ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра кібербезпеки

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

СИЛАБУС

Навчальна дисципліна: “*Безпека вебресурсів*”

Освітньо-професійна програма: «Кібербезпека та захист інформації»

Рівень вищої освіти: перший (бакалаврський)

Загальна інформація

Позиція	Інформація
Викладач(і)	Муляр Ігор Володимирович
Профайл викладач(ів)	https://kb.khmnu.edu.ua/mulyar-igor-volodymyrovych
E-mail викладача(ів)	muliariv@khmnu.edu.ua
Контактний телефон	+3 8 067 938-15-44
Сторінка дисципліни в ІСУ	https://msn.khmnu.edu.ua/course/view.php?id=6795
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us04web.zoom.us/j/5011940672 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2024-2025, семестр IV (зимово-весняний)
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	2	4	5	150	54	18	36	-	-	96	-	-	+	-

Анотація дисципліни

Дисципліна викладається для студентів очної денної форми навчання спеціальності «Кібербезпека та захист інформації». При викладанні дисципліни використовуються наступні форми (методи) навчання: пояснювально-ілюстративні, практичні, продуктивні, контекстні, застосування інформаційно-комп’ютерних технологій.

Пререквізити: основи інформаційної безпеки; операційні системи та технології їх захисту.

Кореквізити: комплексні системи захисту інформації.

Анотація дисципліни

Дисципліна формує у студентів знання про архітектуру веб-систем і вебдодатків, класифікацію веб-атак (вразливостей), принципи тестування вебресурсів, основні поняття аудиту вебресурсів, методику організації та проведення аудиту вебресурсів.

Дисципліна викладається для студентів денної форми навчання спеціальності «Кібербезпека». При викладанні дисципліни використовуються наступні форми (методи) навчання: пояснювально-ілюстративні, практичні, продуктивні, контекстні, застосування інформаційно-комп'ютерних технологій (MS Visual studio, ПЗ для тестування захищеності вебдодатків).

Пререквізити: захищені бази даних.

Кореквізити: проектно-технологічна практика, комплексні системи захисту інформації: проектування, в провадження, супровід.

Мета і завдання дисципліни

Дисципліна «Безпека вебресурсів» - складова професійної підготовки бакалаврів зі спеціальності «Кібербезпека», є однією з профілюючих дисциплін.

Метою викладання навчальної дисципліни «Безпека вебресурсів» є формування у майбутніх спеціалістів умінь та компетенцій для оцінювання та забезпечення необхідного рівня захищеності вебресурсів; розвиток у студентів фахового стилю мислення; надання глибоких та міцних знань з питань сучасного програмно-апаратного забезпечення вебресурсів, тощо.

Предметом дисципліни є сучасні програмні та програмно-апаратні методи та засоби оцінювання та забезпечення необхідного рівня захищеності вебресурсів.

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*:**

ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

результати навчання:

ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

Студент, який успішно завершив вивчення дисципліни, повинен: *реалізовувати* заходи з протидії отриманню несанкціонованого доступу до вебресурсів в інформаційних та інформаційно-телекомунікаційних системах; *використовувати* сучасні методи та моделі інформаційної безпеки та/або кібербезпеки, теорії та методи захисту для забезпечення безпеки вебресурсів, як елементів інформаційно-телекомунікаційних систем.

Тематичний і календарний план вивчення дисципліни

№ тиж-ня	Тема лекції*	Тема лаб. роботи **	Самостійна роботи		
			Зміст	Год.	Література
1	**Архітектура веб-систем і вебдодатків** Основні поняття та термінологія. Архітектура "файл-сервер". Архітектура "клієнт-сервер". Архітектура розподілених систем. Архітектура вебдодатків	**ЛР №1** Збирання інформації про веб-ресурси. Виявлення вразливостей вебдодатків засобами сканування. Аналіз HTTP- параметрів для запитів GET/POST	Опрацювання теоретичного матеріалу лекції №1. Підготовка до виконання ЛР №1.	6	[8] с. 272-284 [9] с. 34-47 [10] chapter 2 [13] с. 4-9 [15]
2	**Вимоги до захисту вебресурсів (частина 1)** Ідентифікація та аутентифікація. Обробка помилок, логування дій користувачів та ведення журналу. Обробка вхідних і вихідних даних	-	Опрацювання теоретичного матеріалу.	5	[4] [10] chapter 4
3	**Вимоги до захисту вебресурсів (частина 2)** Конфігурація та операції. Управління сеансами. Контроль доступу	**ЛР №2** Виявлення вразливостей вебсервера за допомогою інструментів мережевого сканування	Опрацювання теоретичного матеріалу лекції №2. Підготовка до виконання ЛР №2. Підготовка до захисту ЛР №1.	6	[4] [8] с. 272-284 [9] с. 6-47 [10] chapter 4 [13] с. 4-14
4	**Організація та способи передачі даних мережі Інтернет** Стек протоколів TCP/IP Система доменних імен DNS Протоколи Інтернет прикладного рівня	-	Опрацювання теоретичного матеріалу.	5	[1] с. 9-26 [11] с. 446-485
5	**Захист інформації у гіпертекстових протоколах** HTTP-запити та відповіді, методи та повідомлення. HTTPS (протокол передачі гіпертексту через захищені сокети). Cookie	**ЛР №3** Виявлення та аналіз ін'єкцій (SQL, Function, code, command)	Опрацювання теоретичного матеріалу лекції №3. Підготовка до виконання ЛР №3. Підготовка до захисту ЛР №2.	6	[1] с. 9-26 [9] с. 6-47 [12] с. 39-71, с. 601-613 [13] с. 9-14, с. 21-26

6	**Захист інформації на рівні сокетів** Протокол SSL (Secure Sockets Layer). Симетричне та асиметричне шифрування в протоколах обміну інформацією	-	Опрацювання теоретичного матеріалу.	5	[1] с. 9-26 [2] с. 47-69
7	**Захист інформації у протоколах доступу до об'єктів** Використання та захист протоколу простого доступу до об'єктів (SOAP). Відмінності між SOAP і REST	**ЛР №4** Прогнозування/фіксація сесії (Session Prediction/Fixation)	Опрацювання теоретичного матеріалу лекції №4. Підготовка до виконання ЛР №4. Підготовка до захисту ЛР №3.	6	[8] с. 284-296 [12] с. 601-613 [13] с. 21-32 [16]
8	**Захист інформації у поштових протоколах** Принципи організації електронної пошти. Поштові сервери, шлюзи і клієнти, як об'єкт захисту. Захист конфіденційності у протоколах електронної пошти (IMAP, POP3, SMTP, UUCP)	-	Опрацювання теоретичного матеріалу.	5	[1] с. 9-26 [14] с. 219-227 [17] с. 12-16
9	**Захист інформації у проксі-серверах** Призначення та типи проксі-серверів. Реалізації проксі серверів та їх характеристики, як об'єктів захисту. Захист від перехоплення проксі	**ЛР №5** Аналіз та виявлення XSS-атак	Опрацювання теоретичного матеріалу лекції №5. Підготовка до виконання ЛР №5. Підготовка до захисту ЛР №4.	6	[6] с. 77-97 [8] с. 284-296 [12] с. 824-842 [13] с. 28-32
10	**Теоретичні відомості про веб-атаки** Приклади веб-атак Цілі веб-атак	-	Опрацювання теоретичного матеріалу.	5	[3]

11	**Класифікація веб-атак та вразливостей (частина 1)** Аутентифікація (Brute Force, недостатня аутентифікація, небезпечне відновлення паролів). Авторизація (передбачуване значення ідентифікатора сесії, недостатня авторизація, відсутність таймауту сесії, фіксація сесії)	**ЛР №6** Аналіз та виявлення міжсайтової підробки запитів CSRF	Опрацювання теоретичного матеріалу лекції №6. Підготовка до виконання ЛР №6. Підготовка до захисту ЛР №5.	6	[12] с. 159-255, с. 824-842 [17] с. 12-16
12	**Класифікація веб-атак та вразливостей (частина 2)** Виконання коду (переповнення буфера, атака на функції форматування рядків, LDAP Injection, виконання команд ОС, SQL Injection, SSI Injection, XPath Injection) Атаки на клієнтів (підміна вмісту, Clickjacking, міжсайтовий скріптинг (XSS), розщеплення HTTP-запиту, міжсайтова підробка запиту (CSRF))	-	Опрацювання теоретичного матеріалу.	5	[12] с. 287-354 с. 431-571

13	**Класифікація веб-атак та вразливостей (частина 3)** Розголошення інформації (індексування директорій, ідентифікація додатків, витік інформації, зворотний шлях в директоріях). Логічні атаки (зловживання функціональними можливостями, відмова в обслуговуванні (DoS-атака), недостатня протидія автоматизації, недостатня перевірка процесу)	**ЛР №7** Атаки на авторизацію, парольні атаки	Опрацювання теоретичного матеріалу лекції №7. Підготовка до виконання ЛР №7. Підготовка до захисту ЛР №6.	6	[12] с. 257-287 с. 405-431, с. 747-771 [17] с. 12-16
14	**Способи захисту від веб-атак** Загальні поради для захисту від веб-атак. Захист вебдодатків	-	Опрацювання теоретичного матеріалу.	5	[4]
15	**Проект тестування OWASP** Основні принципи тестування та оцінювання безпеки вебдодатків. Програмні засоби для тестування та оцінювання безпеки вебдодатків. Виведення вимог до оцінювання безпеки вебдодатків	**ЛР №8** Методи та засоби виявлення XML-атаки XXE ін'єкції	Опрацювання теоретичного матеріалу лекції №8. Підготовка до виконання ЛР №8. Підготовка до захисту ЛР №7.	6	[5] с. 1-73 [12] с. 669-699, с. 747-771
16	**Забезпечення технологій вебдодатків (SWAT)** SWAT DSL. Опис DSL та структури даних Повторно використовувані HTTP-запити. Тести безпеки, інтегровані в робочі процеси розробки та тестування	-	Опрацювання теоретичного матеріал.	5	[12] с. 117-157

17	**Аудит та журнали безпеки** Відслідковування подій веб-додатку. Основні етапи аудиту безпеки. Ведення та керування журналами безпеки	**Тестування**	Опрацювання теоретичного матеріалу лекції №9. Підготовка до захисту ЛР №8. Підготовка до тестування.	8	[10] chapter 8, 9 [12] с. 669-699

*** лекції проводяться по 2 години раз в 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, лабораторні роботи 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.

Набуті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок перезарахування результатів навчання та визначення академічної різниці у ХНУ https://www.khnu.km.ua/root/files/01/10/03/006.pdf.

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	-
Тема	1-4	1-4	-
Ваговий коефіцієнт	0,45	0,15	-

<u>Оцінювання лабораторних робіт</u>. 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 тестових завдань. Контрольний захід (тест) для кожного студента складається з тридцяти тестових завдань, кожне з яких оцінюється одним балом. Максимальна сума балів, яку може набрати студент, складає 30.

Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту

Сума балів за тестове завдання	1–15	16–21	22–27	28–30
Оцінка за 4-ри бальною шкалою	2	3	4	5

На тестування відводиться 30 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 30 хвилин студенти здають викладачу завдання з талонами відповідей.

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

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

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.

Студент, який не набрав позитивний середньозважений бал за поточну роботу або не виконав індивідуальний план з дисципліни повністю, вважається невстигаючим.

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».

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

Співвідношення інституійної 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. Протокол передачі гіпертексту.
2. HTTP-запити та відповіді, методи та повідомлення.
3. Кукі.
4. HTTPS (протокол передачі гіпертексту через захищені сокети).
5. Протокол SSL (Secure Sockets Layer).
6. Симетричне та асиметричне шифрування.
7. Перехоплення проксі та HTTPS.
8. Використання протоколу простого доступу до об’єктів (SOAP).
9. Протокол SMTP (Simple Mail Transfer Protocol).
10. Протокол поштового відділення (POP3).
11. Протокол доступу до Інтернету (IMAP).
12. Архітектура веб-систем і вебдодатків.
13. Об’єкти захисту/атаки.
14. Класифікація веб-атак (уразливості).
15. Груба сила (Brute Force).
16. Недостатня аутентифікація.
17. Недостатнє відновлення пароля (перевірка слабкого відновлення пароля).
18. Прогнозування вхідних даних/сеансів.
19. Недостатня авторизація.
20. Недостатнє закінчення сеансу.
21. Фіксація сеансу.
22. Викрадення сеансу.
23. Перехресні сценарії (XSS).
24. Сценарії крос-кадрів (XFS) або iframe-ін’єкція.
25. Підробка запитів на місцях, CSRF.
26. Зловживання JSON.
27. Переповнення буфера.
28. LDAP-ін’єкція.
29. SQL-ін’єкція.
30. SSI-ін’єкція.
31. XPath-ін’єкція.
32. Індексування каталогів.
33. Витоки інформації.
34. Пошук шляху (трасування).
35. Передбачуване розташування ресурсів.
36. Забезпечення технологій вебдодатків (SWAT).
37. Обробка помилок та ведення журналу.
38. Аутентифікація.
39. Обробка вхідних і вихідних даних.
40. Конфігурація та операції.
41. Управління сеансами.
42. Контроль доступу.
43. Проект тестування OWASP.
44. Принципи тестування.
45. Пояснення техніки тестування.
46. Виведення вимог до тестування безпеки.
47. Тести безпеки, інтегровані в робочі процеси розробки та тестування.
48. Аналіз і звітність тестових даних безпеки.
49. Інструменти тестування.
50. Основні поняття аудиту вебдодатків.
51. Методика організації та проведення аудиту вебдодатків.

52. Призначення проксі-серверів.
53.Типи проксі-серверів.
54. Реалізації проксі серверів та їх характеристики

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни «Безпека вебресурсів» повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі - https://msn.khnu.km.ua/course/view.php?id=6795

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

№	Назва	Режим доступу
1.	Технології та протоколи інфокомунікаційних мереж. Частина 1 [Електронний ресурс]/ О.Л. Недашківський. – Київ, 2017.	http://www.dut.edu.ua/uploads/l_1799_76743031.pdf
2.	Технології забезпечення безпеки мережевої інфраструктури/ В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.	http://elibrary.kubg.edu.ua/id/eprint/27191/1/VL_Buriachok_TZBMI.pdf
3.	Відкритий проект захисту вебдодатків (OWASP). Стандарт оцінювання відповідності безпеки додатків 3.0 [Електронний ресурс]. – 2015.	https://owasp.org/www-pdf-archive/ASVS_3_0_Ukrainian_Beta.pdf
4.	Основи інформаційної та кібернетичної безпеки. Навчальний посібник/ В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К., 2018. – 320 с.	http://elibrary.kubg.edu.ua/id/eprint/27370/1/V_Buriachok_Posibnik_2019_FITU.pdf
5.	Технології захисту інформації / Ю. А. Тарнавський – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.	https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf
6.	Інформаційна безпека: навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєвта інші; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.	https://drive.google.com/file/d/1Zqzz0pxqtm8KfmDnUvqYRWDYi0o6qsR_/view?usp=sharing
7.	Захист веб-сервісів: лабораторний практикум [Електронний ресурс]/ І.А. Терейковський, Л.О. Терейковська, К.О. Радченко, С.О. Гнатюк. – Київ: КПІ ім. Ігоря Сікорського, 2018.	https://ela.kpi.ua/bitstream/123456789/22234/1/Zahist_web_servisiv_Laboratornyi_praktikum.pdf
8.	Professional Pen Testing for Web Applications (Programmer to Programmer)/ Andres Andreu. – Wrox, 2006. – 548 p.	https://drive.google.com/file/d/1erFjeX63JwhWM4dm5NQ3EvDjS2mUy4OT/view?usp=sharing
9.	Конспект лекцій з дисципліни «Захист інформації у комп'ютерних системах»/ Р.О. Жаровський. – Тернопіль, 2019. – 268 с	http://elartu.tntu.edu.ua/bitstream/lib/29278/1/%21%21_Lek_print_zahust_123.pdf
10.	The Web Applicaion Hackers's Handbook: Finding and Exploiting Security Flaws/D. Stuttard, M. Pinto. - John Wiley & Sons, Inc, 2011. – 877 p.	http://index-of.es/EBooks/11_TheWeb%20Application%20Hackers%20Handbook.pdf
11.	Методичні вказівки до виконання практичних робіт з курсу «Безпека програм та даних» [Електронний ресурс]/ Р.П. Шевчук, І.А. Дарморост. – Тернопіль, 2018.	https://drive.google.com/file/d/1nxSPy2HrvXjhYzAU-4wzNBbeUrSNPuR9/view?usp=sharing
12.	Протоколи SLI, PPP, SMTP і POP3. Поняття DNS, DHCP, RAS [Електронний ресурс]	http://lib.mdpu.org.ua/e-book/oi/lection3.htm

Додаткова

13.	OWASP Foundation. Testing Guide v4.0 [Електронний ресурс]. – 2019.	https://owasp.org/www-pdf-archive/OWASP_Application_Security_Verification_Standard_4.0-en.pdf
14.	Botnets 1st Edition The Killer Web Applications/ Craig Schiller	https://doc.lagout.org/security/Botn

	James Binkley. – Syngress, 2007. – 480 p.	ets%20-%20The%20killer%20web%20applications.pdf
15.	Bulletproof SSL and TLS: Understanding and deploying SSL/TLS and PKI to secure servers and web applications [Електронний ресурс]/ I. Ristic. – Feisty Duck Limited, 2014.	https://www.feistyduck.com/books/bulletproof-ssl-and-tls/bulletproof-ssl-and-tls-introduction.pdf
16.	Architecture Modeling and Analysis of Security in Android Systems/ B. Schmerl et al. – Software Architecture. – 2016. – P. 274-290.	http://acme.able.cs.cmu.edu/pubs/uploads/pdf/andorid-modeling-security-submitted.pdf
17.	Проблеми інформаційної безпеки в Україні, шляхи їх вирішення/ М. Згуровський. – Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2018. – С. 10 – 14.	https://ela.kpi.ua/handle/123456789/15949
18.	Безпека вебдодатків: актуальні проблеми та їх аналіз/ О. Бондаренко, І. Ушкаленко. – Формування ринкової економіки в Україні. – 2017. - Вип. 38. - С. 28-36.	http://socrates.vsau.org/repository/getfile.php/17100.PDF
19.	Удосконалення захисту вебресурсів від атак на основі комбінованого евристично-статистичного підходу/ Д.П. Присяжний. – Реєстрація, зберігання і обробка даних. – 2016. – Т. 18, № 1. - С. 63-69.	http://dspace.nbuv.gov.ua/handle/123456789/131601
20.	Основи сучасних веб-технологій. Ч.1: навч. посіб./ Л. В. Зубик, І. М. Карпович, О. М. Степанченко. – Рівне : НУВГП, 2016. – 290 С.	http://ep3.nuwm.edu.ua/3686/
21.	Універсальній метод захисту вебдодатків/ І.В. Василенко. – Системи обробки інформації. – 2016. – вип.1 (138). – С. 122-124	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwilz8_zjM3rAhWOjYsKHdIjC2UQFjAAegQIBRAB&url=http%3A%2F%2Fwww.hups.mil.gov.ua%2Fperiodic-app%2Farticle%2F15259%2Fsoi_2016_1_27.pdf&usg=AOvVaw14lPeMosea6LfLA3BV-jdT
22.	Класифікація профілів інформаційної безпеки акторів у соціальних інтернет-сервісах (на прикладі мікроблогу Twitter) / Р. В. Грищук, В. М. Мамарєв, К. В. Молодецька-Гринчук. – Інформаційні технології та комп'ютерна інженерія. – 2017. – № 2. – С.12-19	https://itce.vntu.edu.ua/index.php/itce/article/view/672
23.	Метод оцінювання ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах / К. Молодецька-Гринчук. – Автоматизація технологічних і бізнес-процесів. – 2017. – Volume 9, Issue 2. – С. 36-42	https://journals.onaft.edu.ua/index.php/atbp/article/view/560
24.	Метод виявлення ознак інформаційних впливів у соціальних інтернет-сервісах за змістовними ознаками / К. В. Молодецька-Гринчук. – Радіоелектроніка, інформатика, управління. - 2017. - № 2. - С.117-126.	http://nbuv.gov.ua/UJRN/riu_2017_2_15
25.	Виявлення інформаційних впливів у соціальних інтернет-сервісах на основі інтелектуального аналізу текстового контенту / К. В. Молодецька-Гринчук // Актуальні питання забезпечення кібербезпеки та захисту інформації : тези доп. учасн. III міжнар. наук.-практ. конф., 22–25 лют. 2017 р. – К. : Європ. ун-т, 2017. – С. 121–122.	http://ir.znau.edu.ua/handle/123456789/7865

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання (розміщені усі необхідні матеріали з дисципліни, в тому числі завдання для поточного та семестрового контролю знань). Доступ до ресурсу: https://msn.khnu.km.ua/course/view.php?id=6795
2. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.