

# ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій  
Кафедра кібербезпеки



ЗАТВЕРДЖУЮ

Декан ФІТ

Тетяна ГОВОРУЩЕНКО

2024 р.

## СИЛАБУС

Навчальна дисципліна: «Технології та системи захисту інформації»

Освітньо-професійна програма: «Кібербезпека та захист інформації»

Рівень вищої освіти: другий (магістерський)

### Загальна інформація

Позиція	Інформація
Викладач(і)	Чешун Віктор Миколайович
Профайл викладача(ів)	<a href="https://kb.khmnu.edu.ua/sklad-kafedry/">https://kb.khmnu.edu.ua/sklad-kafedry/</a>
E-mail викладача(ів)	<a href="mailto:cheshunvn@khmnu.edu.ua">cheshunvn@khmnu.edu.ua</a>
Контактний телефон	Наявний в ІСУ
Сторінка дисципліни в ІСУ	<a href="https://msn.khnu.km.ua/course/view.php?id=8037">https://msn.khnu.km.ua/course/view.php?id=8037</a>
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: <a href="https://us04web.zoom.us/j/3927472324">https://us04web.zoom.us/j/3927472324</a> * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2024-2025, семестр II (зимово-весняний)
Консультації	Очні: згідно графіку консультацій Онлайн: за необхідністю та попередньою домовленістю

### Характеристика дисципліни

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин							Форма семестрового контролю		
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, у т.ч. ІРС	Курсовий проект			Курсова робота
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття						
ОД	1	2	5	150	54	18	36	-	-	96	-	-	-	+

### Анотація дисципліни

Дисципліна викладається для студентів денної форми навчання спеціальності «Кібербезпека та захист інформації». При викладанні дисципліни використовуються наступні форми (методи) навчання: словесні та наочні (лекції); практичні та частково-пошукові (лабораторні роботи); пояснювально-ілюстративні та дослідницькі (самостійна робота).

**Пререквізити** – моніторинг та менеджмент інформаційної безпеки, методологія організації атак та тестування на проникнення

**Кореквізити** – професійна практика.

## **Мета і завдання дисципліни**

**Метою викладання** навчальної дисципліни є формування у майбутніх спеціалістів умінь та компетенцій для розробки та проєктування захищених інформаційно-комунікаційних систем; розробки, впровадження та використання методів та засобів технічного захисту інформації; систем управління доступом до інформаційних ресурсів; для планування навчання, контролю та супроводу роботи з персоналом.

**Предметом дисципліни** є сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); програмне та програмно-апаратне забезпечення (засоби) кіберзахисту.

**Завданням дисципліни** є забезпечити набуття компетентностей та досягнення програмних результатів навчання відповідно до освітньо-професійної програми підготовки магістрів зі спеціальності «Кібербезпека та захист інформації»:

### **компетентності:**

КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

### **результати навчання:**

РН3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та/або кібербезпеки.

Студент, який успішно завершив вивчення дисципліни, повинен: *проводити* дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного захисту інформації у кіберпросторі; *досліджувати, розробляти* і *супроводжувати* системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах

інформаційної діяльності та критичної інфраструктури; *аналізувати, контролювати та забезпечувати* ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації; *досліджувати, розробляти, впроваджувати та використовувати* методи та засоби технічного захисту інформації бізнес/операційних процесів; *планувати* навчання, а також *супроводжувати та контролювати* роботу з персоналом у напрямку інформаційної безпеки та/або кібербезпеки.

### Тематичний і календарний план вивчення дисципліни

№ тижня	Тема лекції*	Тема лаб. роботи **	Самостійна робота		
			Зміст	Год.	Література
1	<b>Тема 1. Захист операційних систем</b> Проектування та розробка захищених операційних систем (ОС)	<b>ЛР1.</b> Проектування “довіреної” версії ОС за допомогою антивірусного захисту	Опрацювання теоретичного матеріалу лекції №1.	4	[1] с. 4-156
2	-	<b>ЛР1.</b> Підгрупа 2	Підготовка до виконання лабораторної роботи №1.	4	[22] с. 30-34
3	<b>Тема 2. Захист мережної інфраструктури</b> Концепції та методологія безпеки мережної інфраструктури	<b>ЛР2.</b> Проектування захищеної мережі на основі технології Honeypot	Опрацювання теоретичного матеріалу лекції №2.	4	[2] с. 8-69, 183-213 [35]
4	-	<b>ЛР2.</b> Підгрупа 2	Підготовка до захисту лабораторної роботи №1. Підготовка до виконання лабораторної роботи №2.	7	[22] с. 30-34 [24] [25] [26]
5	<b>Тема 2. Захист мережної інфраструктури</b> Технології Honeypot та Decerption, DLP-системи	<b>ЛР3.</b> Проектування захищеної мережі на основі технології Decerption	Опрацювання теоретичного матеріалу лекції №3.	4	[4] с. 163-217 [24] [25] [26] [27] [28]
6	-	<b>ЛР3.</b> Підгрупа 2	Підготовка до захисту лабораторної роботи №2. Підготовка до виконання лабораторної роботи №3.	7	[24] [25] [26]
7	<b>Тема 3. Захист веб-ресурсів</b> Проектування та розробка захищених веб-ресурсів	<b>ЛР4.</b> Проектування та дослідження DLP-системи	Опрацювання теоретичного матеріалу лекції №4.	4	[5] [6] [7]

8	-	<b>ЛР4.</b> Підгрупа 2	Підготовка до захисту лабораторної роботи №3. Підготовка до виконання лабораторної роботи №4.	7	[24] [25] [26] [27] [28]
9	<b>Тема 4. Програмно-технічні складові захисту інформації</b> Аутифікація і системи контролю та управління доступом (СКУД)	<b>ЛР5.</b> Забезпечення безпеки багатокомпонентних веб-додатків	Опрацювання теоретичного матеріалу лекції №5.	4	[8] с. 115-140 [9] с. 7-135 [10] [29] [30] [34]
10	-	<b>ЛР5.</b> Підгрупа 2	Підготовка до захисту лабораторної роботи №4. Підготовка до виконання лабораторної роботи №5.	7	[5] [6] [27] [28]
11	<b>Тема 4. Програмно-технічні складові захисту інформації</b> Методи та засоби захисту від витоку інформації.	<b>ЛР6.</b> Проектування системи аутифікації на основі розпізнавання зображень	Опрацювання теоретичного матеріалу лекції №6.	4	[11] с. 17-60 [31] [32]
12	-	<b>ЛР6.</b> Підгрупа 2	Підготовка до захисту лабораторної роботи №5. Підготовка до виконання лабораторної роботи №6.	7	[5] [6] [9] с. 69-87
13	<b>Тема 5. Захист інформації на об'єктах критичної інфраструктури</b>	<b>ЛР7.</b> Проектування системи відеомоніторингу, контролю та управління доступом	Опрацювання теоретичного матеріалу лекції №7.	4	[3] с. 23-52, 61-89 [11] с. 60-81 [13] с. 87-164 [14] с. 9-151 [15] с. 7-54
14	-	<b>ЛР7.</b> Підгрупа 2	Підготовка до захисту лабораторної роботи №6. Підготовка до виконання лабораторної роботи №7.	7	[9] с. 69-87 [10] [23] с. 178-188
15	<b>Тема 6. Організаційно-технічні та режимні заходи захисту інформації</b> Організація режиму та охорони, робота з персоналом	<b>ЛР8.</b> Проектування систем захисту від витоку інформації акустичними каналами та через побічне електромагнітне випромінювання	Опрацювання теоретичного матеріалу лекції №8.	4	[12] с. 159-186, с. 202-214 [16] с. 95-104 [17] с. 7-121 [18] с. 55-149

16	-	ЛР8. Підгрупа 2	Підготовка до захисту лабораторної роботи №7. Підготовка до виконання лабораторної роботи №8.	7	[10] [11] с. 26-60 [23] с. 178-188
17	<b>Тема 7. Комплексне забезпечення інформаційної безпеки</b> Сучасні підходи до побудови систем інформаційної безпеки (СІБ)	-	Опрацювання теоретичного матеріалу лекції №9.	4	[19] с. 103-124, 210-250 [20] с. 500-564 [21] [33] [36]
18	-	Підсумкове заняття <b>Тестування</b>	Підготовка до захисту лабораторної роботи №8. Підготовка до тестування	7	[11] с. 26-60

\* лекції проводяться по 2 години раз на два тижні;

\*\* лабораторні проводяться по 4 години раз в два тижні.

### ПОЛІТИКА ДИСЦИПЛІНИ

Організація освітнього процесу з дисципліни відповідає вимогам положень про організаційне і навчально-методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції і лабораторні заняття згідно з розкладом, не запізнюватися на заняття, вчасно виконувати та здавати лабораторні роботи. Термін виконання лабораторної роботи вважається своєчасним, якщо студент здав/захистив її на поточному або наступному за ним занятті. За несвоєчасний захист лабораторної роботи з набраної студентом суми балів вираховується один бал. Пропущене з поважної причини лабораторне заняття студент повинен відпрацювати у встановлений викладачем термін.

Виконуючи усі навчальні завдання з дисципліни, студент має дотримуватися політики доброчесності. У разі наявності плагіату він отримує незадовільну оцінку і має виконати завдання за новою темою.

Набуті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок визнання та перерахування результатів навчання здобувачів вищої освіти у ХНУ.

### ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ

Оцінювання академічних досягнень студента здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Кожний вид роботи з дисципліни оцінюється за інституційною чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих видів її робіт.

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

	<b>Аудиторна робота</b>	<b>Контрольні заходи</b>	<b>Підсумковий контрольний захід</b>
Вид заняття	Лабораторні роботи	Тестування	Семестровий контроль (іспит)
Тема	1-4	5-7	1-7
Ваговий коефіцієнт	0,4	0,2	0,4

**Оцінювання лабораторних робіт.** Оцінка, яка виставляється за лабораторну роботу, складається з таких елементів: знання теоретичного матеріалу з теми; якість оформлення звіту; вільне володіння студентом спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні рішення; своєчасний захист лабораторної роботи.

Термін захисту звіту з лабораторної роботи вважається своєчасним, якщо студент захистив її в день виконання або на наступному після виконання роботи занятті. Пропущене заняття студент зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін з реєстрацією у відповідному журналі кафедри, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Оцінку за лабораторну роботу викладач оголошує одразу після захисту звіту і проставляє в електронний журнал дисципліни.

**Оцінювання тестових завдань.** Тематичний тест для кожного студента складається з двадцяти тестових завдань, кожне з яких оцінюється одним балом. Максимальна сума балів, яку може набрати студент, складає 20.

**Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту**

Сума балів за тестове завдання	1–10	11–14	15–17	18–20
Оцінка за 4-ри бальною шкалою	2	3	4	5

На тестування відводиться 20 хвилин (для закритої форми тестів – по одній хвилині на кожне завдання). Правильні відповіді студент записує у талоні відповідей. При цьому усі графи для відповідей мають бути заповнені цифрами, що відповідають правильним, на погляд студента, відповідям. Через 20 хвилин студенти здають викладачу завдання з талонами відповідей.

Тестування студент може також пройти і в онлайн режимі в модульному середовищі для навчання MOODLE.

Оцінку за тестування викладач проставляє в електронний журнал дисципліни не пізніше ніж через десять днів після проведення заходу.

**Семестровий контроль (іспит).** Підсумковий контрольний захід з дисципліни проводиться в формі іспиту. Екзаменаційний білет складається з двох теоретичних питань і задачі. Під час іспиту за наданими відповідями і рішеннями (розв'язками) виконується оцінювання рівня засвоєння студентом матеріалу дисципліни.

Оцінка за підсумковий контрольний захід проставляється викладачем в електронний журнал дисципліни в день здачі іспиту і враховується в автоматизованому режимі при визначенні підсумкової семестрової оцінки студента з дисципліни за інституційною шкалою і шкалою ЄКТС

Засвоєння студентом матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями.

### Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	Узагальнений критерій
Відмінно	Студент глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає, логічний виклад відповіді державною мовою (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними інструментами. Студент не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві-три несуттєві похибки.
Добре	Студент виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом і фаховою термінологією, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання закономірностей тощо. Відповідь студента будується на основі самостійного мислення. Студент у відповіді допустив дві-три несуттєві помилки.
Задовільно	Студент виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, допускає неточності і суттєві помилки у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно	Студент виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка "незадовільно" виставляється студенту, який не може продовжити навчання без додаткової роботи з вивчення дисципліни.

Якщо студент отримав негативну оцінку за певним видом робіт, то він має перездати її в установленому порядку, але обов'язково до терміну наступного контролю.

У випадку, коли студент не виконав індивідуальний план з дисципліни у заплановані терміни без поважних причин, то під час відпрацювання заборгованості при позитивній відповіді йому виставляється оцінка «задовільно».

Студент, який у встановлені терміни не виконав індивідуальний план поточної роботи з дисципліни повністю або частково, до здачі підсумкового контрольного заходу не допускається.

Студент, який набрав позитивний середньозважений бал за поточну роботу і не здав підсумковий контрольний захід (іспит), вважається невестигаючим.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

**Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС**

Оцінка ЄКТС	Інституційна інтервальна шкала балів	Інституційна оцінка, критерії оцінювання	
А	4,75–5,00	5	<i><b>Відмінно</b></i> – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
В	4,25–4,74	4	<i><b>Добре</b></i> – повне знання навчального матеріалу з кількома незначними помилками
С	3,75–4,24	4	<i><b>Добре</b></i> – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74	3	<i><b>Задовільно</b></i> – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24	3	<i><b>Задовільно</b></i> – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	2	<i><b>Незадовільно</b></i> – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99	2	<i><b>Незадовільно</b></i> – необхідна серйозна подальша робота і повторне вивчення дисципліни



## ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ ЗДОБУТИХ СТУДЕНТАМИ РЕЗУЛЬТАТІВ НАВЧАННЯ

1. Принципи створення захищених ОС.
2. Розробка захищених ОС “з нуля”.
3. Побудова “довірених” версій шляхом модернізації існуючих ОС.
4. Визначення вимог до архітектури комплексу засобів захисту в залежності від задач, які виконує ОС.
5. Адміністративні заходи захисту ОС.
6. Принципи організації безпеки мережної інфраструктури.
7. Моделі управління мережними ресурсами.
8. Безпека міжмережної взаємодії.
9. Технології побудови захищених корпоративних мереж.
10. Проєктування мереж, включаючи розуміння цілей безпеки, операційних цілей та компромісів між ними.
11. Переваги та недоліки застосування технологій Sandboxing у мережній інфраструктурі.
12. Переваги та недоліки застосування технологій Honeypots та Honeynets у мережній інфраструктурі.
13. Переваги та недоліки застосування технологій Deserption у мережній інфраструктурі.
14. Підвищення мережної безпеки за рахунок впровадження Honeynet- та Deserption-технологій.
15. Аналіз недоліків систем DLP.
16. Методи для підвищення ефективності та законності DLP-систем.
17. Особливості проєктування систем DLP.
18. Архітектура, функціонування та механізми безпеки веб-додатків і веб-серверів.
19. Взаємодія між веб-сервісами як елемент інформаційної безпеки.
20. REST-інтерфейс та його безпека.
21. Особливості застосування баз даних для побудови захищених веб-рішень
22. Відкритий проєкт по забезпеченню безпеки веб-додатків (OWASP).
23. Перспективи організації та виконання тестування рівня безпеки для певного веб-ресурсу.
24. Аналіз існуючих підходів до вирішення задач аутентифікації
25. Біометрична аутентифікація на основі розпізнавання зображень (штучні нейронні та капсульні мережі, алгоритм розпізнавання облич Eigenface та його реалізація).
26. Визначення вимог до СКУД відповідно до політики інформаційної безпеки. Обґрунтування моделі управління доступом.
27. Концепція та етапи створення СКУД. Розробка технічного завдання, проєктування, дослідна експлуатація, супровід.
28. Ідентифікація та дослідження каналів витоку інформації.
29. Організаційно-технічні заходи щодо блокування каналів витоку інформації на об’єкті.
30. Проєктування систем захисту від витоку інформації.
31. Визначення інформації, що потребує захисту на об’єктах критичної інфраструктури (ОКІ).
32. Канали витоку інформації на ОКІ та підстави їх утворення.
33. Засоби та комплекси виявлення прихованого підключення до інформаційних мереж.
34. Види прихованого підключення до інформаційних мереж (радіозакладні пристрої, приховане під’єднання до ліній зв’язку, приховані відеокамери, прихований майнінг тощо).
35. Порядок проведення обстеження і аналізу ОКІ з метою забезпечення захисту інформації.
36. Робота з документами та документованою інформацією.
37. Організація розробки і використання документів та носіїв конфіденційної інформації.
38. Облік документів та документованої інформації.
39. Виконання та повернення документів та документованої інформації.

40. Зберігання і знищення документів та документованої інформації.
41. Використання технічних засобів збору, обробки, накопичення і зберігання конфіденційної інформації.
42. Підбір та розстановка персоналу.
43. Навчання персоналу.
44. Контроль за роботою персоналу.
45. Відповідальність за порушення правил захисту інформації.
46. Програми класифікації інформації організації та процедур компромісу інформації.
47. Інструменти та методи проектування СІБ.
48. Модель можливостей і зрілості (СММІ) при розробці СІБ.
49. Основні принципи побудови сучасних СІБ.
50. Особливості розроблення та реалізації плану безпеки. Керування конфігурацією.

## МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі MOODLE.

## РЕКОМЕНДОВАНА ЛІТЕРАТУРА

### Основна

1. Захищені операційні системи: Конспект лекцій / Ю. В. Баришев, О. В. Дмитришин, В. А. Капун. Вінниця: ВНТУ, 2018. 161 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. Основи інформаційної безпеки: навч. посібник/ В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2020. 128 с.
4. Основи кібербезпеки та кібероборони: підручник/ Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. Одеса.: ОНАЗ ім. О.С. Попова, 2019. 320 с.
5. OWASP Top 10 API Security Risks – 2023 [Електронний ресурс]. Режим доступу: <https://owasp.org/API-Security/editions/2023/en/0x11-t10/>
6. Web Application Security Testing v4.2 [Електронний ресурс]. Режим доступу: [https://owasp.org/www-project-web-security-testing-guide/v42/4-Web\\_Application\\_Security\\_Testing/](https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/)
7. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу [Електронний ресурс]. Режим доступу: <https://tzi.com.ua/downloads/2.5-010-03.pdf>
8. Комплексна безпека інформаційних мережевих систем. Навчальний посібник/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. Львів, «Магнолія 2006», 2016. 256 с.
9. Біометричні технології: навч. посіб./ Р.Ю. Царьов, Т. М. Лемеха. Одеса: ОНАЗ ім. О.С. Попова, 2016. 140 с.
10. The Access Control Technologies Handbook. Prepared by Space and Naval Warfare Systems Center Atlantic, 2015. 53 p.
11. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник/ С.О. Іванченко, О.В. Гавриленко, О.А. Липський, А.С. Шевцов. К.: ІСЗЗІ НТУУ «КПІ», 2016. 104 с.
12. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ Г.М. Гулак. К.: Видавництво НА СБ України, 2020. 256 с.
13. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України: аналітична доповідь/ Д.Г. Бобро, С.П. Іванюта, С.І. Кондратов, О.М. Суходоля/ за заг. ред. О. М. Суходолі. К.: НІСД, 2019. 224 с.
14. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монограф./ О. П. Єрменчук. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.
15. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності. Навчальний посібник/ О.А. Лаптев, В.А. Савченко, Г.В. Шуклін. К.:ДУТ, 2020. 126 с.
16. Основи інформаційної безпеки. Конспект лекцій./ Б.А. Заплотинський. КПВіП НУ «ОЮА», кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. 128 с.
17. Сучасні методи забезпечення надійності персоналу: навчальний посібник у схемах і таблицях/ З.Б. Живко. Львів: ЛьвДУВС, 2019. 128 с.
18. Інформаційна безпека: питання правового регулювання: монографія / А.Ю. Нашинець-Наумова. Київ: Видавничий дім «Гельветика», 2017. 168 с.
19. Проектування комплексних систем захисту інформації. Підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів: Видавництво Львівської політехніки, 2020. 320 с.
20. Інформаційна безпека: навчальний посібник / [Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін.]; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. Львів: Видавництво Львівської політехніки, 2019. 580 с.

21. CMMI High Maturity Handbook [Електронний ресурс]. Режим доступу: [http://uploads.worldlibrary.net/uploads/pdf/20151101020335cmmi\\_high\\_maturity\\_hand\\_book\\_amazon.pdf](http://uploads.worldlibrary.net/uploads/pdf/20151101020335cmmi_high_maturity_hand_book_amazon.pdf)
22. Learning Malware Analysis. Explore the concepts, tools, and techniques to analyze and investigate Windows malware Security/ Edited by Monnappa K A. Packt Publishing Ltd, 2018. 500 p.
23. Проектування та монтаж локальних комп'ютерних мереж: [навчальний посібник]/ І. М. Журавська. Миколаїв: Видавництво ЧДУ ім. Петра Могили, 2016. 396 с.

#### Додаткова

24. 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>
25. Human vs bots: Detecting human attacks in a honeypot environment/ Shreya Udhani, Alexander Withers, Masooda Bashir. - 7th International Symposium on Digital Forensics and Security, ISDFS 2019. - <https://doi.org/10.1109/ISDFS.2019.8757534>
26. Secure and Resilient Artificial Intelligence of Things: a HoneyNet Approach for Threat Detection and Situational Awareness/ Liang Tan, Keping Yu, Fangpeng Ming, Xiaofeng Chen, Gautam Srivastava. - IEEE Consumer Electronics Magazine, 2021. – 10.1109/MCE.2021.3081874
27. Data Leakage Prevention System: A Systematic Report/ Sheela Gowr. P, Kumar. N. - International Journal of Recent Technology and Engineering (IJRTE), Volume-8 Issue-4, November 2019. – pp. 367-377. - DOI:10.35940/ijrte.D6904.118419
28. A survey on data leakage prevention systems/ Sultan Alneyadi, Elankayer Sithirasenan, Vallipuram Muthukkumarasamy. - Journal of Network and Computer Applications, Volume 62 Issue, C February, 2016. – pp. 137–152. - <https://doi.org/10.1016/j.jnca.2016.01.008>
29. One-Time-Username: A Threshold-based Authentication System/ Abdulrahman Alhothailya, Arwa Alrawaisa, Chunqiang Hua, Wei Li. - Procedia Computer Science 129 (2018), Elsevier Ltd. – pp. 427-431. - <https://doi.org/10.1016/j.procs.2018.03.019>
30. Design and Implementation of a Computerized User Authentication System for E-Learning/ Z. Faizal Khan, Sultan Refa Alotaibi. - iJET – Vol. 15, No. 9, 2020 - pp. 4-18. - <https://doi.org/10.3991/ijet.v15i09.12387>
31. Information leakage analysis of software: How to make it useful to IT industries?/ Kushal Anjaria, Arun Mishra/ - Faculty of Computers and Information Technology, Future University in Egypt. Production and hosting by Elsevier B.V., 2017. PP. 10-18. <https://doi.org/10.1016/j.fcij.2017.04.002>
32. Research on Behavior-Based Data Leakage Incidents for the Sustainable Growth of an Organization/ Jawon Kim, Jaesoo Kim, Hangbae Chang. Sustainability 2020, 12, 6217. PP. 1-14. doi:10.3390/su12156217
33. Yamfashije, Jeanne. (2017). Capability Maturity Model Integration. 10.13140/RG.2.2.35219.94247.
34. Використання розподілених хеш-таблиць надання доступу до хмарних сервісів/ Ю. П. Кльоц, І. В. Муляр, В. М. Чешун, О. В. Бурдюг// Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. Київ: ВІКНУ, 2020. Вип. 67. С. 85–95.
35. Удосконалення систем захисту інформації в комп'ютерних мережах Державної прикордонної служби України/ Андрошук О., Коваленко О., Тітова В., Чешун В., Поляков А. Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: військові та технічні науки, 85(2-3). 2021. С. 5-21.
36. Використання інформаційних технологій для підвищення якості роботи та безпеки телекомунікаційних мереж/ Хмельницький, Ю., Чешун, В., Джулій А., Чорненький, В.// Measuring and Computing Devices in Technological Processes, (2022). (1), С. 36–42. <https://doi.org/10.31891/2219-9365-2022-69-1-5>

## ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання. URL : <https://msn.khmnu.edu.ua/>
2. Електронна бібліотека університету. URL: <http://lib.khmnu.edu.ua/>