ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету ІТ
_____ Олег САВЕНКО
Підпис Ім'я, ПРІЗВИЩЕ
«31» 08 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Безпека вебресурсів

Галузь знань	12 – Інформаційні технології
Спеціальність	125 – Кібербезпека та захист інформації
Рівень вищої освіти	Перший бакалаврський
Освітньо-професійна програма	Кібербезпека та захист інформації
Обсяг дисципліни	5 кредитів ЄКТС
Шифр дисципліни	ОПП.07
Мова навчання	Українська
Статус дисципліни	Обов'язкова, дисципліна професійної підготовки
Факультет	Інформаційних технологій
Кафедра	Кібербезпеки

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття					Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття				Залік	Іспит
Очна (денна)	2	4	5	150	54	18	36			96			+	

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

Робоча програма складена _____ канд. техн. наук, доц. Ігор МУЛЯР
Підпис(и) автора(ів) Ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

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

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

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

Хмельницький 2023

БЕЗПЕКА ВЕБРЕСУРСІВ

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

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.

Зміст навчальної дисципліни: Організація та способи передачі даних мережі Інтернет. Стек протоколів TCP/IP. Система доменних імен DNS. Протоколи Інтернет прикладного рівня. Основи клієнт-серверних технологій веб-сервери. Протоколи HTTP та HTTPS. Cookie. Організація поштових серверів. Принципи організації електронної пошти. Поштові сервери і клієнти. Протоколи передачі електронної пошти (IMAP, POP3, SMTP, UUCP). Архітектура вебсистем і вебдодатків. Архітектура "файл-сервер". Архітектура "клієнт-сервер". Архітектура розподілених систем. Класифікація веб-атак та вразливостей. Вразливості аутентифікації (Brute Force, недостатня аутентифікація, небезпечне відновлення паролів). Вразливості авторизації (передбачуване значення ідентифікатора сесії, недостатня авторизація, відсутність таймауту сесії, фіксація сесії). Атаки на клієнтів (підміна вмісту, Clickjacking, міжсайтовий скріптинг (XSS), розщеплення HTTP-запиту, міжсайтова підробка запиту (CSRF)). Атака через виконання коду (переповнення буфера, атака на функції форматування рядків, LDAP Injection, виконання команд ОС, SQL Injection, SSI Injection, XPath Injection). 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). Розробка захищених вебдодатків. Вимоги до захисту вебдодатків. Проект тестування OWASP. Основні принципи тестування та оцінювання безпеки вебдодатків. Програмні засоби для тестування та оцінювання безпеки вебдодатків. Аудит та журнали безпеки.

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

Кореквізити: технології виявлення вразливостей та вторгнень.

Запланована навчальна діяльність: лекцій 18, лабораторних занять 36 год., самостійної роботи 96 год., разом 150 год.

Форми (методи) навчання: пояснювально-ілюстративні, практичні, продуктивні, контекстні, застосування інформаційно-комп'ютерних технологій (MS Visual studio, ПЗ для тестування захищеності вебдодатків).

Форми оцінювання результатів навчання: усне опитування, захист лабораторних робіт, тестування, підсумковий контрольний захід (семестровий контроль).

Вид семестрового контролю: іспит.

Навчальні ресурси:

1 Технології та протоколи інфокомунікаційних мереж. Частина 1/ О.Л. Недашківський. – Київ, 2017. – 67 с.

2. Бурячок В. Л. 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.

3. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. Навчальний посібник/ В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К., 2018. – 320 с.

4. КІБЕРБЕЗПЕКА: WEB-технології [Електронний ресурс]: Навчально- довідковий посібник / С.П. Євсеєв, А.М. Ткачов, В.О. Алексієв, Ю.М. Рябуха – Харків : ХНЕУ ім. С. Кузнеця, – Львів: Видавництво «Новий Світ – 2000», 2021. – 390 с.

5. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khnu.km.ua.

Викладач: кандидат технічних наук, доцент Муляр І.В.

ВСТУП

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.

СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	**Кількість годин відведених на:**		
	лекції	**лабораторні роботи**	**самостійну роботу**
Тема 1. Розробка захищених вебресурсів	4	4	20
Тема 2. Методи захисту протоколів обміну інформацією	6	4	20
Тема 3. Веб-атаки та вразливості вебресурсів	4	16	30
Тема 4. Аналіз захищеності вебресурсів	4	11	26
Разом:	**18**	**36**	**96**

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотація	Години
	Тема 1. Розробка захищених вебресурсів	
1	**Вимоги до захисту вебресурсів (частина 1)** 1. Ідентифікація та аутентифікація 2. Обробка помилок, логування дій користувачів та ведення журналу 3. Обробка вхідних і вихідних даних Літ.: [4]; [11] chapter 4	2
2	**Вимоги до захисту вебресурсів (частина 2)** 1. Конфігурація та операції 2. Управління сеансами 3. Контроль доступу Літ.: [4]; [11] chapter 4	2
	Тема 2. Методи захисту протоколів обміну інформацією	
3	**Захист інформації у гіпертекстових протоколах** 1. HTTP-запити та відповіді, методи та повідомлення 2. HTTPS (протокол передачі гіпертексту через захищені сокети) 3. Cookie Літ.: [1] с. 9-26; [13] с. 39-71	2
4	**Захист інформації на рівні сокетів та у протоколах доступу до об'єктів** 1. Протокол SSL (Secure Sockets Layer) 2. Симетричне та асиметричне шифрування в протоколах обміну інформацією 3. Використання та захист протоколу простого доступу до об'єктів (SOAP) 7. Відмінності між SOAP і REST Літ.: [1] с. 9-26; [2] с. 47-69; [17]	2
5	**Захист інформації у поштових протоколах** 1. Принципи організації електронної пошти 2. Поштові сервери і клієнти, як об'єкт захисту 3. Захист конфіденційності у протоколах електронної пошти (IMAP, POP3, SMTP, UUCP) Літ.: [1] с. 9-26; [15] с. 219-227	2
	Тема 3. Веб-атаки та вразливості вебресурсів	
6	**Класифікація веб-атак та вразливостей (частина 1)** 1. Аутентифікація (Brute Force, недостатня аутентифікація, небезпечне відновлення паролів) 2. Авторизація (передбачуване значення ідентифікатора сесії, недостатня авторизація, відсутність таймауту сесії, фіксація сесії) Літ.: [13] с. 159-255	2
7	**Класифікація веб-атак та вразливостей (частина 2)** 1. Виконання коду (переповнення буфера, атака на функції форматування рядків, LDAP Injection, виконання команд ОС, SQL Injection, SSI Injection, XPath Injection) 2. Атаки на клієнтів (підміна вмісту, Clickjacking, міжсайтовий скріптинг (XSS), розщеплення HTTP-запиту, міжсайтова підробка запиту (CSRF)) 3. Розголошення інформації (індексування директорій, ідентифікація додатків, витік інформації, зворотний шлях в директоріях) 4.Логічні атаки (зловживання функціональними можливостями, відмова	2

	в обслуговуванні (DoS-атака), недостатня протидія автоматизації, недостатня перевірка процесу) Літ.: [13] с. 257-354; с. 405-571	
Тема 4. Аналіз захищеності вебресурсів		
8	**Проект тестування OWASP** 1. Основні принципи тестування та оцінювання безпеки вебдодатків 2. Програмні засоби для тестування та оцінювання безпеки вебдодатків 3. Виведення вимог до оцінювання безпеки вебдодатків Літ.: [5] с. 1-73	2
9	**Забезпечення технологій вебдодатків (SWAT)** 1. SWAT DSL. Опис DSL та структури даних 2. Повторно використовувані HTTP-запити 3. Тести безпеки, інтегровані в робочі процеси розробки та тестування [13] с. 117-157	2
	Разом за семестр:	**18**

Зміст лабораторних робіт

№ п/п	Теми лабораторних робіт	Кількість годин
1	Збирання інформації про веб-ресурси. Виявлення вразливостей вебдодатків засобами сканування. Аналіз HTTP- параметрів для запитів GET/POST Літ.: [8] с. 272-284; [14] с. 4-9	4
2	Виявлення вразливостей вебсервера за допомогою інструментів мережевого сканування Літ.: [10] с. 6-47; [14] с. 9-14	4
3	Виявлення та аналіз ін'єкцій (SQL, Function, code, command) Літ.: [7] с. 26-40; [9] с. 45-54; [14] с. 14-21	4
4	Прогнозування/фіксація сесії (Session Prediction/Fixation) Літ.: [13] с. 601-613; [14] с. 21-26	4
5	Аналіз та виявлення XSS-атак Літ.: [8] с. 284-296; [14] с. 28-32	4
6	Аналіз та виявлення міжсайтової підробки запитів CSRF Літ.: [13] с. 824-842	4
7	Атаки на авторизацію, парольні атаки Літ.: [13] с. 747-771	4
8	Методи та засоби виявлення XML-атаки XXE ін’єкції Літ.: [13] с. 669-699	4
9	Підсумкове заняття. Тестування.	4
	Разом за семестр:	**36**

Зміст самостійної (у т.ч. індивідуальної) роботи

Об'єм самостійної роботи з дисципліни "Безпека вебресурсів" становить 96 годин. Він включає опрацювання лекційного матеріалу та літературних джерел, підготовку до тестування, підготовку до виконання та захисту лабораторних робіт. Керівництво самостійною роботою здійснює викладач згідно з розкладом консультацій в позаурочний час.

Номер тижня	**Вид самостійної роботи**	**Кількість годин**
1	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР1	6
2	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР1.	5
3	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР2	6
4	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР2	5
5	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР3	6
6	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР3	5
7	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР4	6
8	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР №4	5
9	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР5	6
10	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР5	5
11	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР6	6
12	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР6	5
13	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР7	6
14	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР7	5
15	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР8	6
16	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР8	5
17	Опрацювання теоретичного матеріалу. Підготовка до тестування	8
	Разом:	**96**

ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції проводяться пояснювально-ілюстративними методами з супроводом презентаційних матеріалів, лабораторні заняття проводяться практичними, продуктивними, контекстними методами, з використанням інформаційно-комп'ютерних технологій (MS Visual studio, ПЗ для тестування захищеності вебдодатків) і мають за мету – набуття студентами практичних навичок у забезпеченні безпеки вебресурсів.

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

При вивченні дисципліни можуть бути зараховані результати навчання, здобуті у неформальній освіті. Визнання результатів навчання, здобутих у неформальній освіті, реалізується згідно з чинним законодавством і регулюється Положенням про порядок перезарахування результатів навчання та визначення академічної різниці у ХНУ https://www.khnu.km.ua/root/files/01/10/03/006.pdf.

МЕТОДИ КОНТРОЛЮ

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

При цьому використовуються такі методи поточного контролю:

- усне опитування;
- захист лабораторної роботи;
- тестування.

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

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ

Оцінювання академічних досягнень студента здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Кожний вид роботи з дисципліни оцінюється за інституційною чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих видів її робіт.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів за ваговими коефіцієнтами

	Аудиторна робота	**Контрольні заходи**	**Підсумковий контрольний захід**
Вид заняття	Лабораторні роботи	Тестування	-
Тема	1-4	1-4	-
Ваговий коефіцієнт	0,8	0,2	-

<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.

<u>Оцінювання тестових завдань.</u> 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 інституційної 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 вебсистем 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.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Технології та протоколи інфокомунікаційних мереж. Частина 1[Електронний ресурс]/ О.Л. Недашківський. – Київ, 2017. – режим доступу: 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.
3. Відкритий проект захисту вебдодатків (OWASP). Web Security Testing Guide V4.2 [Електронний ресурс]. – 2024. –режим доступу: https://owasp.org/www-project-web-security-testing-guide/
4. Основи інформаційної та кібернетичної безпеки. Навчальний посібник/ В. Л. Бурячок, Р. В. Киричок, П. М. Складанний – К., 2018. – 320 с.
5. КІБЕРБЕЗПЕКА: WEB-технології [Електронний ресурс]: Навчально- довідковий посібник / С.П. Євсеєв, А.М. Ткачов, В.О. Алексієв, Ю.М. Рябуха – Харків : ХНЕУ ім. С. Кузнеця, – Львів: Видавництво «Новий Світ – 2000», 2021. – 390 с.
6. Інформаційна безпека: навчальний посібник/ Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик ; 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.
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, 2022. – режим доступу: https://ela.kpi.ua/bitstream/123456789/22234/1/Zahist_web_servisiv_Laboratornyi_praktikum.pdf
8. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ2000», 2020 . – 678 с.
9. Конспект лекцій з дисципліни «Захист інформації у комп’ютерних системах» / Р.О. Жаровський. – Тернопіль, 2019. – 268 с.
10. The Web Applicaion Hackers’s Handbook: Finding and Exploiting Security Flaws/D. Stuttard, M. Pinto. - John Wiley & Sons, Inc, 2011. – 877 p.
11. Методичні вказівки до виконання практичних робіт з курсу «Безпека програм та даних» [Електронний ресурс]/ Р.П. Шевчук, І.А. Дармороcт. – Тернопіль, 2018. – режим доступу: http://dspace.tneu.edu.ua/bitstream/316497/30542/1/BPD_lab_2018.pdf
12. Комп’ютерні мережі: навчальний посібник/ Ю. І. Лосев, К. М. Руккас, С. І. Шматков. – Х.: ХНУ імені В. Н. Каразіна, 2013. – 248 с.

Додаткова

13. OWASP Foundation. Testing Guide v4.0. – 2019. – режим доступу: https://cdn.oiipdf.com/pdf/c315c2a2-0794-47a4-b0bf-ab9b645f749f.pdf
14. Botnets 1st Edition The Killer Web Applications/ Craig Schiller James Binkley. – Syngress, 2007. – 480 p.
15. Bulletproof SSL and TLS: Understanding and deploying SSL/TLS and PKI to secure servers and web applications/ I. Ristic. – Feisty Duck Limited, 2014. – 517 p.

16. Architecture Modeling and Analysis of Security in Android Systems/ B. Schmerl et al. –Software Architecture. – 2016. – P. 274-290.

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.

18. Безпека вебдодатків: актуальні проблеми та їх аналіз/ О. Бондаренко, І. Ушкаленко. – Формування ринкової економіки в Україні. – 2017. – Вип. 38. – С. 28-36.

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.

20. Основи сучасних веб-технологій. Ч.1: навч. посіб./ Л. В. Зубик, І. М. Карпович, О. М. Степанченко. – Рівне : НУВГП, 2016. – 290 с.

21. Універсальній метод захисту вебдодатків/ І.В. Василенко. – Системи обробки інформації. – 2016. – вип.1 (138). – С. 122-124.

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.

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.

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.

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. ІІІ міжнар. наук.-практ. конф., 22–25 лют. 2017 р. – К. : Європ. ун-т, 2017. – С. 121–122.

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.