ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра кібербезпеки

ЗАТВЕРДЖУЮ
Декан ФІТ
Тетяна ГОВОРУЩЕНКО
«31» серпня 2024 р.

СИЛАБУС

Навчальна дисципліна: "*Технології виявлення вразливостей та вторгнень*"

Освітньо-професійна програма: «Кібербезпека»

Рівень вищої освіти: перший (бакалаврський)

Загальна інформація

Позиція	Інформація
Викладач(і)	Петляк Наталія Сергіївна
Профайл викладач(ів)	https://kb.khmnu.edu.ua/petlyak-nataliya-sergiyivna/
E-mail викладача(ів)	npetlyak@khmnu.edu.ua
Контактний телефон	Наявний в ІСУ
Сторінка дисципліни в ІСУ	https://msn.khmnu.edu.ua/course/view.php?id=8956
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us02web.zoom.us/j/88595100831 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2024-2025, семестр VI (зимово-весняний)
Консультації	Очні: згідно графіку консультацій Онлайн: за необхідністю та попередньою домовленістю

Характеристика дисципліни

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
ОД	3	6	5	150	68	34	34	-	-	82	-	-	-	+

Анотація дисципліни

Дисципліна викладається для студентів очної денної форми навчання спеціальності «Кібербезпека». При викладанні дисципліни використовуються наступні форми (методи) навчання: словесні та наочні (лекції); практичні та застосування інформаційно-комп'ютерних технологій (лабораторні роботи); пояснювально-ілюстративні та дослідницькі (самостійна робота).

Пререквізити: основи інформаційної безпеки; технології програмування та алгоритмізації; операційні системи та технології їх захисту; безпека вебресурсів.

Кореквізити: комплексні системи захисту інформації.

Мета і завдання дисципліни

Метою викладання навчальної 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 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.

Завданням дисципліни є 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.

Тематичний і календарний план вивчення дисципліни

№ тижня	Тема лекції*	Тема лаб. роботи **	Самостійна роботи		
			Зміст	Год.	Література
1	**Тема 1. Вірусологія** Комп'ютерна вірусологія	**ЛР1.** Пошук вразливостей веб-сайту та застосування сканерів вразливостей GVM, OWASP	Опрацювання теоретичного матеріалу лекції №1.	4	[7] с. 68-87 [8] с. 54-78 [9] с. 28-57
2	**Тема 1. Вірусологія** Антивіруси	**ЛР1.** Підгрупа 2	Опрацювання теоретичного матеріалу лекції №2. Підготовка до виконання лабораторної роботи №1	4	[1] с. 112-121 [2] с.316-318 [10] с. 240-256 [46-47]
3	**Тема 1. Вірусологія** Інструменти та аналіз коду	**ЛР2.** Аналіз коду експлойту	Опрацювання теоретичного матеріалу лекції №3. Опрацювання теоретичного матеріалу лекції №2.	5	[11] [12] [13]
4	**Тема 1. Вірусологія** Використання вразливостей програми	**ЛР2.** Підгрупа 2	Опрацювання теоретичного матеріалу лекції №4. Підготовка до захисту лабораторної роботи №1. Підготовка до виконання лабораторної роботи №2.	5	[14] [15] [12-13]
5	**Тема 2. Засоби аналізу та тестування мережного трафіку** Аналіз мережного трафіку	**ЛР3.** Використання сканерів мережевого трафіка Wireshark та Snort	Опрацювання теоретичного матеріалу лекції №5. Опрацювання теоретичного матеріалу лекції №3.	4	[1] с. 44-62
6	**Тема 2. Засоби аналізу та тестування мережного трафіку** Інструменти моніторингу безпеки мережі	**ЛР3.** Підгрупа 2	Опрацювання теоретичного матеріалу лекції №6. Підготовка до захисту лабораторної роботи №2. Підготовка до виконання лабораторної роботи №3.	4	[1] с. 142-148 [16] [16] [25]
7	**Тема 2. Засоби аналізу та тестування мережного трафіку** Методи та інструменти тестування безпеки мережі	**ЛР4.** Розвідка на основі відкритих джерел (OSINT)	Опрацювання теоретичного матеріалу лекції №7. Опрацювання теоретичного матеріалу лекції №4.	5	[1] с. 39-44 [17]

8	**Тема 2. Засоби аналізу та тестування мережного трафіку** Міжмережні екрани	**ЛР4.** Підгрупа 2	Опрацювання теоретичного матеріалу лекції №8. Підготовка до захисту лабораторної роботи №3. Підготовка до виконання лабораторної роботи №4.	5	[1] с. 62-89 [7] с.110-113 [2] с. 318-325 [48-51]
9	**Тема 3. Системи виявлення та запобігання вторгненням** Інструменти та програми для виявлення вторгнень	**ЛР5.** Активний збір даних про мережу та пошук вразливостей	Опрацювання теоретичного матеріалу лекції №9. Опрацювання теоретичного матеріалу лекції №5.	4	[5] с. 154-205 [2] с. 325-331 [18-21]
10	**Тема 3. Системи виявлення та запобігання вторгненням** Збір інформації та сканування вразливостей	**ЛР5.** Підгрупа 2	Опрацювання теоретичного матеріалу лекції №10. Підготовка до захисту лабораторної роботи №4. Підготовка до виконання лабораторної роботи №5.	4	[22] с. 46-55 [23] [24] [17] [3] с 25-35
11	**Тема 3. Системи виявлення та запобігання вторгненням** Відкриті системи виявлення вторгнень	**ЛР6.** Використання сканерів вразливостей enum4linux, IPscanner, rapid7 та Nessus	Опрацювання теоретичного матеріалу лекції №11. Опрацювання теоретичного матеріалу лекції №6.	4	[6] с. 17-43 [25-32]
12	**Тема 3. Системи виявлення та запобігання вторгненням** Програмні та програмно-апаратні засоби виявлення вторгнень	**ЛР6.** Підгрупа 2	Опрацювання теоретичного матеріалу лекції №12. Підготовка до захисту лабораторної роботи №5. Підготовка до виконання лабораторної роботи №6.	4	[6] с. 43-66 [33-35] [52-55]
13	**Тема 4. Інструменти аналізу та оцінка вразливостей** Оцінка вразливостей кінцевого пристрою	**ЛР7.** Збір інформації та пошук вразливостей за допомогою Metasploit	Опрацювання теоретичного матеріалу лекції №13. Опрацювання теоретичного матеріалу лекції №7.	4	[36-38]

14	**Тема 4. Інструменти аналізу та оцінка вразливостей** Вразливості дротових і бездротових мереж	**ЛР7.** Підгрупа 2	Опрацювання теоретичного матеріалу лекції №14. Підготовка до захисту лабораторної роботи №6. Підготовка до виконання лабораторної роботи №7.	4	[4] с. 132-155 [39] [3] с. 88-110 [56]
15	**Тема 4. Інструменти аналізу та оцінка вразливостей** Хмарна, мобільна та безпека Інтернету речей	**ЛР8.** Енкодери та експлуатація вразливостей за допомогою Metasploit	Опрацювання теоретичного матеріалу лекції №15. Опрацювання теоретичного матеріалу лекції №8.	5	[40] [41]
16	**Тема 5. Контроль та управління доступом** Списки контролю доступу (ACL)	**ЛР8.** Підгрупа 2	Опрацювання теоретичного матеріалу лекції №16. Підготовка до захисту лабораторної роботи №7. Підготовка до виконання лабораторної роботи №8.	5	[4] с. 155-161 [42] [2] с. 331-336 [3] с. 110-125 [56]
17	**Тема 5. Контроль та управління доступом** Active Directory (частина 1)		Опрацювання теоретичного матеріалу лекції №17.	5	[43-45]
18	**Тема 5. Контроль та управління доступом** Active Directory (частина 2)		Опрацювання теоретичного матеріалу лекції №18.	5	[43-45]

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 перезарахування 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

	Аудиторна робота	**Контрольні заходи**	**Підсумковий контрольний захід**
Вид заняття	Лабораторні роботи	Тестовий контроль	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**	**Вітчизняна оцінка, критерії**	
A	4,75–5,00	зараховано	***Відмінно*** – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74		***Добре*** – повне знання навчального матеріалу з кількома

			незначними помилками
C	3,75–4,24		***Добре*** – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74		***Задовільно*** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24		***Задовільно*** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	незарахова но	***Незадовільно*** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99		***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 повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі MOODLE.

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. 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. 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. 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. 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. 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://lib.khmnu.edu.ua/asp/php_f/p1age_lib.php