ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра кібербезпеки

ЗАТВЕРДЖУЮ
Декан ФІТ
_____ Тетяна ГОВОРУЩЕНКО
«__24__» ____08_____ 2024 р.

СИЛАБУС

Навчальна дисципліна: "*Методологія організації атак та тестування на проникнення*"

Освітньо-професійна програма: «Кібербезпека та захист інформації»

Рівень вищої освіти: другий (магістерський)

Загальна інформація

Позиція	Інформація
Викладач(і)	Кльоц Юрій Павлович
Профайл викладач(ів)	http://kb.khnu.km.ua/sklad-kafedry/
E-mail викладача(ів)	klots@khmnu.edu.ua
Контактний телефон	Наявний в ІСУ
Сторінка дисципліни в ІСУ	https://msn.khnu.km.ua/course/view.php?id=7862
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us04web.zoom.us/j/8577265687 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2024-2025, семестр І (осінньо-зимовий)
Консультації	Очні: згідно графіку консультацій Онлайн: за необхідністю та попередньою домовленістю

Характеристика дисципліни

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття					Залік	Іспит
ОД	1	1	5	150	51	17	34	-	-	99	-	-	-	+

Анотація дисципліни

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

Пререквізити – вихідна

Кореквізити – технології та системи захисту інформації, моніторинг та менеджмент інформаційної безпеки.

Мета і завдання дисципліни

Метою викладання є підготовка фахівців з тестування на проникнення, на базі освоєння принципів та методів збору цифрової інформації для дослідження вразливостей операційних систем, комп'ютерних та бездротових мереж, хмарних технологій, технологій Інтернету речей та SCADA, проведення статичного аналізу вразливостей інформаційних систем, використовуючи інструменти та методи тестування на проникнення.

Предметом дисципліни є інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); інструменти та методи тестування на проникнення.

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

Компетентності:

КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.

КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

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

КФ11. Здатність проводити сканування на вразливості і розпізнавати вразливості в системах безпеки інформації, застосовувати методи виявлення вторгнень на базі хоста та мережі за допомогою технологій виявлення вторгнень, інтерпретувати інформацію, зібрану інструментами моніторингу мережі, аналізувати шкідливе програмне забезпечення.

Результати навчання:

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

РН24. Розпізнавати та класифікувати типи вразливостей і пов'язаних з ними атак, виявляти вторгнення на базі хоста та мережі за допомогою технологій виявлення вторгнень, використовувати аналізатори протоколів та виконувати аналіз трафіку на рівні пакетів, перевіряти попередження системи виявлення вторгнень щодо мережного

трафіку за допомогою інструментів аналізу пакетів для локалізації та видалення шкідливого програмного забезпечення.
РН25. Характеризувати та аналізувати мережний трафік для виявлення аномальної активності (метадані), шкідливих дій, потенційних загроз мережним ресурсам, слабких місць, методів експлуатації, впливу на систему та інформацію.

Студент, який успішно завершив вивчення дисципліни, повинен: *аналізувати* та *оцінювати* захищеність інформаційних систем, прикладного та спеціалізованого програмного забезпечення; *обґрунтовувати* використання, *впроваджувати* та *аналізувати* кращі світові стандарти, практики з метою розв'язання задач професійної діяльності, пов'язаних з виявленням вразливостей та тестуванням на проникнення; *виявляти* уразливості інформаційних систем та ресурсів, *аналізувати* та *оцінювати* на основі виявлених вразливостей ризики для інформаційної безпеки та/або кібербезпеки організації; *приймати* обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у ситуаціях, пов'язаних з виявленням вразливостей та тестуванням на проникнення; *розпізнавати* та *класифікувати* типи вразливостей і пов'язаних з ними атак, *використовувати* аналізатори протоколів та *виконувати* аналіз трафіку на рівні пакетів; *характеризувати* та *аналізувати* мережний трафік для виявлення слабких місць, методів експлуатації, впливів на систему та інформацію.

Тематичний і календарний план вивчення дисципліни

№ тижня	Тема лекції*	Тема лаб. роботи **	Самостійна роботи		
			Зміст	**Год.**	**Література**
1	**Тема 1. Технології тестування на проникнення та аналіз вразливостей** Методи тестування безпеки систем	**ЛР1.** Розвідка та збирання інформації з відкритих джерел за допомогою Maltego	Опрацювання теоретичного матеріалу лекції №1.	5	[4] с. 84-105 [5] с. 383-411 [13] [14] [15] [22]
2	-	**ЛР1.** Підгрупа 2	Підготовка до виконання та захисту лабораторної роботи №1.	6	[4] с. 115-123
3	**Тема 1. Технології тестування на проникнення та аналіз вразливостей** Розвідка на основі відкритих джерел (OSINT)	**ЛР2.** Розгортання pen-test станції. Підготовка до роботи Metasploit та postgresql	Опрацювання теоретичного матеріалу лекції №2.	5	[4] с. 106-149 [8] с. 144-164 [12]
4	-	**ЛР2.** Підгрупа 2	Підготовка до виконання та захисту лабораторної роботи №2.	6	[1] с. 10-38
5	**Тема 1. Технології тестування на проникнення та аналіз вразливостей** Аналіз вразливостей та тестування на проникнення комп'ютерних мереж	**ЛР3.** Збір інформації та аналіз вразливостей за допомогою Metasploit	Опрацювання теоретичного матеріалу лекції №3.	5	[4] с. 149-237 [6] с. 142-224 [7] с. 89-114 [16]
6	-	**ЛР3.** Підгрупа 2	Підготовка до виконання та захисту лабораторної роботи №3.	6	[1] с. 40-88

7	**Тема 1. Технології тестування на проникнення та аналіз вразливостей** Аналіз вразливостей та тестування на проникнення бездротових мереж, Інтернету речей, OT/SCADA та хмарних технологій	**ЛР4.** Дослідження використання енкодерів для обходу захисту антивірусних програм	Опрацювання теоретичного матеріалу лекції №4.	5	[4] с. 364-449 [6] с. 541-586 [10] с. 53-66
8	-	**ЛР4.** Підгрупа 2	Підготовка до виконання та захисту лабораторної роботи №4.	6	[3] с. 189-207
9	**Тема 1. Технології тестування на проникнення та аналіз вразливостей** Аналіз вразливостей веб-ресурсів	**ЛР5.** Дослідження експлуатації та пост-експлуатації виявлених вразливостей	Опрацювання теоретичного матеріалу лекції №5.	5	[4] с. 316-364 [6] с. 280-360
10	-	**ЛР5.** Підгрупа 2	Підготовка до виконання та захисту лабораторної роботи №5.	6	[1] с. 188-237
11	**Тема 1. Технології тестування на проникнення та аналіз вразливостей** Бінарний аналіз вразливостей програмного забезпечення	**ЛР6.** Дослідження стійкості паролів WPA2/WPA за допомогою Hashcat в Kali Linux	Опрацювання теоретичного матеріалу лекції №6.	5	[10] с. 66-74 [11] с. 44-72, 144-154 [17] [18] [19] [20] [21]
12	-	**ЛР6.** Підгрупа 2	Підготовка до виконання та захисту лабораторної роботи №6.	6	[1] с. 341-359
13	**Тема 2. Теоретичні засади тестування на проникнення** Підходи до тестування на проникнення та юридичні аспекти	**ЛР7.** Дослідження стійкості мережі через стрес-тести (DoS веб-сайту) з SlowHTTPTest в Kali Linux	Опрацювання теоретичного матеріалу лекції №7.	5	[2] с. 5-36 [9]
14	-	**ЛР7.** Підгрупа 2	Підготовка до виконання та захисту лабораторної роботи №7.	6	[3] с. 175-189
15	**Тема 2. Теоретичні засади тестування на проникнення** Організаційне забезпечення тестування на проникнення	**ЛР8.** Аналіз уразливостей WordPress: WPScanner і Plecost. Робота з W3af в Kali Linux	Опрацювання теоретичного матеріалу лекції №8.	5	[2] с. 36-55 [9]
16	-	**ЛР8.** Підгрупа 2	Підготовка до виконання та захисту лабораторної роботи №8.	6	[3] с. 175-189

17	**Тема 2. Теоретичні засади тестування на проникнення** Методика та документаційне забезпечення тестування на проникнення	Підсумкове заняття **Тестування**	Опрацювання теоретичного матеріалу лекції №9. Підготовка до тестування за матеріалом лекцій 7-9.	10	[2] с. 55-70 [4] с. 465-483 [9]

*** лекції проводяться по 2 години раз на два тижні;**
**** лабораторні проводяться по 4 години раз в два тижні.**

ПОЛІТИКА ДИСЦИПЛІНИ

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

Виконуючи усі навчальні завдання з дисципліни, студент має дотримуватися політики доброчесності. В 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	Тестування	Семестровий контроль (іспит)
Тема	1	2	1-2
Ваговий коефіцієнт	0,4	0,2	0,4

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

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

тижні до кінця теоретичних занять у семестрі.

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

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

Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту

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

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

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

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

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

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

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

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	**Узагальнений критерій**
Відмінно	Студент глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає, логічний виклад відповіді державною мовою (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними інструментами. Студент не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві-три несуттєві похибки.
Добре	Студент виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом і фаховою термінологією, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання закономірностей тощо. Відповідь студента будується на основі самостійного мислення. Студент у відповіді допустив дві–три несуттєві помилки.

Задовільно	Студент виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, допускає неточності і суттєві помилки у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно	Студент виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка "незадовільно" виставляється студенту, який не може продовжити навчання без додаткової роботи з вивчення дисципліни.

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

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

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

Студент, який набрав позитивний середньозважений бал за поточну роботу і не здав підсумковий контрольний захід (іспит), вважається 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	***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	***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. Підходи до виявлення вразливостей.
2. Підходи до оцінювання безпеки інформаційних систем.
3. Методологія організації атак на інформаційну безпеку.
4. Методика оцінювання безпеки брандмауера.
5. Методика оцінювання безпеки маршрутизатора.
6. Методика оцінювання безпеки комутатора.
7. Методика оцінювання безпеки систем виявлення вторгнень.
8. OSINT через Всесвітню павутину (WWW)
9. Аналіз веб-сайтів
10. DNS-опитування.
11. Автоматизація роботи з OSINT за допомогою інструментів/фреймворків/скриптів.
12. Інформація зовнішньої мережі, розвідка, сканування вразливостей.
13. Внутрішня мережна інформаційна розвідка, сканування вразливостей.
14. Дослідження вразливостей локальної системи.
15. Дослідження вразливостей віддаленої системи.
16. Дослідження вразливостей WLAN.
17. Процес аналізу трафіка WLAN.
18. Методологія проведення атаки на WLAN.
19. Атаки на Bluetooth.
20. Дослідження вразливостей IoT.
21. Дослідження вразливостей OT/SCADA.
22. Проблеми безпеки в IoT.
23. Проблеми безпеки OT/SCADA.
24. Поверхня атаки і пов’язані загрози.
25. Спеціальні методики виявлення вразливостей IoT.
26. Спеціальні методики виявлення вразливостей OT/SCADA.
27. Дослідження вразливостей хмари.
28. Обмеження хмарних архітектур з точки зору інформаційної безпеки.
29. Спеціальні методики виявлення вразливостей хмари.
30. Принципи та підходи бінарного аналізу програмного забезпечення.
31. Інструментарій бінарного аналізу.
32. Дослідження вразливостей програмного забезпечення.
33. Безпека та тестування на проникнення.
34. Види тестування на проникнення.
35. Цілі тестування на проникнення.
36. Класифікація тестування на проникнення.
37. Юридичні причини тестування на проникнення.
38. Правові рамки тестування на проникнення.
39. Важливі умови договору між тестером на проникнення та клієнтом.
40. Організаційні вимоги до тестування на проникнення.
41. Вимоги до персоналу.
42. Технічні вимоги тестування на проникнення.
43. Етичні питання тестування на проникнення.
44. Вимоги до методики випробування на проникнення.
45. П'ять фаз тесту на проникнення.
46. Етап підготовки тестування.
47. Етап розвідки.
48. Етап аналізу інформації/ризиків.
49. Етап активних спроб вторгнення.
50. Етап остаточного аналізу.
51. Етап написання звітів.

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. Metasploit Penetration Testing Cookbook. Third Edition/ Daniel Teixeira, Abhinav Singh, Monika Agarwal. Packt Publishing 2018. 398 p.
2. Опорний конспект лекцій з курсу «Тестування комп'ютерних систем на проникнення»/ Яцків В.В. Тернопіль: ТНЕУ, 2019. 119 с.
3. Metasploit for Beginners/ Sagar Rahalkar. Packt Publishing 2017. 232 p.
4. Kali Linux 2018: Assuring Security by Penetration Testing. Fourth Edition/ Shiva V. N Parasram, Alex Samm, Damian Boodoo, Gerard Johansen, Lee Allen, Tedi Heriyanto, Shakeel Ali. Packt Publishing 2018. 502 p.
5. Network Analysis Using Wireshark 2 Cookbook. Second Edition/ Nagendra Kumar Nainar, Yogesh Ramdoss, Yoram Orzach. Packt Publishing 2018. 434 p.
6. Nmap: Network Exploration and Security Auditing Cookbook. Second Edition/ Paulino Calderon. Packt Publishing 2017. 786 p.
7. Hands-On Penetration Testing on Windows/ Phil Bramwell. Packt Publishing 2018. 424 p.
8. Основи кримінального аналізу: навчальний посібник/ І. А. Федчак. Львів: Львівський державний університет внутрішніх справ, 2021. 288 с.
9. Пентест від А до Я: посібник з тестування на проникнення [Електронний ресурс]. Режим доступу: https://kr-labs.com.ua/blog/testuvannya-na-pronyknennya-pentest-vid-a-do-ya
10. Методи штучного інтелекту в кібербезпеці: навч. посіб./ І.В. Стьопочкіна, О.М. Новіков. Київ: КПІ ім. Ігоря Сікорського, 2022. 82 с.
11. Тестування програмного забезпечення. Навчальний посібник/ Авраменко А.С., Авраменко В.С., Косенюк Г.В. Черкаси: ЧНУ імені Богдана Хмельницького, 2017. 284 с.

Додаткова

12. OSINT, як перспективний інструмент контролю за лобістською діяльністю в контексті державної безпеки/ Яровой, Т. С. Експерт: парадигми юридичних наук і державного управління, 2019, 4(6), 201-208. https://doi.org/10.32689/2617-9660-2019-4(6)-201-208
13. Модель нелегітимного абонента забезпечення безпеки IP-телефонії/ О. С. Андрощук, В. М. Джулій, Ю. П. Кльоц, І. В. Муляр// Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах» 2020. № 2. С. 39-45.
14. Підвищення функціональності і стабільності завадостійких безпроводових інформаційно-комунікаційних систем/ В.М. Джулій, Ю.П. Кльоц, В.С. Орленко, В.Ю. Тітова, Ю.В. Хмельницький// Вісник Хмельницького національного університету. Технічні науки. 2021. № 1. С. 12–16.
15. Дослідження характеристик надійності та інформаційної безпеки вузлів комп'ютерної мережі/ І. В. Толок, Ю. П. Кльоц, А. О. Рамський, В. В. Рикун // Тези доповідей XVI Міжнародної науково-практичної конференції "Військова освіта і наука: сьогодення та майбутнє", 27 листоп. 2020 р. Київ: ВІКНУ, 2020. Т. 1.С. 63–64.
16. Тестування обладнання корпоративної мережі/ Т. М. Кисіль, Ю. П. Кльоц, Т. В. Бондаренко, Є. С. Шаховал // Тези доповідей XVI Міжнародної науково-практичної конференції "Військова освіта і наука: сьогодення та майбутнє", 27 листоп. 2020 р. Київ: ВІКНУ,2020. Т. 1. С. 39–40.
17. Software Vulnerability Analysis and Discovery Using Deep Learning Techniques: A Survey/ Zeng, Peng & Lin, Gunjun & Pan, Lei & Yonghang, Tai// IEEE Access. 10.1109/ACCESS.2020.3034766.
18. Software vulnerability prediction: A systematic mapping study/ Ilias Kalouptsoglou, Miltiadis Siavvas, Apostolos Ampatzoglou, Dionysios Kehagias, Alexander Chatzigeorgiou// Information

and Software Technology, Volume 164, 2023, 107303, ISSN 0950-5849, https://doi.org/10.1016/j.infsof.2023.107303.
19. BVDetector: A program slice-based binary code vulnerability intelligent detection system/ Junfeng Tian, Wenjing Xing, Zhen Li// Information and Software Technology, Volume 123, 2020, 106289, ISSN 0950-5849, https://doi.org/10.1016/j.infsof.2020.106289.
20. Automated Binary Analysis: A Survey/ Liu, Zian & Chen, Chao & Ejaz, Ahmed & Liu, Dongxi & Zhang, Jun// 2023. 10.1007/978-3-031-22677-9_21.
21. A Systematic Review of Binary Program Vulnerabilities Feature Extraction and Discovery Strategy Generation Methods/ Bo Zhang, Zesheng Xi// Journal of Physics: Conference Series 1827, 2021. 012090 doi:10.1088/1742-6596/1827/1/012090
22. Security testing technology based on the provisions of the simulation models scaling theory/ Kovalenko O. // Ukrainian Scientific Journal of Information Security, 2018, vol. 24, issue 2, PP.110-117

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