ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Декан факультету інформаційних технологій

_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

29 серпня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Технології виявлення вразливостей та вторгнень

Назва дисципліни

Галузь знань – 12 Інформаційні технології
Спеціальність – 125 Кібербезпека та захист інформації
Рівень вищої освіти – Перший (бакалаврський)
Освітньо-професійна програма – Кібербезпека та захист інформації
Обсяг дисципліни – 6 кредитів ЄКТС
Шифр дисципліни – ОПП.12
Мова навчання – Українська
Статус дисципліни – Обов'язкова (професійної підготовки)
Факультет – Інформаційних технологій
Кафедра – Кібербезпеки

Форма здобуття освіти	Курс	Семестр	Загальний обсяг		Кількість годин						Курсовий проєкт*	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття					Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття				Залік	Іспит
Д	3	7	5	180	66	32	34			114				+
Разом ДФН			**5**	**180**	**66**	**32**	**34**			**114**				**1**

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека та захист інформації» за спеціальністю 125 «Кібербезпека та захист інформації»

Робоча програма складена _____ д-р філософії Наталія ПЕТЛЯК
Підпис(и) автора(ів) Науковий ступінь, учене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 29.08 2025 № 1. Зав. кафедри _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

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

Хмельницький 2025

ЛИСТ ПОГОДЖЕННЯ

Посада	Назва кафедри	Підпис	Ініціали, прізвище
Завідувач кафедри, канд. техн. наук, доц.	Кібербезпеки		Юрій КЛЬОЦ
Гарант освітньо-професійної програми, канд. техн. наук, доц.	Кібербезпеки		Віктор ЧЕШУН

3. Пояснювальна записка

Дисципліна «Технології виявлення вразливостей та вторгнень» є однією із дисциплін фахової підготовки і займає провідне місце у підготовці здобувачів першого (бакалаврського) рівня вищої освіти, очної (денної) (далі – денної) форми здобуття вищої освіти, які навчаються за освітньо-професійною програмою «Кібербезпека та захист інформації» в межах спеціальності 125 «Кібербезпека та захист інформації».

***Пререквізити*:** ОПП.06 Захист інформації в інформаційно-комунікаційних системах; ОПП.11 Адміністрування та захист баз і сховищ даних.

***Кореквізити**:* ОПП.14 Комплексні системи захисту інформації; ОПП.16 Виробнича практика 2.

Відповідно до освітньої програми дисципліна сприяє забезпеченню:

***компетентностей*:** ІК Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризуються комплексністю та неповною визначеністю умов; ЗК 2 Знання та розуміння предметної області та розуміння професії; ЗК 4 Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням; ФК 2 Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки; ФК 3 Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах; ФК 5 Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки; ФК 8 Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку; ФК 11 Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки; ФК 12 Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки

***програмних результатів навчання*:** ПРН 4 Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; ПРН 6 Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; ПРН 11 Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; ПРН 18 Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; ПРН 20 Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; ПРН 28 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; ПРН 29 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; ПРН 30 Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; ПРН 41 Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; ПРН 42 Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; ПРН 48 Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; ПРН 49 Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; ПРН 50 Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); ПРН 51 Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; ПРН 52 Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

Мета дисципліни. Формування формування системи знань та розуміння предметної області необхідних для формалізованого опису, аналізу й синтезу вразливостей та вторгнень; розв'язування складних спеціалізованих задач; застосування методів та засобів планування, проведення тестувань, впровадження та супроводу комплексних систем виявлення та запобігання вторгненням.

Предмет дисципліни. Методи, методики, інформаційно-комунікаційні технології, програмно-апаратне забезпечення комплексних систем захисту інформації, їх впровадження та супроводу.

Завдання дисципліни. Забезпечити набуття компетентностей та досягнення програмних результатів навчання відповідно до Стандарту вищої освіти та освітньо-професійної програми підготовки бакалаврів зі спеціальності „Кібербезпека та захист інформації".

Результати навчання. Після вивчення дисципліни студент повинен: *виконувати* аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; *використовувати* програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; *забезпечувати* функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; *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; *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; *здійснювати* оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; *забезпечувати* неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; *впроваджувати* процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; *виконувати* впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; *забезпечувати* належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; *забезпечувати* функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); *підтримувати* працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; *використовувати* інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; *аналізувати*, *аргументувати*, *приймати рішення* при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; *критично осмислювати* основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

4. Структура залікових кредитів дисципліни

Назва розділу (теми)	Кількість годин, відведених на:		
	лекції	лабораторні роботи	СРС
Тема 1. Вірусологія	6	8	23
Тема 2. Засоби аналізу та тестування мережного трафіку	8	4	20
Тема 3. Системи виявлення та запобігання вторгненням	8	12	36
Тема 4. Інструменти аналізу та оцінка вразливостей	6	10	25
Тема 5. Контроль та управління доступом	4		10
Разом :	**32**	**34**	**114**

5. Програма навчальної дисципліни

5.1 Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотації	Кількість годин
	Тема 1. Вірусологія	**6**
1	**Комп'ютерна вірусологія** Класифікація комп'ютерних вірусів. Властивості комп'ютерних вірусів. Ознаки різних типів вірусів та шкідливого програмного забезпечення Літ.: [6] с. 68-87; [8] с. 28-57	2
2	**Антивіруси** Призначення. Архітектура. Функції антивірусів. Сигнатурний, поведінковий, евристичний аналіз, аналіз контрольних сум Літ.: [1] с. 112-121; [2] с. 316-318; [4] с. 70-85	2
3	**Інструменти та аналіз коду** Основні концепції створення сценаріїв і розробки програмного забезпечення. Використання інструментів тестування на проникнення та аналіз коду експлойту Літ.: [5] с. 199-220; [7] с. 183-201; [10-12];	2
	Тема 2. Засоби аналізу та тестування мережного трафіку	**8**
4	**Аналіз мережевого трафіку** Методологія аналізу мережного трафіку. Інструменти та процеси. Аналіз на рівні пакетів Літ.: [1] с. 44-62; [5] с. 221-243	2
5	**Інструменти моніторингу безпеки мережі** Аналізатори мережевих протоколів: Wireshark і Tcpdump. Аналізатори мережевих протоколів NetFlow. Security Information Event Management (SIEM). Security orchestration, automation, and response (SOAR) Літ.: [1] с. 142-148; [15]	2
6	**Методи та інструменти тестування безпеки мережі** Тестування та оцінка безпеки мережі. Типи мережевих тестів. Інструменти Nmap, Zenmap, SuperScan Літ.: [1] с. 39-44; [16]	2
7	**Міжмережні екрани** Призначення МЕ. Архітектура МЕ. Функції МЕ. Підключення та налаштування апаратних МЕ Літ.: [1] с. 62-89; [2] с. 318-325; [5] с. 256-263; [6] с. 110-113	2
	Тема 3. Системи виявлення та запобігання вторгненням	**8**
8	**Інструменти та програми для виявлення вторгнень** Загальні поняття IPS та IDS. Системи виявлення вторгнень (IDS). Системи запобігання вторгненням (IPS) Літ.: [2] с. 325-331; [5] с. 271-276; [17-19]	2
9	**Збір інформації та сканування вразливостей** Виконання пасивної розвідки. Проведення активної розвідки. Розуміння мистецтва сканування вразливостей. Розуміння того, як аналізувати результати сканування вразливостей Літ.: [5] с. 54-59; [20] с. 46-55; [21]; [22]	2

10	**Відкриті системи виявлення вторгнень** Snort. Prelude SIEM. NetSTAT. Zeek. OSSEC. Suricata. Security Onion Літ.: [24-30]	2
11	**Програмні та програмно-апаратні засоби виявлення вторгнень** Cisco IPS (Secure IPS). NETSCOUT. Symantec™ Cyber Security Services: DeepSight™ Intelligence. Check Point IPS. DefensePro. Kismet. McAfee Network Security Platform Літ.: [31-33]	2
	Тема 4. Інструменти аналізу та оцінка вразливостей	**6**
12	**Оцінка вразливостей кінцевого пристрою** Профілювання мережі та серверів. Загальна система оцінки вразливостей (CVSS). Безпечне управління пристроями Літ.: [34-36]	2
13	**Вразливості дротових і бездротових мереж** Вразливості дротових мереж. Вразливості бездротових мереж Літ.: [4] с. 215-226; [5] с. 464-469; [38]	2
14	**Хмарна, мобільна та безпека Інтернету речей** Дослідження векторів атак і здійснення атак на хмарні технології. Пояснення поширених атак і вразливостей проти спеціалізованих систем Літ.: [5] с. 469-514; [39]	2
	Тема 5. Контроль та управління доступом	**4**
15	**Списки контролю доступу (ACL)** Вступ до списків контролю доступу. Маскування підстановок. Налаштування ACL. Зниження атак за допомогою ACL Літ.: [2] с. 331-336; [40]	2
16	**Active Directory** Механізм організації захисту служби каталогу Active Directory. Протокол Kerberos. Процес автентифікації на базі протоколу Kerberos. Огляд існуючих областей безпеки, що підлягають настроюванню за допомогою групових політик. Аудит і ведення журналу безпеки. Поняття шаблону безпеки. Аналіз системи безпеки Літ.: [41-43]	2
	Разом:	**32**

5.2 Зміст лабораторних занять

№ п/п	Тема лабораторного заняття	Кількість годин
	Тема 1. Вірусологія	**8**
1	**Пошук вразливостей веб-сайту та застосування сканерів вразливостей** Літ.: [7] с. 67-95; [9] с. 6-14; [55]	4
2	**Аналіз коду експлойту** Літ.: [3] с. 61-70; [9] с. 14-19; [11-12]	4
	Тема 2. Засоби аналізу та тестування мережного трафіку	**4**
3	**Використання сніферів мережевого трафіка** Літ.: [3] с. 116-121; [7] с. 46-54,95-104; [9] с. 19-25; [15]	4
	Тема 3. Системи виявлення та запобігання вторгненням	**12**
4	**Збір даних на основі відкритих джерел** Літ.: [3] с. 88-92; [9] с. 25-31; [47-49]	4
5	**Активний збір даних про мережу та пошук вразливостей** Літ.: [3] с. 96-102; [9] с. 31-37; [16]	4
6	**Використання сканерів вразливостей** Літ.: [3] с. 102-108; [9] с. 37-44; [50-53]	4
	Тема 4. Інструменти аналізу та оцінка вразливостей	**8**
7	**Збір інформації та пошук вразливостей за допомогою Metasploit** Літ.: [3] с. 70-88; [4] с. 198-215; [9] с. 44-50; [54]	4
8	**Експлуатація вразливостей за допомогою Burp Suite** Літ.: [2] с. 283-291; [9] с. 50-53	4
9	*Підсумкове заняття*	**2**
	Разом	**34**

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

Самостійна робота студентів полягає у систематичному опрацюванні програмного матеріалу з відповідних джерел інформації, підготовці до виконання і захисту лабораторних робіт, тестування тощо. Керівництво самостійною роботою здійснюється викладачем згідно з розкладом консультацій у позаурочний час. Крім цього до послуг студентів сторінка навчальної дисципліни у Модульному середовищі для навчання, де розміщені Робоча програма дисципліни та необхідні документи з її навчально-методичного забезпечення.

Номер тижня	Вид самостійної роботи	Кількість годин
1-2	Опрацювання теоретичного матеріалу з Т №1. Підготовка до виконання ЛР №1.	13
3-4	Опрацювання теоретичного матеріалу з Т №1. Підготовка до захисту ЛР №1. Підготовка до виконання ЛР №2.	13
5-6	Опрацювання теоретичного матеріалу з Т №2. Підготовка до захисту ЛР №2. Підготовка до виконання ЛР №3.	14
7-8	Опрацювання теоретичного матеріалу з Т №2. Підготовка до захисту ЛР №3. Підготовка до виконання ЛР №4.	14
9-10	Опрацювання теоретичного матеріалу з Т №3. Підготовка до захисту ЛР №4. Підготовка до виконання ЛР №5.	14
11-12	Опрацювання теоретичного матеріалу з Т №3. Підготовка до захисту ЛР №5. Підготовка до виконання ЛР №6.	14
13-14	Опрацювання теоретичного матеріалу з Т №4. Підготовка до захисту ЛР №6. Підготовка до виконання ЛР №7.	14
15-16	Опрацювання теоретичного матеріалу з Т №5. Підготовка до захисту ЛР №7. Підготовка до виконання ЛР №8.	14
17	Повторення теоретичного матеріалу за Т1-5. Тестування. Підготовка до захисту ЛР №8.	4
	Разом 1-й семестр:	**114**

***Примітки*:** Т – тема навчальної дисципліни, ЛР – лабораторна робота.

6. Технології та методи навчання

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних технологій та методів. Зокрема, лекції проводяться з використанням словесних, наочних, інтерактивних та проблемних методів з супроводом мультимедійних технологій та презентаційних матеріалів; лабораторні роботи – з використанням практичних та частково-пошукових методів, із застосуванням сучасних інформаційно-комп'ютерних технологій, технологій ситуативного та контекстного навчання; самостійна робота – з використанням пояснювально-ілюстративних та частково-пошукових методів.

7. Методи контролю

Поточний контроль здійснюється під час лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочою програмою і графіком освітнього процесу, в т.ч. з використанням Модульного середовища для навчання. При цьому використовуються такі методи поточного контролю:

– оцінювання результатів захисту лабораторних робіт;

– тестовий контроль засвоєння теоретичного та практичного матеріалу.

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

8. Політика дисципліни

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

Здобувачі вищої освіти мають дотримуватися встановлених термінів виконання всіх видів навчальної роботи

відповідно до робочої програми навчальної дисципліни. Пропущене практичне заняття студент зобов'язаний відпрацювати у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за результатами опитування під час практичних занять, захисту лабораторних робіт та тестування.

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

У межах вивчення навчальної дисципліни здобувачам вищої освіти передбачено визнання і зарахування результатів навчання, набутих шляхом неформальної освіти, що розміщені на доступних платформах (наприклад https://www.netacad.com, https://prometheus.org.ua/), які сприяють формування компетентностей і поглибленню результатів навчання, визначених робочою програмою дисципліни, або забезпечують вивчення відповідної теми та/або виду робіт з програми навчальної дисципліни (детальніше у Положенні про порядок визнання та зарахування результатів навчання здобувачів вищої освіти у ХНУ).

9. Оцінювання результатів навчання студентів у семестрі

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

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

Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти

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

Структурування дисципліни за видами навчальної роботи і оцінювання результатів навчання студентів

Аудиторна робота								Контрольні заходи	Семестровий контроль	
Захист лабораторних робіт								Тестовий контроль	Іспит	Разом балів
1	2	3	4	5	6	7	8	Т1-5	Т1-5	
Кількість балів за вид навчальної роботи (мінімум-максимум)										
3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5	12-20	**24-40**	**60-100***
24-40								**12-20**	**24-40**	

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

Оцінювання результатів захисту лабораторної роботи

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

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

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

При оцінюванні лабораторних робіт викладач керується узагальненими критеріями, наведеними у таблиці «**Критерії оцінювання навчальних досягнень здобувача вищої освіти**».

Оцінку, отриману за лабораторну роботу, викладач оголошує студенту одразу після захисту лабораторної роботи і проставляє в електронний журнал дисципліни.

Оцінювання результатів тестового контролю

Кожний з тестів, передбачених Робочою програмою, складається із 50 тестових завдань, кожне з яких є рівнозначним.

Відповідно до таблиці структурування видів робіт за тестовий контроль здобувач залежно від кількості правильних відповідей може отримати від 12 до 20 балів.

Розподіл балів в залежності від наданих правильних відповідей на тестові завдання

Кількість правильних відповідей	0-29	30-31	32-33	34-36	37-38	39-41	42-43	44-46	47-48	49-50
Відсоток правильних відповідей	0-58	60-62	64-66	68-72	74-76	78-82	84-86	88-92	94-96	98-100
Кількість балів	0	12	13	14	15	16	17	18	19	20

На тестування відводиться 60 хвилин. Студент проходить тестування в он-лайн режимі у Модульному середовищі для навчання. Також, студент може проходити тестування письмово, записуючи правильні відповіді у талоні відповідей. При отриманні негативної оцінки тест слід перездати до терміну ***наступного*** контролю.

Оцінювання результатів підсумкового семестрового контролю (іспит)

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

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

Види завдань	**Для кожного окремого виду завдань**		
	Мінімальний (достатній) бал (задовільно)	**Потенційні позитивні бали* (середній бал) (добре)**	**Максимальний (високий) бал (відмінно)**
Теоретичне питання № 1	6	8	10
Теоретичне питання № 2	6	8	10
Практичне завдання №1	12	16	20
Разом:	**24**	**32**	**40**

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

Для кожного окремого виду завдань підсумкового семестрового контролю застосовуються критерії оцінювання навчальних досягнень здобувача вищої освіти, наведені вище (**Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти)**.

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

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

Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

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

10. Питання для самоконтролю результатів навчання

1. Властивості комп'ютерних вірусів
2. Класифікація комп'ютерних вірусів
3. Ознаки різних типів вірусів та шкідливого програмного забезпечення
4. Призначення антивірусних засобів
5. Архітектура антивірусів
6. Методи виявлення шкідливого програмного забезпечення
7. Методи усунення наслідків зараження шкідливого програмного забезпечення
8. Технологія виявлення шкідливого програмного забезпечення
9. Сигнатурний, поведінковий, евристичний аналіз, аналіз контрольних сум
10. Основні концепції створення сценаріїв і розробки програмного забезпечення
11. Використання інструментів тестування на проникнення та аналіз коду експлойту
12. Розуміння вразливостей на основі ін'єкцій
13. Використання вразливостей на основі автентифікації
14. Використання вразливостей на основі авторизації
15. Розуміння вразливостей міжсайтового сценарію (XSS)
16. Розуміння атак підробки міжсайтових запитів (CSRF/XSRF) і підробки запитів на стороні сервера
17. Розуміння Clickjacking
18. Використання неправильних налаштувань безпеки
19. Використання вразливості включення файлів
20. Використання небезпечного коду
21. Методологія аналізу мережного трафіку
22. Аналізатори мережних протоколів: Wireshark і Tcpdump
23. Аналізатор мережних протоколів NetFlow
24. Security Information Event Management
25. Security orchestration, automation, and response
26. Тестування та оцінка безпеки мережі
27. Типи мережевих тестів
28. Інструменти Nmap та Zenmap, SuperScan
29. Призначення міжмережевих екранів
30. Функції міжмережевих екранів
31. Підключення та налаштування апаратних міжмережевих екранів
32. Система виявлення вторгнень

33. Система запобігання вторгненням
34. Виконання пасивної розвідки
35. Проведення активної розвідки
36. Сканування вразливостей
37. Аналіз результатів сканування вразливостей
38. Відкриті системи виявлення вторгнень
39. Програмні та програмно-апаратні засоби виявлення вторгнень
40. Загальна система оцінки вразливостей
41. Безпечне управління пристроями
42. Використання вразливостей мережі
43. Використання вразливостей бездротового зв'язку
44. Дослідження векторів атак і здійснення атак на хмарні технології
45. Списки контролю доступу
46. Active Directory

11. Навчально-методичне забезпечення

Освітній процес з дисципліни «Технології виявлення вразливостей та вторгнень» забезпечений необхідними навчально-методичними матеріалами, що розміщені в Модульному середовищі для навчання MOODLE:

1. Курс «Технології виявлення вразливостей та вторгнень»: https://msn.khmnu.edu.ua/course/view.php?id=8956

Зокрема, викладачами кафедри підготовлені і видані такі роботи:

1. Технології виявлення вразливостей та вторгнень: методичні рекомендації до лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 125 «Кібербезпека та захист інформації» / Ю. П. Кльоц, Н. С. Петляк, О. С. Савенко, М. В. Капустян. Хмельницький : ХНУ, 2024. 60 с.

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

Інформаційна та комп'ютерна підтримка: ПК або ноутбук, проєктор, доступ до мережі Інтернет, робота з презентаціями. Програмне забезпечення: ОС Windows, ОС Kali Linux, VirusTotal, VirtualBox, Nmap, Wireshark, Hydra, Angry IP Scanner, Nessus Essentials, Enum4linux, Metasploit Framework, Burp Suite, вебресурси Shodan, Censys, Netcraft, Bgp та SpiderFoot.

13. Рекомендована література

Основна

1. Жилін А.В., Шаповал О.М., Успенський О.А. Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. Київ: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с.
2. Вступ до кібербезпеки: навч. посіб. / Смірнов О.А. та ін. Кропивницький: ЦНТУ, 2022. 967 с.
3. Живило Є.О. Тестування на проникнення: навч. посіб. Ч.1. Полтава : ПНТУ "Полтавська політехніка ім. Юрія Кондратюка", 2024. 134 с.
4. Живило Є.О. Тестування на проникнення: навч. посіб. Ч.2. Полтава : ПНТУ "Полтавська політехніка ім. Юрія Кондратюка", 2024. 239 с.
5. Кравчук С.О. Протидія хакерським атакам в мобільних інфокомунікаціях : навч. посіб. Київ: КПІ ім. Ігоря Сікорського, 2025. 814 с.

Додаткова

6. Вишня В.Б., Гавриш О.С., Рижков Е.В. Основи інформаційної безпеки: навч. посіб. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
7. Пірог О.В. Безпека вебдодатків : навч. посіб. Житомир : Житомирська політехніка, 2025. 290 с.
8. Терейковський І.А., Корченко О.Г., Погорелов В.В. Методи розпізнавання кібератак: розпізнавання комп'ютерних вірусів: посібник. Київ : КПІ ім. Ігоря Сікорського, 2022. 127 с.
9. Технології виявлення вразливостей та вторгнень : методичні рекомендації / Кльоц Ю.П. та ін. Хмельницький : ХНУ, 2024. 60 с.
10. Богданова Є., Чорна Т., Малахов С. Огляд поточного стану загроз, що обумовлені впливом експлойтів. *Комп'ютерні науки та кібербезпека*. 2022. № 2, С. 35-40. DOI: 10.26565/2519-2310-2022-2-04
11. Functions and Procedures. Programming. Computing. URL: https://www.advanced-ict.info/programming/functions.html (дата звернення 12.07.2025)
12. Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers. URL: https://www.exploit-db.com/ (дата звернення 12.07.2025)
13. OWASP Top Ten. OWASP Foundation OWASP. URL: https://owasp.org/www-project-top-ten/ (дата звернення 12.07.2025)
14. Guide to Web Application Penetration Testing. URL: https://relevant.software/blog/penetration-testing-for-web-applications/ (дата звернення 14.07.2025)
15. Wireshark Documentation. URL: https://www.wireshark.org/docs/ (дата звернення 14.07.2025)
16. Nmap Network Scanning. URL: https://nmap.org/book/toc.html (дата звернення 15.07.2025)
17. Liu Q, Hagenmeyer V., Keller H. A Review of Rule Learning-Based Intrusion Detection Systems and Their Prospects in Smart Grids. *IEEE Access.* 2021. Vol. 9, P. 57542-57564. DOI: 10.1109/ACCESS.2021.3071263.
18. What is an Intrusion Prevention System (IPS)? URL: https://informationsecurityasia.com/what-is-an-intrusion-

prevention-system-ips (дата звернення 15.07.2025)
19. IPS. URL: https://www.process.com/docs/multinet5_6/install_admin/chapter_30.html (дата звернення 18.07.2025)
20. Яцків В. В. Тестування комп'ютерних систем на проникнення. Тернопіль: ТНЕУ, 2019. 119 с.
21. Vulnerability Assessment Report: A Beginner's Guide. URL: https://www.getastra.com/blog/security-audit/vulnerability-assessment-report/ (дата звернення 18.07.2025)
22. Vulnerability assessment results categories. URL: https://www.ibm.com/docs/en/sga?topic=vulnerability-assessment-results-categories (дата звернення 20.07.2025)
23. Snort. URL: https://www.snort.org/ (дата звернення 20.07.2025)
24. Prelude. URL: https://www.prelude-siem.com/ (дата звернення 23.07.2025)
25. Netstat. URL: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/netstat (дата звернення 23.07.2025)
26. Zeek. URL: https://zeek.org/ (дата звернення 23.07.2025)
27. OSSEC. URL: https://www.ossec.net/docs (дата звернення 23.07.2025)
28. Suricata. URL: https://suricata.io/documentation (дата звернення 24.07.2025)
29. Samhain. URL: https://www.la-samhna.de/samhain/index.html (дата звернення 24.07.2025)
30. Security Onion Solutions. URL: https://securityonionsolutions.com/ (дата звернення 25.07.2025)
31. McAfee Network Security Platform 10.1.9 Product Guide. URL: https://docs.trellix.com/bundle/network-security-platform-10.1.x-product-guide/page/GUID-373C1CA6-EC0E-49E1-8858-749D1AA2716A.html (дата звернення 26.07.2025)
32. Kismet. URL: https://www.kismetwireless.net/ (дата звернення 26.07.2025)
33. DefensePro X: The Next Level of DDOS Protection. URL: https://www.radware.com/products/defensepro/ (дата звернення 27.07.2025)
34. National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). URL: http://nvd.nist.gov/ (дата звернення 27.07.2025)
35. Common Vulnerability Scoring System Calculator Version 3. URL: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator (дата звернення 27.07.2025)
36. CVSS v3 User Guide. URL: https://www.first.org/cvss/v3.1/user-guide (дата звернення 27.07.2025)
37. Підпалий О. І., Романов О. І. Аналіз вразливості бездротової мережі WI-FI з новим протоколом захищеності WPA3. *Збірник матеріалів Міжнародної науково-технічної конференції «Перспективи телекомунікацій»*. М. Київ, 13-17 квітня 2020.
38. Абакумов А.І., Харченко В.С. Тестування на проникнення систем інтернету речей: кіберзагрози, методи та етапи. *Електрон. моделювання*. 2022. № 4, С. 79—104. DOI: 10.15407/emodel.44.04.079
39. Katherine Rongstad,Ruidong Zhang. Enterprise network security from cloud computing perspective. *Information Systems*. 2021. Vol. 22, P. 107-113.
40. Access Control List. URL: https://learn.microsoft.com/uk-ua/windows-hardware/drivers/ifs/access-control-list (дата звернення 04.08.2025)
41. Motero C.D., Higuera J.R.B., Higuera J.B., Montalvo J.A.S., Gómez N.G. On Attacking Kerberos Authentication Protocol in Windows Active Directory Services: A Practical Survey. *IEEE Access*. 2021. Vol. 9, P. 109289-109319. DOI: 10.1109/ACCESS.2021.3101446.
42. Mokhtar B.I., Jurcut A.D., ElSayed M.S., Azer M.A. Active Directory Attacks—Steps, Types, and Signatures. *Electronics*. 2022. Vol. 11, P. 2629. DOI: 10.3390/electronics11162629
43. Guido Grillenmeier. Now's the time to rethink Active Directory security. *Network Security*, 2021. Vol. 7, P. 13-16. DOI: 10.1016/S1353-4858(21)00076-3.
44. Open Source Vulnerability Management. URL: https://www.greenbone.net/en/open-source-vulnerability-management (дата звернення 02.08.2025)
45. OWASP. URL: https://owasp.org/ (дата звернення 02.08.2025)
46. Shodan. URL: https://www.shodan.io (дата звернення 05.08.2025)
47. Getting Started with Search - Censys. URL: https://search.censys.io/search/getting-started (дата звернення 09.08.2025)
48. Netcraft. https://sitereport.netcraft.com URL: https://www.netcraft.com/ (дата звернення 09.08.2025)
49. Hurricane Electric BGP Toolkit URL: https://bgp.he.net/ (дата звернення 09.08.2025)
50. Enum4linux. Kali Linux Tools. URL: https://www.kali.org/tools/enum4linux/ (дата звернення 13.08.2025)
51. Advanced IP Scanner. URL: https://www.advanced-ip-scanner.com/ua/ (дата звернення 13.08.2025)
52. Rapid7 - Practitioner-First Cybersecurity Solutions. URL: https://www.rapid7.com/ (дата звернення 17.08.2025)
53. Tenable Nessus. URL: https://docs.tenable.com/ (дата звернення 17.08.2025)
54. Metasploit Documentation Penetration Testing Software, Pen Testing Security URL: https://docs.metasploit.com/ (дата звернення 12.07.2025)
55. Nikto. Kali Linux Tools URL: https://www.kali.org/tools/nikto (дата звернення 17.08.2025)

14. Інформаційні ресурси

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/course/view.php?id=8956
2. Електронна бібліотека ХНУ. URL: https://library.khmnu.edu.ua/
3. Інституційний репозитарій ХНУ. URL : https://elar.khmnu.edu.ua/

ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ТА ВТОРГНЕНЬ

Тип дисципліни	Обов'язкова
Рівень вищої освіти	Перший (бакалаврський*)*
Мова викладання	Українська
Семестр	Сьомий
Кількість призначених кредитів ЄКТС	6,0
Форми здобуття освіти, для яких викладається дисципліна	Очна (денна)

Результати навчання. Після вивчення дисципліни студент повинен: *виконувати* аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; *використовувати* програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; *забезпечувати* функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; *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; *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; *здійснювати* оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; *забезпечувати* неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; *впроваджувати* процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; *виконувати* впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; *забезпечувати* належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; *забезпечувати* функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); *підтримувати* працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; *використовувати* інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; *аналізувати*, *аргументувати*, *приймати рішення* при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; *критично осмислювати* основні теорії, принципи, методи і поняття у навчанні та професійній діяльності..

Зміст навчальної дисципліни. Вірусологія. Засоби аналізу та тестування мережного трафіку. Системи виявлення та запобігання вторгненням. Інструменти аналізу та оцінка вразливостей. Контроль та управління доступом.

Пререквізити: захист інформації в інформаційно-комунікаційних системах; адміністрування та захист баз і сховищ даних.

Кореквізити: комплексні системи захисту інформації; виробнича практика 2.

Запланована навчальна діяльність: Мінімальний обсяг навчальних занять в одному кредиті ЄКТС навчальної дисципліни для ***першого*** (бакалаврського) рівня вищої освіти за денною формою здобуття освіти становить 10 годин на 1 кредит ЄКТС.

Форми (методи) навчання: лекції (з використанням словесних, наочних, інтерактивних та проблемних методів); лабораторні роботи (з використанням практичних та частково-пошукових методів, ситуативного та контекстного навчання); самостійна робота (з використанням пояснювально-ілюстративних та частково-пошукових методів).

Форми оцінювання результатів навчання: оцінювання результатів захисту лабораторних робіт; тестування; іспит.

Вид семестрового контролю: іспит.

Навчальні ресурси:

1. Жилін А.В., Шаповал О.М., Успенський О.А. Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. Київ: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с.
2. Вступ до кібербезпеки: навч. посіб. / Смірнов О.А. та ін. Кропивницький: ЦНТУ, 2022. 967 с.
3. Живило Є.О. Тестування на проникнення: навч. посіб. Ч.1. Полтава : ПНТУ "Полтавська політехніка ім. Юрія Кондратюка", 2024. 134 с.
4. Живило Є.О. Тестування на проникнення: навч. посіб. Ч.2. Полтава : ПНТУ "Полтавська політехніка ім. Юрія Кондратюка", 2024. 239 с.
5. Кравчук С.О. Протидія хакерським атакам в мобільних інфокомунікаціях : навч. посіб. Київ: КПІ ім. Ігоря Сікорського, 2025. 814 с.
6. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/course/view.php?id=8956
7. Електронна бібліотека ХНУ. URL: https://library.khmnu.edu.ua/

Викладач: д-р філософії, ст. викл. Наталія Петляк.