ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет програмування та комп'ютерних і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем і мереж

ЗАТВЕРДЖУЮ
Декан ФПКТС
_____ Савенко О.С.
підпис
«31» 08 2020 р.

СИЛАБУС
Навчальна дисципліна: "Безпека Web-ресурсів"

Освітньо-професійна програма: «Кібербезпека»

Рівень вищої освіти: перший (бакалаврський)

Загальна інформація

Позиція	Інформація
Викладач(і)	Молодецька Катерина Валеріївна
Профайл викладач(ів)	http://ksm.khnu.km.ua/sklad-kafedry/
E-mail викладача(ів)	kksmkhnu@gmail.com
Контактний телефон	Наявний в ІСУ
Сторінка дисципліни в ІСУ	https://msn.khnu.km.ua/enrol/index.php?id=6795
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us04web.zoom.us/j/ 5212277 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2021-2022, семестр V (осінньо-зимовий)
Розклад	
Консультації	

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
Д	3	5	5	150	68	34	34	-	-	82	-	-	-	+

Анотація дисципліни

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

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 веб-додатків).

Пререквізити: захищені бази даних.

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

Мета і завдання дисципліни

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

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

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

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

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

результати навчання:

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

РН 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 веб-ресурсів в інформаційних та інформаційно-телекомунікаційних системах; *використовувати* сучасні методи та моделі інформаційної безпеки та/або кібербезпеки, теорії та методи захисту для забезпечення безпеки веб-ресурсів, 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 веб-додатків** Основні поняття та термінологія. Архітектура "файл-сервер". Архітектура "клієнт-сервер". Архітектура розподілених систем. Архітектура веб-додатків	**ЛР №1** Розмежування повноважень користувачів на основі парольної аутентифікації	Опрацювання теоретичного матеріалу лекції №1. Підготовка до виконання ЛР №1.	3	[8] с. 272-284 [9] с. 34-47 [10] chapter 2 [13] с. 4-9 [15]
2	**Вимоги до захисту веб-ресурсів (частина 1)** Ідентифікація та аутентифікація. Обробка помилок, логування дій користувачів та ведення журналу. Обробка вхідних і вихідних даних	-	Опрацювання теоретичного матеріалу лекції №2. Підготовка до захисту ЛР №1.	3	[4] [10] chapter 4
3	**Вимоги до захисту веб-ресурсів (частина 2)** Конфігурація та операції. Управління сеансами. Контроль доступу	**ЛР №2** Логування дій користувачів у веб-ресурсах	Опрацювання теоретичного матеріалу лекції №3. Підготовка до виконання ЛР №2.	5	[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 лекції №4. Підготовка до захисту ЛР №2.	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** Захист веб-ресурсів від ботів та спаму за допомогою механізму CAPTCHA	Опрацювання теоретичного матеріалу лекції №5. Підготовка до виконання ЛР №3.	5	[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 лекції №6. Підготовка до захисту ЛР №3.	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** Захист веб-ресурсів за допомогою технології Blockchain	Опрацювання теоретичного матеріалу лекції №7. Підготовка до виконання ЛР №4.	5	[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 лекції №8. Підготовка до захисту ЛР №4.	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** Захист веб-ресурсів від SQL-ін'єкцій, XSS-атак та інших форм злому	Опрацювання теоретичного матеріалу лекції №9. Підготовка до виконання ЛР №5.	5	[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 лекції №10. Підготовка до захисту ЛР №5.	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** Захист поштових серверів та шлюзів	Опрацювання теоретичного матеріалу лекції №11. Підготовка до виконання ЛР №6.	5	[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 лекції №12. Підготовка до захисту ЛР №6.	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** Збирання інформації про веб-ресурси	Опрацювання теоретичного матеріалу лекції №13. Підготовка до виконання ЛР №7.	5	[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 веб-додатків	-	Опрацювання теоретичного матеріалу лекції №14. Підготовка до захисту ЛР №7.	5	[4]
15	**Проект тестування OWASP** Основні принципи тестування та оцінювання безпеки веб-додатків. Програмні засоби для тестування та оцінювання безпеки веб-додатків. Виведення вимог до оцінювання безпеки веб-додатків	**ЛР №8** Аналіз захищеності веб-ресурсів	Опрацювання теоретичного матеріалу лекції №15. Підготовка до виконання ЛР №8.	5	[5] с. 1-73 [12] с. 669-699, с. 747-771
16	**Забезпечення технологій веб-додатків (SWAT)** SWAT DSL. Опис DSL та структури даних Повторно використовувані HTTP-запити. Тести безпеки, інтегровані в робочі процеси розробки та тестування	-	Опрацювання теоретичного матеріалу лекції №16. Підготовка до захисту ЛР №8.	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 №17. Підготовка до тестування.	6	[10] chapter 8, 9 [12] с. 669-699

*** лекції проводяться по 2 години щотижня;**
**** 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	Семестровий контроль (іспит)
Тема	1-4	1-4	1-4
Ваговий коефіцієнт	0,45	0,15	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 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 MOODLE.

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

Семестровий контроль (іспит). Підсумковий контрольний захід з дисципліни проводиться в формі іспиту. Екзаменаційний білет складається з двох теоретичних питань. 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.

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 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. 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 веб-додатків.
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 веб-додатків (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 веб-додатків.
51. Методика організації та проведення аудиту веб-додатків.

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

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни «Безпека Web-ресурсів» повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі MOODLE - 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.	Обзор уязвимостей, некоторых видов атак и средств защиты [Електронний ресурс] / Ю.А. Семенов. – ГНЦ ИТЭФ, 2015 р.	http://book.itep.ru/6/intrusion.htm
4.	Средства противодействия атакам [Електронний ресурс] / Ю.А. Семенов. – ГНЦ ИТЭФ, 2015 р.	http://book.itep.ru/6/defence.htm
5.	Відкритий проект захисту веб-додатків (OWASP). Стандарт оцінювання відповідності безпеки додатків 3.0 [Електронний ресурс]. – 2015.	https://owasp.org/www-pdf-archive/ASVS_3_0_Ukrainian_Beta.pdf
6.	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
7.	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
8.	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
9.	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
10.	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
11.	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
12.	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
13.	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
14.	Протоколи SLI, PPP, SMTP і POP3. Поняття DNS, DHCP, RAS [Електронний ресурс]	http://lib.mdpu.org.ua/e-book/oi/lection3.htm
15.	Клієнт-серверна система для безпечного обміну приватними повідомленнями із застосуванням криптографії з відкритим ключем/ О.М. Петренко, С.В. Клименко, Г.О. Поляков. - Строительство, материаловедение, машиностроение. – 2017. – вип. 101. – С. 177-182.	http://srd.pgasa.dp.ua:8080/bitstream/123456789/2859/1/Petrenko.pdf
16.	Учебник по ASP.NET [Електронний ресурс]	http://www.realcoding.net/articles/glava-6-soap.html

17.	Продукти ESET для бізнесу [Електронний ресурс]	https://infotel.ua/files/eset/Catalog_ESET_for_business_ukr.pdf

Додаткова

18.	OWASP Foundation. Testing Guide v4.0 [Електронний ресурс]. – 2019.	https://owasp.org/www-pdf-archive/OWASP_Application_Security_Verification_Standard_4.0-en.pdf
19.	Botnets 1st Edition The Killer Web Applications/ Craig Schiller James Binkley. – Syngress, 2007. – 480 p.	https://doc.lagout.org/security/Botnets%20-%20The%20killer%20web%20applications.pdf
20.	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
21.	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
22.	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
23.	Безпека веб-додатків: 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
24.	Удосконалення захисту Web-ресурсів 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
25.	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/
26.	Універсальній метод захисту веб-додатків/ 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
27.	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
28.	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
29.	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
30.	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. ІІІ 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.
2. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.

Розробник _____ д.т.н., професор _____ К.В. Молодецька
Підпис Вчений ступінь, звання Ініціали, прізвище викладача(ів)

Погоджено

Гарант освітньої програми _____ к.т.н., доцент _____ В.М. Чешун
Підпис Вчений ступінь, звання Ініціали, прізвище

Зав. кафедри кібербезпеки та
комп'ютерних систем і мереж _____ к.т.н., доцент _____ Ю.П. Кльоц
Підпис Вчений ступінь, звання Ініціали, прізвище