	4
Тема 6. Захист інформації в операційних системах	36	2	10	24	36		6	30
Тема 7. Міжмережевий екран	12	2	2	8	12		2	10
Тема 8. Безпека мережевих Інтернет-протоколів	6	1	-	5	6		-	6
Разом за змістовим модулем 2	60	7	12	41	60	2	8	50
Разом за модулем 1	90	15	15	60	90	4	10	76
Модуль 2 (М2)								
Змістовий модуль 3. Завадостійкі системи передавання інформації								
Тема 9. Інформаційні системи передачі даних	15	2	4	9	15	2	2	11
Тема 10. Характеристики інформаційних каналів	15	4	2	9	15		-	15
Тема 11. Синтез елементів інформаційних систем	15	2	6	7	15	2	2	11
Разом за змістовим модулем 3	45	8	12	25	45	4	4	37

Назви змістових модулів і тем	Кількість годин							
	денна форма				заочна форма			
	усього	у тому числі			усього	у тому числі		
		л	лаб	с.р.		л	лаб	с.р.
Змістовий модуль 4. Принципи забезпечення інформаційної безпеки в системах передавання інформації								
Тема 12. Багатоканальні мережі передачі	15	2	8	5	15	2	2	11
Тема 13. Завадостійкість систем передачі інформації	15	2	6	7	15		2	13
Тема 14. Системи бездротової передачі інформації та захист інформаційних ресурсів	15	2	6	7	15		2	13
Тема 15. Множинний доступ до інформаційних ресурсів	30	1	13	16	30		2	28
Разом за змістовим модулем 4	75	7	33	35	75	2	8	65
Разом за модулем 2	120	15	45	60	120	6	12	102
Модуль 3 (МЗ)								
Змістовий модуль 5. Утиліти в системах захисту інформації								
Тема 16. Kali Linux. Інсталяція, вбудовані засоби захисту інформації	10	2	2	6	10	2	1	7
Тема 17. Використання утиліт моніторингу трафіку для захисту інформації в локальних мережах	10	2	2	6	10		1	9
Тема 18. Використання утиліт виявлення вразливостей для захисту інформації в локальних мережах	10	2	2	6	10		1	9
Разом за змістовим модулем 5	30	6	6	18	30	2	3	25
Змістовий модуль 6. Системи захисту інформації								
Тема 19. Засоби виявлення вторгнень і системи запобігання вторгненням	7	2	2	3	7	2	1	4
Тема 20. Використання технологій обману (Deception Technology) і технології безпечного виконання програм (Sandbox) в захисті ІТС	7	2	2	3	7		1	6
Тема 21. Пентестинг	7	2	2	3	7		1	6
Тема 22. SIEM системи	9	3	3	3	9		1	8
Разом за змістовим модулем 6	30	9	9	12	30	2	4	24

Назви змістових модулів і тем	Кількість годин							
	денна форма				заочна форма			
	усього	у тому числі			усього	у тому числі		
		л	лаб	с.р.		л	лаб	с.р.
Разом за модулем 3	60	15	15	30	60	4	7	49
Модуль 4 (М4)								
Курсовий проект	90	-	-	90	90	-	-	90
Разом (М1+М2+М3+М4)	360	45	75	240	360	14	29	317

Для студентів заочної форми навчання читаються оглядові лекції за темами змістових модулів в обсягах відповідно до вищенаведеної таблиці.

Теми практичних занять

Практичні роботи програмою не передбачені

Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		ДФН	ЗФН
1	Захист інформації засобами BIOS	2	-
2	Захист від вірусних загроз	1	2
3	Налаштування доступу користувачів до інформаційних ресурсів в Windows	2	2
4	Захист файлових ресурсів	2	-
5	Налаштування локальної політики безпеки в Windows	2	2
6	Захищене резервне копіювання та відновлення	2	-
7	Система аудиту доступу до ресурсів у Windows	2	2
8	Робота брандмауера в Windows	2	2
9	Моделювання комп'ютерних мереж	2	-
10	Дослідження міцності парольного захисту	2	2
11	IP-безпека (IPSec)	2	-
12	Файлова система та розмежування доступу в Linux	2	2
13	Забезпечення цілісності та доступності даних в Linux	2	-
14	Шифрування даних Linux.	2	-
15	Налаштування параметрів мережевого обладнання TP-Link	2	-
16	Налаштування параметрів мережевого обладнання Cisco	2	2

№ з/п	Назва теми	Кількість годин	
		ДФН	ЗФН
17	Міжмережевий екран з фільтрацією пакетів та з подвійним шлюзом	2	-
18	Міжмережевий екран з ізолюваним хостом та з ізолюваною підмережею	2	-
19	Захист електронної пошти засобами шифрування та автентифікації	2	-
20	Захист електронної пошти від вірусів та спаму	2	2
21	Захист веб-ресурсів	2	-
22	Протокол для реалізації автентифікації RADIUS	2	2
23	Налаштування тунелю GRE «точка-точка»	2	-
24	Основи роботи з Tor	2	-
25	OpenVPN	2	-
26	Побудова захищених віртуальних приватних мереж за допомогою Wireguard	2	-
27	Засоби VLAN	2	-
28	Захист бездротових мереж	2	-
29	VoIP Asterisk	2	-
30	Система радіодоступу	3	2
31	Засоби захисту інформації в Kali Linux	2	1
32	Утіліти моніторингу трафіку	2	1
33	Утіліти виявлення вразливостей локальної мережі	2	1
34	Засоби виявлення мережних атак	2	1
35	Honeypot	2	1
36	Пентестинг	2	1
37	Налаштування систем SIEM	3	1
Разом		75	29

Студенти заочної форми виконують роботи № 2, 3, 5, 7, 8, 10, 12, 16, 20, 22, 30 із розрахунку 2 год./ 1 лаб. роботу та роботи № 31-37 із розрахунку 1 год./ 1 лаб. роботу.

Самостійна робота

Самостійна робота здобувача вищої освіти є однією з форм організації навчання, основною формою оволодіння навчального матеріалу в час, вільний від обов'язкових навчальних занять.

Метою самостійної роботи є повторення й осмислення студентом основних питань кожної теми, висвітлених на лекційних і лабораторних заняттях. Самостійна робота проводиться в лабораторіях НУК, читальних

залах, на об'єктах майбутньої діяльності і/або вдома. Результати цієї роботи фіксуються студентом в індивідуальному робочому зошиті (конспекті).

Навчальний матеріал дисципліни, передбачений для засвоєння здобувачем вищої освіти в процесі самостійної роботи, виноситься на підсумковий контроль поряд з навчальним матеріалом, який опрацьовувався при проведенні навчальних занять.

В рамках самостійної роботи також виконується індивідуальне науково-дослідне завдання у формі курсової роботи.

Розподіл годин самостійної роботи для денної форми навчання:

- підготовка до лекційних занять – 0,5 год. / 1 заняття (на 1 лекцію);
- самостійне опрацювання окремих тем навчальної дисципліни (які не викладаються на лекціях) – 1-3 год. / 1 заняття;
- підготовка до лабораторних занять – 1 год. / 1 заняття;
- підготовка до модульних контрольних робіт 2-15 год на 1 роботу
- підготовка до екзаменів – 15 год. на 1 захід.

Розподіл годин самостійної роботи для заочної форми навчання:

- підготовка до лекційних занять – 0,5 - 2 год. / 1 заняття (на 1 лекцію);
- самостійне опрацювання окремих тем навчальної дисципліни (які не викладаються на лекціях) – 1-3 год. / 1 заняття;
- підготовка до лабораторних занять – 2-3 год. / 1 заняття;
- підготовка до модульних контрольних робіт 8-15 год на 1 роботу
- підготовка до екзаменів – 15-30 год. на 1 захід.

Розподіл годин самостійного опрацювання окремих тем навчальної дисципліни

№ з/п	Назва теми	Кількість годин	
		Д.Ф.Н	З.Ф.Н.
М1			
1	До теми 1. Захист інформації засобами BIOS	0,25	0,5
2	До теми 2. Нормативно-правове забезпечення захисту інформації в телекомунікаційних системах і мережах	0,5	0,5
3	До теми 3. Статистика віддалених атак на розподілені обчислювальні системи	0,25	0,5
4	До теми 4. Сучасні антивірусні програми	0,25	0,5
5	До теми 5. Сучасні апаратні засоби побудови захищених телекомунікаційних систем і мереж	0,5	0,5
6	До теми 6. Сучасні програмні засоби побудови захищених телекомунікаційних систем і мереж	0,5	1
7	До теми 7. Сучасні засоби інспекції потоків даних	0,5	1
8	До теми 8. Мультиагентні системи захисту інформації	0,25	0,5
Усього годин за модуль 1		3	5

№ з/п	Назва теми	Кількість годин	
		Д.Ф.Н	З.Ф.Н.
М2			
9	До теми 9. Сучасні засоби моделювання комп'ютерних мереж	0,5	4
10	До теми 10. Програмні засоби створення захищених розподілених систем під Linux	0,5	4
11	До теми 11. Сучасні мережеві протоколи	0,25	3
12	До теми 12. Мережеве обладнання TP-Link і Cisco	0,25	3
13	До теми 13. Рекомендації Cert-UA щодо захисту інформації в комп'ютерних мережах	0,5	4
14	До теми 14. Tor	0,5	4
15	До теми 15. Проблеми захисту інформації при застосуванні WI-Fi і BlueTooth	0,5	4
Усього годин за модуль 2		3	26
Разом		6	31

Розподіл годин підготовки самостійної роботи

№	Вид роботи	Кількість годин	
		Денна форма навчання	Заочна форма навчання
М1			
1	Підготовка до лекцій	4	1
2	Підготовка до лабораторних робіт	8	10
3	Підготовка до модульних контрольних робіт	30	30
4	Самостійне опрацювання окремих тем навчальної дисципліни	3	5
5	Підготовка до екзамену	15	30
Усього годин за модуль 1		60	76
М2			
1	Підготовка до лекцій	4	4
2	Підготовка до лабораторних робіт	22	12
3	Підготовка до модульних контрольних робіт	16	30
4	Самостійне опрацювання окремих тем навчальної дисципліни	3	26
5	Підготовка до екзамену	15	30
Усього годин за модуль 2		60	102

№	Вид роботи	Кількість годин	
		Денна форма навчання	Заочна форма навчання
М3			
1	Підготовка до лекцій	4	4
2	Підготовка до лабораторних робіт	7	14
3	Підготовка до модульних контрольних робіт	4	16
4	Підготовка до екзамену	15	15
Усього годин за модуль 3		30	49
М4			
1	Курсова робота	90	90
Усього годин за модуль 4		90	90
Разом за курсом		240	317

Індивідуальне науково-дослідне завдання

Індивідуальне навчально-дослідне завдання (ІНДЗ) виконується здобувачем під керівництвом викладача і полягає у виконанні курсової роботи у шостому семестрі.

Індивідуальні завдання на курсову роботу видаються студентам на другому тижні шостого семестру.

Виконання курсової роботи створює умови для якнайповнішої реалізації творчих можливостей студентів і має на меті поглиблення, узагальнення та закріплення знань, які здобувачі одержують у процесі навчання, а також застосування знань на практиці.

Індивідуальні завдання виконуються самостійно і не входять до тижневого аудиторного навантаження здобувача. Викладач контролює виконання індивідуального завдання на консультаціях. Студент несе особисту відповідальність за прийняті в роботі рішення і правильність виконання і оформлення роботи.

Курсова робота складається з розрахунково-пояснювальної записки та графічної частини (остання - на аркушах формату А3 або А4). Тематика та зміст курсової роботи спрямовані на здобуття студентами практичних навичок розрахунку та побудови захищених локальних мереж із виходом в Інтернет на базі стандартних апаратних і програмних засобів. Основою для курсової роботи слугує лекційний матеріал, нормативно-правова база захисту інформації в телекомунікаційних системах і мережах, поточний стан якої визначається сайтом Державної служби спеціального зв'язку та захисту інформації, а також будівельні креслення об'єкта інформаційної діяльності, функціональні вимоги

до розроблюваної телекомунікаційної мережі та характеристика інформації, що циркулює в системі.

Індивідуальне завдання курсової роботи може бути пов'язане з тематикою наукової діяльності студента.

Метою курсової роботи є розробка захищеної телекомунікаційної мережі для заданого об'єкта інформаційної діяльності.

Робота полягає у формуванні опису об'єкта інформаційної діяльності; визначенні нормативно-правової бази розробки; розробці структури і виборі устаткування підмереж; виборі устаткування і його розміщення для об'єднання підмереж і для забезпечення виходу в Internet, підтверджених розрахунками; обґрунтуванні вибору операційних систем і апаратно-програмних засобів захисту інформації; розрахунку вартості розробленої мережі.

До складу курсової роботи входять зміст, вступ, основна частина, висновки, перелік посилань та графічна частина, оформлені згідно з вимогами ЄСКД й іншими нормативними документами і виконані студентом у відповідності до індивідуального завдання.

В курсовій роботі мають бути продемонстровані системний підхід до розв'язку задачі та відповідність знань та вмінь студента з дисципліни "Безпека інформаційних та комунікаційних систем" вимогам даної робочої програми.

Тематика курсових робіт:

1. Розробка системи захисту інформаційних ресурсів кафедри.
2. Розробка системи захисту локальної мережі інституту.
3. Розробка системи захисту локальної мережі університету.
4. Розробка захищеної локальної мережі фірми, що має ліцензію на надання послуг в галузі інформаційної безпеки.
5. Розробка захищеної локальної мережі медичної установи.
6. Розробка захищеної локальної мережі районного суду.
7. Розробка захищеної локальної мережі судноплавної компанії.
8. Розробка системи захисту локальної мережі порту.
9. Розробка захищеної телекомунікаційної системи судна.
10. Розробка захищеної кампусної мережі.
11. Розробка захищеної системи IP-телефонії кафедри.
12. Розробка захищеної системи IP-телефонії інституту.
13. Розробка захищеної системи IP-телефонії університету.
14. Розробка захищеної системи IP-телефонії фірми, що має ліцензію на надання послуг в галузі інформаційної безпеки.
15. Розробка захищеної системи IP-телефонії медичної установи.
16. Розробка захищеної системи IP-телефонії районного суду.
17. Розробка захищеної системи IP-телефонії судноплавної компанії.
18. Розробка захищеної системи IP-телефонії порту.
19. Розробка захищеної телекомунікаційної системи судна.
20. Розробка захищеної системи IP-телефонії кампуса.
21. Модернізація системи контролю доступу до інформаційних ресурсів кафедри.

22. Модернізація системи контролю доступу до локальної мережі інституту.
23. Модернізація системи контролю доступу до локальної мережі університету.
24. Модернізація комп'ютерного класу.
25. Дослідження захищеності пристрою мобільного зв'язку.
26. Дослідження захищеності інформаційних ресурсів кафедри.
27. Дослідження захищеності локальної мережі інституту.
28. Дослідження захищеності локальної мережі університету.
29. Дослідження захищеності кампусної мережі.
30. Розробка системи захисту сайту кафедри.
31. Розробка системи захисту інтернет-магазину.
32. Розробка захищеної системи автоматизованого документообігу вузу.
33. Дослідження ефективності захисту електронної пошти від спаму.
34. Дослідження ефективності антивірусного захисту.
35. Виявлення вразливостей захищеної телекомунікаційної системи.

6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування

Здобувач зобов'язаний вивчити теоретичний матеріал та здобути практичні навички у відповідності до тематичного плану навчальної дисципліни.

Методами навчання є:

- пояснення, демонстрування;
- лекція; відеометод;
- робота з літературою;
- лабораторна робота;
- інструктаж (інструктаж з техніки безпеки та пожежної безпеки проводиться одноразово на першому занятті в лабораторії);
- репродуктивний метод;
- проблемного викладу.

При вивченні дисципліни використовуються 3 групи методів навчання:

I група методів - методи організації та здійснення навчально-пізнавальної діяльності:

- словесні: розповідь-пояснення, лекція;
- наочні: ілюстрація, презентація, демонстрація;
- практичні: лабораторні роботи;
- індуктивні методи: узагальнення, пов'язані із проведенням експериментів;
- дедуктивні методи: розвиток абстрактного мислення для засвоєння навчального матеріалу на основі узагальнень;
- репродуктивні методи: робота за готовими прикладами;
- творчі, проблемно-пошукові методи: самостійна, творча пізнавальна діяльність;
- навчальна робота студентів під керівництвом НПП;

– самостійна робота студентів.

II група методів - методи стимулювання й мотивації навчально-пізнавальної діяльності:

– методи стимулювання інтересу до навчання: створення ситуації інтересу при викладанні матеріалу; аналіз життєвих ситуацій;

– методи стимулювання обов'язку й відповідальності: роз'яснення мети навчального предмета; вимоги до вивчення предмета; заохочення та покарання в навчанні;

III група методів - методи контролю (самоконтролю, взаємоконтролю), корекції (самокорекції, взаємокорекції) за ефективністю навчально-пізнавальної діяльності:

Засобами оцінювання результатів навчання є:

- модульні контрольні роботи;
- звіти з лабораторних робіт;
- командні проєкти; індивідуальні та групові завдання;
- завдання на лабораторному обладнанні;
- захист курсового проєкту;
- екзаменаційна робота;
- комплексна контрольна робота (за необхідністю).

Методами демонстрування результатів навчання є:

- усні відповіді;
- письмові відповіді;
- виконання завдань із застосуванням комп'ютерної техніки;
- оформлення звітів з лабораторних робіт;
- презентації результатів виконаних завдань та досліджень.

Допускається застосування дистанційних технологій для діагностики результатів навчання.

7. Форми поточного та підсумкового контролю

Досягнення здобувача вищої освіти оцінюються за 100-бальною системою Університету.

Поточний контроль проводиться в межах навчальних занять і передбачає оцінювання теоретичної підготовки здобувачів вищої освіти із зазначених тем (у тому числі, самостійно опрацьованого матеріалу) та практичних навичок, набутих під час виконання лабораторних робіт.

Поточний контроль здійснюється протягом семестру в наступних формах:

- перевірка екзаменаційних робіт;
- перевірка та захист звітів з лабораторних робіт;
- проведення та перевірка модульних контрольних робіт;
- контроль виконання розділів індивідуального науково-дослідного завдання;
- контрольна робота на заочній формі навчання;
- семестрова атестація;

- перевірка конспекту лекцій;
- контроль відвідування занять.

Перевірка звіту з лабораторної роботи включає оцінювання правильності та повноти виконання завдання, правильності та повноти висновків, правильності оформлення звіту.

Процедура захисту звіту з лабораторної роботи включає один або декілька елементів:

- письмове викладення відповідей на запитання за тематикою роботи;
- усне опитування за тематикою роботи;
- виконання завдань із застосуванням комп'ютерної техніки.

При виконанні модульних контрольних робіт здобувач вищої освіти відтворює засвоєні знання шляхом надання письмових відповідей на поставлені запитання. На теоретичні запитання необхідно давати розгорнуті відповіді, супроводжуючи їх прикладами та ілюстраціями. Повнота відповідей оцінюється згідно з теоретичним матеріалом, наведеним у джерелах інформації для кожної теми. На тестові запитання потрібно вказати номер правильної відповіді та її формулювання.

Контрольна робота на заочній формі навчання за змістом є об'єднаним представленням модульних контрольних робіт, які проводяться для здобувачів денної форми навчання, і має відповідати тим самим вимогам. Контрольна робота на заочній формі навчання виконується протягом семестру і здається до проведення підсумкового контролю.

Поточний модульний контроль проводиться з урахуванням даних поточного контролю за відповідний змістовний модуль і має на меті оцінку результатів знань студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля.

Процедура захисту звіту з індивідуального науково-дослідного завдання (курсового проекту) включає наступні елементи:

- надання пояснювальної записки звіту з індивідуального науково-дослідного завдання (курсового проекту) в електронному вигляді;
- усне опитування за тематикою роботи;
- виконання завдань із застосуванням комп'ютерної техніки.

Семестрова атестація дає змогу здійснити проміжну оцінку досягнень здобувача вищої освіти. В період семестрової атестації викладач оцінює результати поточного контролю та атестує чи не атестує здобувача вищої освіти.

За рішенням кафедри студентам, які брали участь у науково-дослідній роботі – роботі конференцій, студентських наукових гуртків, підготовці публікацій, а також були учасниками олімпіад, конкурсів, тощо можуть присуджуватися додаткові бали. Додаткові бали також можуть присуджуватися за результатами перевірки конспекту лекцій, контролю відвідування занять та за активність на лекціях і практичних заняттях.

За всі поточні контрольні заходи протягом семестру, з урахуванням додаткових балів, студент сумарно може отримати від 0 до 100 балів.

Умовою допуску студента до семестрового підсумкового контролю є мінімальна сума у 60 балів, яку студент повинен набрати у разі виконання всіх елементів модулів.

Семестровий підсумковий контроль з дисципліни проводиться відповідно до навчального плану у вигляді **екзамену** в терміни, встановлені графіком навчального процесу, та в обсязі навчального матеріалу, визначеному робочою програмою навчальної дисципліни.

Студент, який набрав за всі поточні контрольні заходи менше 60 балів або хоче отримати додаткові бали, пише семестрову екзаменаційну роботу (проводиться у письмовій формі), до якої він допускається, якщо захистив курсову роботу і має за виконання всіх передбачених елементів модулів не менше 35 балів. Максимальна кількість балів за семестрову підсумкову залікову роботу (екзамен) становить 30 балів. Студенти заочної форми навчання пишуть підсумкову залікову роботу обов'язково.

Підсумкова оцінка з дисципліни від 60 до 100 балів визначається як сума балів за змістовими модулями та семестрової залікової роботи (у разі її написання).

Зарахування кредитів навчального курсу можливо тільки після досягнення результатів, запланованих РПНД, що виражається в одній з позитивних оцінок, передбачених чинним законодавством.

8. Критерії оцінювання результатів навчання

8.1 Критерії оцінювання лабораторних робіт

При оцінюванні лабораторних робіт враховуються наступні критерії:

- виконання роботи та правильність виконання;
- наявність звіту, вчасність подачі та якість звіту;
- захист звіту.

Максимальна оцінка за кожну лабораторну роботу для ДФН у четвертому семестрі – 5 балів, у п'ятому семестрі – 2 бали, у шостому семестрі – 7 балів.

Максимальна оцінка за кожну лабораторну роботу для ЗФН у четвертому і п'ятому семестрах – 6 балів, у шостому семестрі – 7 балів.

Максимальна сумарна кількість балів за лабораторні роботи для студентів ДФН становить:

- у четвертому семестрі: $8 \times 5 = 40$ балів;
- у п'ятому семестрі: $22 \times 2 = 44$ бали;
- у шостому семестрі: $6 \times 7 = 42$ бали.

Максимальна сумарна кількість балів за лабораторні роботи для студентів ЗФН становить:

- у четвертому семестрі: $5 \times 6 = 30$ балів;
- у п'ятому семестрі: $5 \times 6 = 30$ балів;
- у шостому семестрі: $6 \times 7 = 42$ бали.

Критерії оцінювання лабораторних робіт

Кількість балів (в дужках для ЗФН)	Критерії оцінювання
М1	
5 (6)	Роботу виконано самостійно, завдання виконано правильно. Звіт здано у встановлений термін, оформлення звіту повністю відповідає вимогам, у висновках проведено коректну інтерпретацію результатів. Студент надав правильні відповіді на всі питання захисту.
4 (5)	Робота виконана правильно з консультаціями викладача. Звіт здано у встановлений термін, можливі несуттєві помилки в оформленні звіту та незначні некоректності у висновках. Студент надав принципово правильні відповіді на питання захисту (без суттєвих помилок).
3 (4)	Роботу виконано із підказками викладача та незначними помилками. Звіт містить неточності у висновках та окремі помилки. Студент відповів на питання захисту частково чи з принциповими помилками.
2 (3)	Завдання виконано у повному об'ємі але з помилками. Звіт містить неточності у висновках та окремі помилки. Студент не відповів на питання захисту.
1 (1)	Завдання виконано не у повному об'ємі (не менше 70%). Надано звіт, що містить неточності і помилки. Студент не відповів на питання захисту.
0 (0)	Робота не виконана.
<i>Максимальна сумарна оцінка студента за даний компонент програми для ДФН – 40 балів (8 робіт по 5 балів). Максимальна сумарна оцінка студента за даний компонент програми для ЗФН – 30 балів (5 робіт по 6 балів). При незначних відхиленнях від вказаних критеріїв оцінка може доповнюватись знаками «-» або «+», що при підсумовуванні відповідає 0,5 бала.</i>	
М2	
2 (6)	Роботу виконано самостійно, завдання виконано правильно. Звіт здано у встановлений термін, оформлення звіту повністю відповідає вимогам, у висновках проведено коректну інтерпретацію результатів. Студент надав правильні відповіді на всі питання захисту.
1,6 (5)	Робота виконана правильно з консультаціями викладача. Звіт здано у встановлений термін, можливі несуттєві помилки в оформленні звіту та незначні некоректності у висновках. Студент надав принципово правильні відповіді на питання захисту (без суттєвих помилок).
1,2 (4)	Роботу виконано із підказками викладача та незначними помилками. Звіт містить неточності у висновках та окремі помилки. Студент відповів на питання захисту частково чи з принциповими помилками.
0,8 (3)	Завдання виконано у повному об'ємі але з помилками. Звіт містить неточності у висновках та окремі помилки. Студент не відповів на питання захисту.
0,4 (1)	Завдання виконано не у повному об'ємі (не менше 70%). Надано звіт, що містить неточності і помилки. Студент не відповів на питання захисту.
0 (0)	Робота не виконана.
<i>Максимальна сумарна оцінка студента за даний компонент програми для ДФН – 44 балів (22 роботи по 2 бали). Максимальна сумарна оцінка студента за даний компонент програми для ЗФН – 30 балів (5 робіт по 6 балів). При незначних відхиленнях від вказаних критеріїв оцінка може доповнюватись знаками «-» або «+», що при підсумовуванні відповідає 0,2 бала.</i>	

Кількість балів (в дужках для ЗФН)	Критерії оцінювання
МЗ	
7 (7)	Роботу виконано самостійно, завдання виконано правильно. Звіт здано у встановлений термін, оформлення звіту повністю відповідає вимогам, у висновках проведено коректну інтерпретацію результатів. Студент надав правильні відповіді на всі питання захисту.
6	Робота виконана правильно з консультаціями викладача. Звіт здано у встановлений термін, можливі несуттєві помилки в оформленні звіту та незначні некоректності у висновках. Студент надав принципово правильні відповіді на питання захисту (без суттєвих помилок).
5	Роботу виконано із підказками викладача та незначними помилками. Звіт містить неточності у висновках та окремі помилки. Студент відповів на питання захисту частково чи з принциповими помилками.
2	Завдання виконано у повному об'ємі але з помилками. Звіт містить неточності у висновках та окремі помилки. Студент не відповів на питання захисту.
1	Завдання виконано не у повному об'ємі (не менше 70%). Надано звіт, що містить неточності і помилки. Студент не відповів на питання захисту.
0	Робота не виконана.
<i>Максимальна сумарна оцінка студента за даний компонент програми – 40 балів (8 робіт по 5 балів). При незначних відхиленнях від вказаних критеріїв оцінка може доповнюватись знаками «-» або «+», що при підсумовуванні відповідає 0,5 бала.</i>	

8.2 Критерії оцінювання модульних контрольних робіт

Для поточного модульного контролю студентами виконуються 6 (шість) модульних контрольних роботи за матеріалами змістовних модулів.

Критерієм оцінювання МКР є відсоток правильних відповідей на питання МКР.

Максимальна кількість балів за кожну МКР для студентів ДФН:

- у четвертому семестрі: 10 балів;
- у п'ятому семестрі: 8 балів;
- у шостому семестрі: 9 балів.

Загальна сума балів за модульні контрольні роботи для студентів ДФН:

- у четвертому семестрі: $2 \times 10 = 20$ балів;
- у п'ятому семестрі: $2 \times 8 = 16$ балів;
- у шостому семестрі: $2 \times 9 = 18$ балів.

Максимальна кількість балів за кожну МКР для студентів ЗФН:

- у четвертому семестрі: 15 балів;
- у п'ятому семестрі: 15 балів;
- у шостому семестрі: 9 балів.

Загальна сума балів за модульні контрольні роботи для студентів ЗФН:

- у четвертому семестрі: $2 \times 15 = 30$ балів;
- у п'ятому семестрі: $2 \times 15 = 30$ балів;
- у шостому семестрі: $2 \times 9 = 18$ балів.

Критерії оцінювання задач та практичних завдань в МКР для ДФН

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Бал (М1)	10	9	8	7	6	5	4	3	2	1
Бал (М2)	2	1,8	1,6	1,4	1,2	1,0	0,8	0,6	0,4	0,2
Бал (М3)	7	6,3	5,6	4,9	4,2	3,5	2,8	2,1	1,4	0,7

Критерії оцінювання задач та практичних завдань в МКР для ЗФН

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Бал (М1)	15	13,5	12	10,5	9	7,5	6	4,5	3	1,5
Бал (М2)	15	13,5	12	10,5	9	7,5	6	4,5	3	1,5
Бал (М3)	7	6,3	5,6	4,9	4,2	3,5	2,8	2,1	1,4	0,7

8.3 Критерії оцінювання курсової роботи

Критеріями оцінювання курсової роботи є:

- самостійність виконання завдання;
- правильність виконання завдання;
- вчасність оформлення звіту з курсової роботи;
- правильність оформлення звіту з курсової роботи;
- правильність відповідей на питання при захисті курсової роботи.

Максимальна кількість балів за курсову роботу становить 100 балів.

Розподіл максимально можливої кількості балів за курсову роботу

Звіт з курсової роботи	Захист курсової роботи	Сума
50	50	100

Критерії оцінювання пояснювальної записки і графічної частини курсової роботи

виконання роботи, %	Критерії оцінювання пояснювальної записки і графічної частини курсової роботи	бал
100	Роботу виконано самостійно, завдання виконано правильно. Звіт здано у встановлений термін, оформлення звіту повністю відповідає вимогам, у висновках проведено коректну інтерпретацію результатів. Графічна частина виконана відповідно до вимог.	50
70 - 99	Робота виконана правильно з консультаціями викладача. Звіт здано у встановлений термін, можливі несуттєві помилки в оформленні звіту та незначні некоректності у висновках і/або у графічній частині курсової роботи.	40
59 - 69	Роботу виконано із підказками викладача та незначними помилками. Звіт містить неточності у висновках та окремі помилки. Графічна частина містить незначні некоректності в оформленні.	30

виконання роботи, %	Критерії оцінювання пояснювальної записки і графічної частини курсової роботи	бал
40 - 58	Завдання виконано у повному об'ємі але з помилками. Звіт (в тому числі графічна частина) містить неточності у висновках та окремі помилки.	20
20 - 39	Завдання виконано не у повному об'ємі. Надано звіт, що містить неточності і помилки. Графічна частина містить помилки.	10
1 - 20	Робота не виконана.	0

Критерії оцінювання захисту курсової роботи

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Бал	50	45	40	35	30	25	20	15	10	5

8.4 Критерії оцінювання екзаменаційної роботи

Максимальна оцінка за екзаменаційні роботи – 40 балів.

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Бал	40	36	32	28	24	20	16	12	8	4

Рівні підсумкової оцінки екзамену з дисципліни (перерахунковий коефіцієнт – 0,4)

Оцінка за 100-бальною шкалою університету / Grade according to 100-points scale of University	Оцінка за шкалою ЄКТС / Grade according to ECTS scale
90-100 (творчий рівень)/(creative level)	A (відмінно) / (excellent)
82-89 (високий рівень)/(high level)	B (дуже добре) / (very good)
74-81 (добрий рівень)/(good level)	C (добре) / (good)
64-73 (середній рівень)/(average level)	D (посередньо) / (average)
60-63 (задовільний рівень)/(satisfactory level)	E (достатньо) / (satisfactory)
35-59 (низький рівень)/(low level)	FX (незадовільно з можливістю повторного складання) / (unsatisfactory with the possibility to repass the exam)
1-34 (незадовільний рівень)/(unsatisfactory level)	F (незадовільно з обов'язковим повторним вивченням) / (unsatisfactory with the compulsory repeating of the course)

8.5 Розподіл балів

Розподіл оцінки за змістовними модулями та видами контролю

		Денна форма		Заочна форма	
		Вид роботи	Кількість балів	Вид роботи	Кількість балів
М1					
ЗМ1	T1	Лабораторна робота 1	5	-	--
	T2	-	-	-	
	T3	-	-	-	-
	T4	Лабораторна робота 2	5	Лабораторна робота 2	6
	МКР1	Тест	10	Тест	15
ЗМ2	T5	-	-	-	-
	T6	Лабораторні роботи 3, 4, 5, 6, 7	25	Лабораторні роботи 3, 5, 7	18
	T7	Лабораторна робота 8	5	Лабораторна робота 8	6
	T8	-	-	-	-
	МКР2	Тест	10	Тест	15
Підсумковий семестровий контроль		екзамен	40	екзамен	40
Всього			100	100	
М2					
ЗМ3	T9	Лабораторні роботи 9, 10	4		
	T10	Лабораторна робота 11	2		
	T11	Лабораторні роботи 12, 13, 14	6	Лабораторна робота 12	6
	МКР3	Тест	8	Тест	15
ЗМ4	T12	Лабораторні роботи 15, 16, 17, 18	8	Лабораторна робота 16	6
	T13	Лабораторні роботи 19, 20, 21	6	Лабораторна робота 20	6
	T14	Лабораторні роботи 22, 23, 24	6	Лабораторна робота 22	6
	T15	Лабораторні роботи 25, 26, 27, 28, 29, 30	12	Лабораторна робота 30	6
	МКР4	Тест	8	Тест	15
Підсумковий семестровий контроль		екзамен	40	екзамен	40
Всього			100	100	
М3					
ЗМ5	T16	Лабораторна робота 31	7	Лабораторна робота 31	7
	T17	Лабораторна робота 32	7	Лабораторна робота 32	7

		Денна форма		Заочна форма	
		Вид роботи	Кількість балів	Вид роботи	Кількість балів
	T18	Лабораторна робота 33	7	Лабораторна робота 33	7
	МКР5	Тест	9	Тест	9
ЗМ6	T19	Лабораторна робота 34	7	Лабораторна робота 34	7
	T20	Лабораторна робота 35	7	Лабораторна робота 35	7
	T21	Лабораторна робота 36	7	Лабораторна робота 36	7
	T22	Лабораторна робота 37	7	Лабораторна робота 37	7
	МКР6	Тест	9	Тест	9
	Підсумковий семестровий контроль	екзамен	40	екзамен	40
Всього			100	100	
М4					
Курсова робота		звіт	100	звіт	100
Всього			100		100

9. Засоби навчання

Апаратне забезпечення, необхідне для вивчення навчальної дисципліни, включає персональний комп'ютер (настільний або ноутбук) та спеціалізовані лабораторні стенди із доступом до Інтернет.

Програмне забезпечення, необхідне для вивчення навчальної дисципліни, включає операційні системи (Windows, Linux, Kali Linux), спеціалізоване програмне забезпечення для захисту комп'ютерних мереж (брандмауери, антивірусні програми, засоби боротьби із спамом, Honeypot, експлойти, утиліти моніторингу трафіку, утиліти виявлення вразливостей, системи виявлення вторгнень, системи запобігання вторгненням, системи SIEM), спеціалізоване програмне забезпечення для інженерних розрахунків та моделювання технічних засобів, текстовий процесор та редактор растрових зображень (для підготовки звітів з практичних робіт); pdf-, djv-переглядач (для ознайомлення з джерелами інформації, представленими в електронному виді).

Використовуються апаратні та програмні можливості лабораторії №130, кафедри КТІБ ННІАЕ НУК.

10. Рекомендовані джерела інформації

Основна література

Навчально-методична література

1. Бабак В.П., Ключников А.А. Теоретические основы защиты информации: учебник / В.П. Бабак, А.А. Ключников; НАН Украины, Ин-т проблем безопасности АЭС. - Чернобыль (Киев.обл.) : Ин-т проблем безопасности АЭС, 2012. - 776 с.

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

3. Бурячок В. Л., Толубко В.Б., Хорошко В. О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект. [Підручник]. / В. Л. Бурячок, В.Б. Толубко, В. О. Хорошко, С.В. Толюпа. – Львів. : «Магнолія 2006», 2018. – 320 с.

4. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група ВНУ, 2009. – 608 с.

5. Жилін А. В. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

6. Конахович Г.Ф., Климчик В.П., Паук С.М., Потапов В.Г. Защита информации в телекоммуникационных системах.- К.: МК-Пресс, 2005. – 288 с.

Нормативно-правова база

Закони України:

7. Доктрина інформаційної безпеки України : Указ Президента України від 25.02.2017 р. № 47/2017 // Офіційний вісник Президента України. – 2017. – № 5. – С. 15. – Ст. 102. <https://www.president.gov.ua/documents/472017-21374>

8. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»/ URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>

9. Закон України “Про основні засади забезпечення кібербезпеки України». URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

10. Стратегія кібербезпеки України : Указ Президента України від 15.03.2016 р. № 96/2016// Офіційний вісник України. – 2016. – № 23. – С. 69. – Ст. 899. <https://zakon.rada.gov.ua/laws/show/96/2016#Text>

Нормативні документи системи ТЗІ:

11. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 № 22

12. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 № 22 (Зміна № 1 наказ від 28.12.2012 № 806)

13. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 № 22 (Зміна № 1 наказ від 15.10.2008 № 172)

Постанови кабінету міністрів України

14. Порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, затверджений постановою №1295 Кабінету міністрів України 23.12.2020. URL: <https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF>

15. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29.03.06 № 373

Допоміжна література

Навчально-методична література

16. Бабак В.П. Теоретичні основи захисту інформації: Підручник.- К.: Книжкове вид-во НАУ, 2008.- 752 с.

17. Богуш В.М., Довидьков О.А., Кривуца В.Г. Теоретичні основи захищених інформаційних технологій. Навч. посібник. – К.: ДУІКТ, 2010. – 454 с.

18. 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.

19. Бурячок В. Л., Козачок В.А., Бурячок Л.В., Складанний П.М. Пентестінг як інструмент комплексної оцінки ефективності захисту інформації в розподілених корпоративних мережах // Сучасний захист інформації. – 2015. - №3. – С.4-12.

20. Васильцов І.В. Атаки спеціального виду на криптопристрої та методи боротьби з ними. – Кременець: Видавничий центр КОГПІ, 2009.- 294.с.

21. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник.– К.: Видавництво НА СБ України, 2020. – 256 с. URL: http://www.immsp.kiev.ua/postgraduate/Biblioteka_trudy/Gulak_MetodolZahystuInfOsnKiberbezp_2020.pdf.

22. Гундарь К.Ю. и др. Защита информации в компьютерных системах. - К.: Корнійчук, 2000.-149 с.

23. Гурокій А.М., Коряк С.Ф., Самсонов В.В., Склярів О.Я. Контроль та керування корпоративними комп'ютерними мережами: інструментальні засоби та технології. -Х.: Компанія СМІТ, 2004.-544 с.

24. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. -К.: ОО Гид "ДС", 2000.-688 с.

25. Дудатьєв А. В. Захист комп'ютерних мереж. Теорія та практика. Навчальний посібник / Дудатьєв А. В., Войтович О. П., Каплун В. А. – Вінниця ВНТУ, 2010. – 219 с.

26. Єсін В. І., Кузнецов О. О., Сорока Л. С. Безпека інформаційних систем і технологій : навчальний посібник [для студентів вищих навчальних закладів, які навчаються за напрямами підготовки «Безпека інформаційних і комунікаційних систем»]. – Х. : ХНУ імені В. Н. Каразіна, 2013. – 632 с.

27. Жуков И.А., Ластовченко М.М. Основы сетевых технологий.- К.: «МК-Прес», 2007. – 432 с.

28. Карачка А.Ф. Технології захисту інформації. Текст лекцій. – Тернопіль: ТНЕУ, 2017. – 86 с.

29. Команда реагування на комп'ютерні надзвичайні події України: URL: <https://cert.gov.ua/>

30. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: Навчальний посібник / В. Д. Козюра, В. О. Хорошко, М. Є. Шелест, Ю. М. Ткач, Я.Ю. Усов. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2019. – 144 с.

31. Піскозуб А.З. Використання тестування на проникнення в комп'ютерні мережі та системи для підняття їх рівня захищеності // Вісник Національного університету "Львівська політехніка". Сер. : Автоматика, вимірювання та керування. - 2013. - № 753. - С. 149-152. - URL: http://nbuv.gov.ua/UJRN/VNULP_2013_753_26/

32. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних.– К.: Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009.–716 с.

33. Kali Linux. URL: <http://www.kali.org/>

34. Microsoft Corporation. Microsoft Internet Security and Acceleration Server 2000: Учебный курс MCSE /Пер. с англ. -М.: изд.-торг.дом “Русская редакция”, 2002.-544 с.

35. SNARE. [URL]: <http://snare.readthedocs.io/>

Нормативно-правова база

Закони України:

36. Про кіберзлочинність : Конвенція Ради Європи від 23.11.01 р. № 994-575. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

Нормативні документи системи ТЗІ:

37. НД ТЗІ 1.1-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. -К.:ТОВ “НікС”, 1999.

38. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. -К.:ТОВ “НікС”, 1999.

39. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час обробки в автоматизованих системах класу 2, наказ ДСТСЗІ СБУ від 13.12.2002 № 84 (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806)

40. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB – сторінки від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 02.04.2003 № 33 (Зміна № 1 наказ від 28.12.2012 № 806).

41. Р–СП Рекомендації з технічного захисту інформації в приміщеннях серверних, електронної пошти та інших спеціальних приміщень. - К.:ТОВ “НікС”, 2003.

Інформаційні ресурси в Інтернеті

1. Верховна Рада України. Законодавство України.
URL: <http://zakon.rada.gov.ua/laws/>
2. Державна служба спеціального зв'язку та захисту інформації.
URL: <https://cip.gov.ua/ua>
3. Команда реагування на комп'ютерні надзвичайні події України.
URL: <https://cert.gov.ua/>
4. Портал безпека. URL: <https://www.bezpeka.com/uk/golovna/>
5. Системи онлайн-освіти. URL: <https://prometheus.org.ua/>,
<https://www.coursera.org>, <http://www.udacity.com>
6. Офіційні сайти: Kali Linux. <http://www.kali.org/>, SNARE. URL: <http://snare.readthedocs.io/>

Зміни та доповнення