ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету ІТ
_____ Олег САВЕНКО
Підпис Ім'я, ПРІЗВИЩЕ
«_08_» _____ 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Технології виявлення вразливостей та вторгнень

Галузь знань	12 – Інформаційні технології
Спеціальність	125 – Кібербезпека
Рівень вищої освіти	Перший бакалаврський
Освітньо-професійна програма	Кібербезпека
Обсяг дисципліни	5 кредитів ЄКТС
Шифр дисципліни	ОПП.14
Мова навчання	Українська
Статус дисципліни	Обов'язкова, дисципліна професійної підготовки
Факультет	Інформаційних технологій
Кафедра	Кібербезпеки

Форма навчання	Курс	Семестр	Обсяг дисципліни		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
Очна (денна)	3	6	5	150	68	34	34			82				+

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека» першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека»

Робоча програма складена _____ канд. техн. наук, доц. Юрій КЛЬОЦ

_____ Наталія ПЕТЛЯК
Підпис(и) автора(ів) Ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 31.08.2023 № 1 Зав. кафедри _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Олег САВЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2023

ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ТА ВТОРГНЕНЬ

Тип дисципліни	Обов'язкова
Освітній рівень	Перший (бакалаврський)
Мова викладання	Українська
Семестр	Шостий
Кількість встановлених кредитів ЄКТС	5
Форми навчання, для яких викладається дисципліна	Очна денна

Результати навчання. Студент, який успішно завершив вивчення дисципліни, повинен: аналізувати інформаційні системи та аргументувати наявність вразливостей, приймати рішення при розв'язанні задач із виявлення та практичних проблем щодо запобігання вторгненням у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів, зокрема застосовувати міжмережні екрани, системи виявлення та запобігання вторгненням, здійснювати контроль та управління доступом; аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході тестувань на виявлення вразливостей чи вторгнень, проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки щодо наявного рівня захисту інформаційної системи; здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах, з використанням різних програмних засобів (Nmap, SurScan, Snort, Metasploit та інші) та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем за допомогою інструментів аналізу та оцінки вразливостей кінцевих пристроїв, дротових та бездротових мереж, хмарних ресурсів та пристроїв IoT; забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур при аналізі мережного трафіку, застосуванні аналізаторів мережевих протоколів, використовуючи інструменти тестування безпеки мережі; впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; виконувати впровадження та підтримку систем виявлення вторгнень (IDS, IPS, IDPS) та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах шляхом застосування систем виявлення вторгнень, зокрема Zeek, Suricata, Security Onion; забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах задля збору інформації шляхом пасивної та активної розвідки; забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень, а саме Cisco IPS, Kismet, McAfee Network Security Platform, Symantec™ Cyber Security Services: DeepSight™ Intelligence, DefensePro та інших; підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

Зміст навчальної дисципліни. Вірусологія, антивіруси; інструменти та аналіз коду; використання вразливостей програми; аналіз мережного трафіку; інструменти моніторингу безпеки мережі; методи та інструменти тестування безпеки мережі; міжмережні екрани; інструменти та програми для виявлення вторгнень; збір інформації та сканування вразливостей; відкриті системи виявлення вторгнень; програмні та програмно-апаратні засоби виявлення вторгнень; оцінка вразливостей кінцевого пристрою; вразливості дротових і бездротових мереж; хмарна, мобільна та безпека Інтернету речей; списки контролю доступу (ACL), Active Directory.

Пререквізити: Основи інформаційної безпеки, Технології програмування та алгоритмізації, Операційні системи та технології їх захисту, Безпека вебресурсів

Кореквізити: Комплексні системи захисту інформації

Запланована навчальна діяльність: лекцій 34 год., лабораторних робіт 36 год., самостійної роботи 80 год., разом 150 год.

Методи навчання: пояснювально-ілюстративні, практичні, продуктивні, застосування інформаційно-комп'ютерних технологій.

Форми оцінювання результатів навчання: усне опитування, письмова контрольна робота, захист

лабораторних робіт, підсумковий контрольний захід (семестровий контроль).

Вид семестрового контролю: іспит.

Навчальні ресурси:

1. Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.
2. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. Вступ до кібербезпеки: навч. посіб. – Кропивницький: ЦНТУ, 2022. – 967 с.
3. Вступ до кібербезпеки: Методичні рекомендації до виконання лабораторних робіт для студентів денної форми навчання галузі 12 Інформаційні технології. / уклад. Смірнов О.А., Буравченко К.О., Смірнова Т.В., Конопліцька-Слободенюк О.К., Смірнов С.А., Козлов Я.О. / М-во освіти і науки України, Центральноукр. нац. техн. ун-т; – Кропивницький: ЦНТУ – 2022. – 155 с.
4. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструк-тури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.
5. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах: навч. посіб. — Кропивницький: Видавець Лисенко В. Ф., 2020. — 295 с.
6. Анна Корченко, Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія, Київ, ЦП «Компринт», 2019 – 361 с.

Викладач: Петляк Н.С.

ВСТУП

Дисципліна “Технології виявлення вразливостей та вторгнень” - складова професійної підготовки бакалаврів зі спеціальності «Кібербезпека».

Метою дисципліни є 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.

Предметом дисципліни є 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”:

компетентності:

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку

КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 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.

результати навчання:

РН 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.

РН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

РН 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.

РН 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.

РН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.

РН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.

РН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.

РН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

РН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.

РН 50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

РН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення

вторгнень в інформаційно-телекомунікаційних системах.

РН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

Студент, який успішно завершив вивчення дисципліни, повинен: аналізувати інформаційні системи та аргументувати наявність вразливостей, приймати рішення при розв'язанні задач із виявлення та практичних проблем щодо запобігання вторгненням у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів, зокрема застосовувати міжмережні екрани, системи виявлення та запобігання вторгненням, здійснювати контроль та управління доступом; аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході тестувань на виявлення вразливостей чи вторгнень, проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки щодо наявного рівня захисту інформаційної системи; здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах, з використанням різних програмних засобів (Nmap, SurScan, Snort, Metasploit та інші) та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем за допомогою інструментів аналізу та оцінки вразливостей кінцевих пристроїв, дротових та бездротових мереж, хмарних ресурсів та пристроїв IoT; забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур при аналізі мережного трафіку, застосуванні аналізаторів мережевих протоколів, використовуючи інструменти тестування безпеки мережі; впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; виконувати впровадження та підтримку систем виявлення вторгнень (IDS, IPS, IDPS) та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах шляхом застосування систем виявлення вторгнень, зокрема Zeek, Suricata, Security Onion; забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах задля збору інформації шляхом пасивної та активної розвідки; забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень, а саме Cisco IPS, Kismet, McAfee Network Security Platform, Symantec™ Cyber Security Services: DeepSight™ Intelligence, DefensePro та інших; підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	Кількість годин відведених на:		
	лекції	**лабораторні роботи**	**самостійну роботу**
Шостий семестр			
Тема 1. Вірусологія	8	8	18
Тема 2. Засоби аналізу та тестування мережного трафіку	8	4	16
Тема 3. Системи виявлення та запобігання вторгненням	8	12	22
Тема 4. Інструменти аналізу та оцінка вразливостей	6	8	14
Тема 5. Контроль та управління доступом	4	4 (підсумкове, контрольна робота)	10
Разом:	**34**	**36**	**80**

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотації	Кількість годин
1	2	3
Тема 1. Вірусологія		
1	**Комп'ютерна вірусологія** 1. Класифікація комп'ютерних вірусів 2. Властивості комп'ютерних вірусів 3. Ознаки різних типів вірусів та шкідливого програмного забезпечення Літ.: [7] с. 68-87, [8] с. 54-78, [9] с. 28-57	2
2	**Антивіруси** 1. Призначення 2. Архітектура 3. Функції антивірусів 4. Сигнатурний, поведінковий, евристичний аналіз**,** аналіз контрольних сум Літ.: [1] с. 112-121, [2] с.316-318, [10] с. 240-256	2
3	**Інструменти та аналіз коду** 1. Основні концепції створення сценаріїв і розробки програмного забезпечення 2. Використання інструментів тестування на проникнення та аналіз коду експлойту Літ.: [11] [12] [13]	2
4	**Використання вразливостей програми** 1. Огляд атак на основі веб-додатків для професіоналів із безпеки та 10 найкращих OWASP 2. Розуміння вразливостей на основі ін'єкцій 3. Використання вразливостей на основі автентифікації та авторизації 4. Розуміння вразливостей міжсайтового сценарію (XSS) 5. Розуміння атак підробки міжсайтових запитів (CSRF/XSRF) і підробки запитів на стороні сервера 6. Розуміння Clickjacking 7. Використання неправильних налаштувань безпеки 8. Використання вразливості включення файлів 9. Використання небезпечного коду Літ.: [14] [15]	2
Тема 2. Засоби аналізу та тестування мережного трафіку		
5	**Аналіз мережного трафіку** 1. Методологія аналізу мережного трафіку 2. Інструменти та процеси. 3. Аналіз на рівні пакетів. Літ.: [1] с. 44-62	2
6	**Інструменти моніторингу безпеки мережі** 1. Аналізатори мережевих протоколів: Wireshark і Tcpdump 2. Аналізатори мережевих протоколів NetFlow 3. Security Information Event Management (SIEM) 4. Security orchestration, automation, and response (SOAR) Літ.: [1] с. 142-148, [16]	2

1	2	3
7	**Методи та інструменти тестування безпеки мережі** 1. Тестування та оцінка безпеки мережі 2. Типи мережевих тестів 3. Інструменти Nmap, Zenmap, SuperScan Літ.: [1] с. 39-44, [17]	2
8	**Міжмережні екрани** 1. Призначення МЕ 2. Архітектура МЕ 3. Функції МЕ 4. Підключення та налаштування апаратних МЕ Літ.: [1] с. 62-89, [7] с.110-113, [2] с. 318-325	2
Тема 3. Системи виявлення та запобігання вторгненням		
9	**Інструменти та програми для виявлення вторгнень** 1. Загальні поняття IPS та IDS 2. Системи виявлення вторгнень (IDS) 3. Системи запобігання вторгненням (IPS) Літ.: [5] с. 154-205, [2] с. 325-331 [18-21]	2
10	**Збір інформації та сканування вразливостей** 1. Виконання пасивної розвідки 2. Проведення активної розвідки 3. Розуміння мистецтва сканування вразливостей 4. Розуміння того, як аналізувати результати сканування вразливостей Літ.: [22] с. 46-55 [23] [24]	2
11	**Відкриті системи виявлення вторгнень** 1. Snort 2. Prelude SIEM 3. NetSTAT 4. Zeek 5. OSSEC 6. Suricata 7. Security Onion Літ.: [6] с. 17-43, [25-32]	2
12	**Програмні та програмно-апаратні засоби виявлення вторгнень** 1. Cisco IPS (Secure IPS) 2. NETSCOUT 3. Symantec™ Cyber Security Services: DeepSight™ Intelligence 4. Check Point IPS 5. DefensePro 6. SolarWinds 7. Kismet 8. McAfee Network Security Platform Літ.: [6] с. 43-66, [33-35]	2
Тема 4. Інструменти аналізу та оцінка вразливостей		
13	**Оцінка вразливостей кінцевого пристрою** 1. Профілювання мережі та серверів 2. Загальна система оцінки вразливостей (CVSS) 3. Безпечне управління пристроями Літ.: [36-38]	2
14	**Вразливості дротових і бездротових мереж** 1. Вразливості дротових мереж 2. Вразливості бездротових мереж Літ.: [4] с. 132-155, [39]	2

1	2	3
15	**Хмарна, мобільна та безпека Інтернету речей** 1. Дослідження векторів атак і здійснення атак на хмарні технології 2. Пояснення поширених атак і вразливостей проти спеціалізованих систем Літ.: [40] [41]	2
Тема 5. Контроль та управління доступом		
16	**Списки контролю доступу (ACL)** 1. Вступ до списків контролю доступу 2. Маскування підстановок 3. Налаштування ACL 4. Зниження атак за допомогою ACL Літ.: [4] с. 155-161, [42] [2] с. 331-336	2
17	**Active Directory** 1. Механізм організації захисту служби каталогу Active Directory 2. Протокол Kerberos 3. Процес автентифікації на базі протоколу Kerberos 4. Огляд існуючих областей безпеки, що підлягають настроюванню за допомогою групових політик 5. Аудит і ведення журналу безпеки 6. Поняття шаблону безпеки 7. Аналіз системи безпеки Літ.: [43-45]	2
	Разом за семестр:	**34**

Перелік лабораторних робіт

№ п/п	Теми лабораторних робіт	Кількість годин
1	**Пошук вразливостей веб-сайту та застосування сканерів вразливостей GVM, OWASP** Літ.:[46-47]	4
2	**Аналіз коду експлойту** Літ.: [12-13]	4
3	**Використання сканерів мережевого трафіка Wireshark та Snort** Літ.: [16] [25]	4
4	**Розвідка на основі відкритих джерел (OSINT)** Літ.: [48-51]	4
5	**Активний збір даних про мережу та пошук вразливостей** Літ.: [17], [3] с 25-35	4
6	**Використання сканерів вразливостей enum4linux, IPscanner, rapid7 та Nessus** Літ.: [52-55]	4
7	**Збір інформації та пошук вразливостей за допомогою Metasploit** Літ.: [3] с. 88-110, [56]	4
8	**Енкодери та експлуатація вразливостей за допомогою Metasploit** Літ.: [3] с. 110-125, [56]	4
9	**Підсумкове заняття.** Контрольна робота	4
	Разом за семестр:	**36**

Зміст самостійної (індивідуальної) роботи

Об’єм самостійної роботи з дисципліни “Технології виявлення вразливостей та вторгнень” становить 80 годин. Він включає опрацювання теоретичного матеріалу (лекційного, методичних вказівок та літературних джерел), підготовку до виконання та захисту лабораторних робіт. Керівництво самостійною роботою та виконанням завдань здійснює викладач згідно з розкладом консультацій в позаурочний час, в тому числі із застосуванням технологій інтерактивного та дистанційного навчання.

Номер тижня	Теми самостійної роботи	Кількість годин
1	Опрацювання теоретичного матеріалу лекції №1. Підготовка до виконання лабораторної роботи №1.	4
2	Опрацювання теоретичного матеріалу лекції №2. Підготовка до виконання лабораторної роботи №1.	4
3	Опрацювання теоретичного матеріалу лекції №3. Підготовка до виконання лабораторної роботи №2. Підготовка до захисту лабораторної роботи №1.	5
4	Опрацювання теоретичного матеріалу лекції №4. Підготовка до виконання лабораторної роботи №2. Підготовка до захисту лабораторної роботи №1.	5
5	Опрацювання теоретичного матеріалу лекції №5. Підготовка до виконання лабораторної роботи №3. Підготовка до захисту лабораторної роботи №2.	4
6	Опрацювання теоретичного матеріалу лекції №6. Підготовка до виконання лабораторної роботи №3. Підготовка до захисту лабораторної роботи №2.	4
7	Опрацювання теоретичного матеріалу лекції №7. Підготовка до виконання лабораторної роботи №4. Підготовка до захисту лабораторної роботи №3.	5
8	Опрацювання теоретичного матеріалу лекції №8. Підготовка до виконання лабораторної роботи №4. Підготовка до захисту лабораторної роботи №3.	5
9	Опрацювання теоретичного матеріалу лекції №9. Підготовка до виконання лабораторної роботи №5. Підготовка до захисту лабораторної роботи №4.	4
10	Опрацювання теоретичного матеріалу лекції №10. Підготовка до виконання лабораторної роботи №5. Підготовка до захисту лабораторної роботи №4.	4
11	Опрацювання теоретичного матеріалу лекції №11. Підготовка до виконання лабораторної роботи №6. Підготовка до захисту лабораторної роботи №5.	4
12	Опрацювання теоретичного матеріалу лекції №12. Підготовка до виконання лабораторної роботи №6. Підготовка до захисту лабораторної роботи №5.	4
13	Опрацювання теоретичного матеріалу лекції №13. Підготовка до виконання лабораторної роботи №7. Підготовка до захисту лабораторної роботи №6.	4
14	Опрацювання теоретичного матеріалу лекції №14. Підготовка до виконання лабораторної роботи №7. Підготовка до захисту лабораторної роботи №6.	4
15	Опрацювання теоретичного матеріалу лекції №15. Підготовка до виконання лабораторної роботи №8. Підготовка до захисту лабораторної роботи №7.	5
16	Опрацювання теоретичного матеріалу лекції №16. Підготовка до виконання лабораторної роботи №8. Підготовка до захисту лабораторної роботи №7.	5
17	Опрацювання теоретичного матеріалу лекції №17. Підготовка до захисту лабораторної роботи №8. Підготовка до контрольної роботи.	5
18	Опрацювання теоретичного матеріалу лекції №18. Підготовка до захисту лабораторної роботи №8. Підготовка до контрольної роботи.	5
	Разом за семестр:	**80**

ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції проводяться пояснювально-ілюстративними методами з супроводом презентаційних матеріалів, лабораторні заняття проводяться практичними, продуктивними методами, з використанням інформаційно-комп'ютерних технологій.

Застосовувані при викладанні дисципліни методи навчання сприяють розвитку у студентів навичок soft skills: прилюдні захисти лабораторних робіт з обґрунтуванням прийнятих рішень щодо вибору методів рішення завдань в діалозі з викладачем і групою сприяють формуванню і удосконаленню вмінь публічних виступів, емпатичного слухання, відстоювання власної точки зору, самоаналізу і самокритики; адаптованість, вміння користуватися інтернет-ресурсами та іншими джерелами інформації, синтезувати та критично осмислювати інформацію з різних джерел передбачені специфікою дисципліни; обмежений час на виконання лабораторних робіт, контрольних завдань, чітко визначені і надані в силабусі терміни проходження контрольних точок і відпрацювання заборгованостей сприяють розвитку пунктуальності, здатності до самоорганізації та управління часом (тайм-менеджменту).

При вивченні дисципліни можуть бути зараховані результати навчання, здобуті у неформальній освіті. Визнання результатів навчання, здобутих у неформальній освіті, реалізується згідно з чинним законодавством і регулюється Положенням про порядок визнання та перезарахування результатів навчання здобувачів вищої освіти у ХНУ https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-poryadok-vyznannya-ta-perezarahuvannya-rezultativ-navchannya.pdf.

МЕТОДИ КОНТРОЛЮ

Поточний контроль здійснюється під час лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочим планом дисципліни.

При цьому використовуються такі методи поточного контролю:

- усне опитування;
- захист лабораторних робіт;
- письмова контрольна робота.

Семестровий контроль проводиться у формі іспиту. При виведенні підсумкової семестрової оцінки враховуються як результати поточного контролю, так і підсумкового контрольного заходу.

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

	Аудиторна робота	**Контрольні заходи**	**Підсумковий контрольний захід**
Вид заняття	Лабораторні роботи	Контрольна робота	Семестровий контроль (іспит)
Тема	1-4	1-5	1-5
Ваговий коефіцієнт	0,4	0,2	0,4

Оцінювання лабораторних робіт. Оцінка, яка виставляється за лабораторне заняття, складається з таких елементів: усне опитування студентів перед допуском до виконання лабораторної роботи; знання теоретичного матеріалу з теми; якість оформлення звіту; 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 лабораторне 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 лабораторне заняття викладач оголошує одразу після захисту звіту з лабораторної роботи і проставляє в електронний журнал дисципліни.

Оцінювання контрольної роботи. Контрольна робота складається з теоретичного питання та практичного завдання. Оцінювання здійснюється за чотирибальною шкалою. Оцінку «відмінно» отримує студент який дав повну письмову відповідь на теоретичне питання та правильно виконав поставлене практичне завдання. Оцінку «добре» отримує студент, який допустив дві-три несуттєві помилки при відповіді на теоретичне питання та правильно виконав поставлене практичне завдання. Оцінку «задовільно» отримує студент, який дав лише часткову відповідь на теоретичне питання або допустив суттєві помилки при виконанні практичного завдання. Оцінку «незадовільно» отримує студент, який не зміг виконати практичне завдання або не дав відповіді на теоретичне питання. Оцінку за контрольну роботу викладач проставляє в електронний журнал дисципліни не пізніше ніж через десять днів після проведення контрольного заходу.

Семестровий контроль (іспит). Підсумковий контрольний захід з дисципліни проводиться в формі іспиту. Екзаменаційний білет складається з двох теоретичних питань і практичного завдання. 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 теоретичного матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями оцінювання знань.

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 невстигаючим.

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**		
A	4,75–5,00	5	Зараховано	***Відмінно*** – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74	4		***Добре*** – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24	4		***Добре*** – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74	3		***Задовільно*** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24	3		***Задовільно*** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	2	Незараховано	***Незадовільно*** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99	2		***Незадовільно*** – необхідна серйозна подальша робота і повторне вивчення дисципліни

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ
ЗДОБУТИХ СТУДЕНТАМИ 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 ШПЗ
7. Методи усунення наслідків зараження ШПЗ
8. Технологія виявлення ШПЗ
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 (SIEM)
25. Security orchestration, automation, and response (SOAR)
26. Тестування та оцінка безпеки мережі
27. Типи мережевих тестів
28. Інструменти Nmap та Zenmap, SuperScan
29. Призначення МЕ
30. Функції МЕ
31. Підключення та налаштування апаратних МЕ
32. IDS
33. IPS
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

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни “Технології виявлення вразливостей та вторгнень” повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, розміщеною в електронному варіанті в модульному середовищі.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.
2. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. Вступ до кібербезпеки: навч. посіб. – Кропивницький: ЦНТУ, 2022. – 967 с.
3. Вступ до кібербезпеки: Методичні рекомендації до виконання лабораторних робіт для студентів денної форми навчання галузі 12 Інформаційні технології. / уклад. Смірнов О.А., Буравченко К.О., Смірнова Т.В., Конопліцька-Слободенюк О.К., Смірнов С.А., Козлов Я.О. / М-во освіти і науки України, Центральноукр. нац. техн. ун-т; – Кропивницький: ЦНТУ – 2022. – 155 с.
4. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструк-тури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.
5. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп’ютерних мережах: навч. посіб. **—** Кропивницький: Видавець Лисенко В. Ф., 2020. **—** 295 с.
6. Анна Корченко, Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія, Київ, ЦП «Компринт», 2019 – 361 с.

Додаткова

7. Основи інформаційної безпеки: навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. - 128 с.
8. Joshua Saxe, Hillary Sanders. MALWARE DATA SCIENCE: Attack Detection and Attribution. San Francisco, 2018, 279 pages
9. Методи розпізнавання кібератак: розпізнавання комп’ютерних вірусів. І.А. Терейковський, О.Г. Корченко, В.В. Погорелов. КПІ ім. Ігоря Сікорського: посібник, 2022. – 127 с.
10. Жаровський Р.О. Захист інформації у комп’ютерних системах. ТНТУ, 2019. – 268 с.
11. Богданова, Є., Чорна, Т., & Малахов, С. (2022). Огляд поточного стану загроз, що обумовлені впливом експлойтів. Комп’ютерні науки та кібербезпека, (2), 35-40. https://doi.org/10.26565/2519-2310-2022-2-04
12. Functions and Procedures. https://www.advanced-ict.info/programming/functions.html
13. Exploit database. https://www.exploit-db.com/
14. Топ-10 OWASP. https://owasp.org/www-project-top-ten/
15. Your 2023 Guide to Web Application Penetration Testing. URL:https://relevant.software/blog/penetration-testing-for-web-applications/
16. Wireshark. https://www.wireshark.org/docs/
17. Nmap. https://nmap.org/book/toc.html
18. Q. Liu, V. Hagenmeyer and H. B. Keller, "A Review of Rule Learning-Based Intrusion Detection Systems and Their Prospects in Smart Grids," in *IEEE Access*, vol. 9, pp. 57542-57564, 2021, doi: 10.1109/ACCESS.2021.3071263.
19. What is an Intrusion Prevention System (IPS)? https://informationsecurityasia.com/what-is-an-intrusion-prevention-system-ips/
20. IPS. https://www.process.com/docs/multinet5_6/install_admin/chapter_30.html
21. Яцків В. В. Опорний конспект лекцій з курсу «Тестування комп’ютерних систем на проникнення» для студентів спеціальності 125 «Кібербезпека» – Тернопіль: ТНЕУ, 2019. – 119 с.
22. Vulnerability Assessment Report: A Beginners’ Guide. https://www.getastra.com/blog/security-audit/vulnerability-assessment-report/

23. Vulnerability assessment results categories. https://www.ibm.com/docs/en/sga?topic=vulnerability-assessment-results-categories
24. Snort. https://www.snort.org/
25. Prelude. https://www.prelude-siem.com/
26. Netstat. https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/netstat
27. Zeek. https://zeek.org/
28. OSSEC. https://www.ossec.net/docs/
29. Suricata. https://suricata.io/documentation/
30. Samhain. https://www.la-samhna.de/samhain/index.html
31. Security Onion Solutions. https://securityonionsolutions.com/
32. McAfee Network Security Platform 10.1.9 Product Guide. https://docs.trellix.com/bundle/network-security-platform-10.1.x-product-guide/page/GUID-373C1CA6-EC0E-49E1-8858-749D1AA2716A.html
33. Kismet. https://www.kismetwireless.net/
34. DefensePro X: The Next Level of DDOS Protection. https://www.radware.com/products/defensepro/
35. National Institute of Standards and Technology (NIST) [Електронний ресурс]: “National Vulnerability Database (NVD). URL: http://nvd.nist.gov/.
36. Common Vulnerability Scoring System Calculator Version 3 [Електронний ресурс] URL : https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator.
37. First [Електронний ресурс] : CVSS v3 User Guide. URL : https://www.first.org/cvss/v3.1/user-guide
38. Підпалий, О. І., & Романов, О. І. (2020). Аналіз вразливості бездротової мережі WI-FI з новим протоколом захищеності WPA3. Збірник матеріалів Міжнародної науково-технічної конференції «Перспективи телекомунікацій». вилучено із http://conferenc.its.kpi.ua/proc/article/view/200855
39. Тестування на проникнення систем інтернету речей: кіберзагрози, методи та етапи ISSN 0204–3572. Електрон. моделювання. 2022. Т. 44. № 4, с. 79—104 А.І. Абакумов, В.С. Харченко DOI: https://doi.org/10.15407/emodel.44.04.079
40. Katherine Rongstad,Ruidong Zhang . Enterprise network security from cloud computing perspective. Issues in Information Systems Volume 22, Issue 3, pp. 107-113, 2021
41. Access Control List. https://learn.microsoft.com/uk-ua/windows-hardware/drivers/ifs/access-control-list
42. C. D. Motero, J. R. B. Higuera, J. B. Higuera, J. A. S. Montalvo and N. G. Gómez, "On Attacking Kerberos Authentication Protocol in Windows Active Directory Services: A Practical Survey," in IEEE Access, vol. 9, pp. 109289-109319, 2021, doi: 10.1109/ACCESS.2021.3101446.
43. Mokhtar, B.I.; Jurcut, A.D.; ElSayed, M.S.; Azer, M.A. Active Directory Attacks—Steps, Types, and Signatures. Electronics 2022, 11, 2629. https://doi.org/10.3390/electronics11162629
44. Guido Grillenmeier. Now's the time to rethink Active Directory security, Network Security, Volume 2021, Issue 7, 2021, Pages 13-16, ISSN 1353-4858, https://doi.org/10.1016/S1353-4858(21)00076-3.
45. Open Source Vulnerability Management. https://www.greenbone.net/en/open-source-vulnerability-management
46. OWASP. https://owasp.org/
47. Shodan. https://www.shodan.io/
48. Censys. https://search.censys.io/
49. Netcraft. https://sitereport.netcraft.com/
50. BGP Toolkit Home. https://bgp.he.net/
51. Tool Documentation: enum4linux. https://www.kali.org/tools/enum4linux/
52. Advanced IP Scanner. https://www.advanced-ip-scanner.com/ua/
53. Rapid7 - Practitioner-First Cybersecurity Solutions. https://www.rapid7.com/
54. Tenable Nessus. https://www.tenable.com/products/nessus
55. Metasploit Documentation. https://docs.metasploit.com/

ІНФОРМАЦІЙНІ РЕСУРСИ

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