МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

Факультет фінансів та цифрових технологій
Кафедра фінансових ринків та технологій

Затверджено
Науково-методичною радою ДПУ
протокол від 21.09 2023 № 1
Голова НМР _____ Іван ШЕМЕЛИНЕЦЬ

Робоча програма
навчальної дисципліни
«Кібербезпека у фінансових технологіях»
(назва)
для підготовки здобувачів вищої освіти другого (магістерського) рівня
(денної та заочної форми навчання)
галузь знань 07 «Управління та адміністрування»
спеціальність 072 «Фінанси, банківська справа, страхування та фондовий ринок»
освітньо-професійна програма «Фінансові технології»
Статус дисципліни: обов'язкова

Ірпінь – 2023

Робоча програма навчальної дисципліни «Кібербезпека у фінансових технологіях» складена на основі освітньо-професійної програми «Фінансові технології» другого (магістерського) рівня спеціальності «Фінанси, банківська справа, страхування та фондовий ринок» затвердженої Вченою радою Університету 21.06 2023 року, протокол № 13

Укладач: _____ Ю. Лах, к.ф.-м.н., доцент кафедри фінансових ринків та технологій
О. Пернарівський к.е.н., доцент , доцент кафедри фінансових ринків та технологій

Гаранти освітньої програми «Фінансові технології» В. Корнєєв _____

Розглянуто і схвалено кафедрою фінансових ринків та технологій, протокол від «30» 08 2023 р. № 1

Завідувач кафедри_____ О. Береславська, д.е.н., професор

Розглянуто і схвалено Вченою радою факультету та цифрових технологій, протокол від «12» 09 2023 р. № 1

Голова вченої ради факультету
фінансів та цифрових технологій _____ В. Корнєєв

Завідувач навчально-методичним відділом _____ І. Качур, к.б.н, доцент

Реєстраційний №_____

Зміст робочої програми навчальної дисципліни

		Стор.
1.	Передмова	4
2.	Опис навчальної дисципліни	5
3.	Програма навчальної дисципліни	11
4.	Критерії оцінювання рівня навчальних досягнень здобувачів вищої освіти	16
5.	Засоби діагностики результатів навчання	20
6.	Форми та питання поточного та підсумкового контролю	21
7.	Рекомендована література	25
8.	Лист моніторингу	26

1. Передмова

Робоча програма навчальної дисципліни “Кібербезпека у фінансових технологіях” складена на основі освітньо-професійної програми «Фінансові технології» для підготовки здобувачів вищої освіти другого (магістерського) рівня денної та заочної форм навчання галузі знань 07 Управління та адміністрування спеціальності 072 “Фінанси, банківська справа, страхування та фондовий ринок”.

Мета навчальної дисципліни полягає в освоєнні студентами теоретичних основ із веб-безпеки та набуття практичних навичок кібербезпеки у фінансових технологіях у галузі архітектури додатків веб-протоколів.

Завданням є вивчення сучасного стану кібербезпеки у фінансових технологіях для поширених технологій Web- програмування.

Предметом є інструментарій інформаційної безпеки як технологій веб-програмування, так і мережевих комп’ютерних інформаційних технологій при здійсненні фінансової діяльності підприємств та установ.

Навчальна дисципліна «Кібербезпека у фінансових технологіях» тісно пов’язана з іншими дисциплінами, такими як «Фінансові технології», «Ризик-менеджмент у фінансовій сфері», «Сучасні платіжні системи».

При вивченні зазначеної дисципліни студенти повинні отримати чітке уявлення про статус, форми організації і функції архітектури додатків веб-протоколів, а також аспекти уразливостей безпеки баз даних в мовах PHP, JavaScripts, SQL, механізмів веб-аутентифікації та способів її обходу, моделювання атак і оцінки ризиків.

Завдання курсу — засвоєння майбутніми фахівцями загальних понять для застосування різних засобів безпеки та оцінці уразливостей при створенні Web–контенту у фінансових технологіях, а також набутті навиків забезпечення безпеки Web- контенту різними засобами.

Методи навчання:

1) Група методів за джерелом інформації і сприйняття навчальної інформації – словені (лекція, лабораторні, бесіда, розповідь); наочні – (ілюстрація, демонстрація, презентація), практичні (програмування, розрахунки, графічно-схематичне зображення інформації).

2) Група методів за логікою передачі і сприйняття навчального матеріалу: – індуктивні, дедуктивні, аналітичні, синтетичні;

3) Група методів за ступенем самостійного мислення при засвоєнні знань – репродуктивні та продуктивні (дослідницькі, пошукові, частково-пошукові);

4) Група методів за ступенем управління навчальним процесом: навчання під керівництвом викладача, самостійна робота здобувача вищої освіти з навчальною та науковою літературою, текстами лекцій, підготовка до семінарських і практичних занять, виконання письмових завдань.

Форми навчання: денна і заочна.

Форма організації занять: навчальний процес здійснюється у таких формах, як класичні лекції, лекції-консультації, лабораторні роботи, тестові завдання, доповіді, презентації, усні та письмові відповіді на теоретичні запитання, запитання понятійного апарату, розв’язання практичних завдань, тренінги, складання конспекту із завдань, що винесені на самостійну роботу, обговорення наукових публікацій тощо.

Організація поточного контролю та підсумкового контролю знань: поточний контроль проводиться у вигляді усного та письмового опитування на лабораторних заняттях, підготовки індивідуальних завдань, написання підсумкових контрольних робіт за кожним модулем.
Підсумковий контроль передбачено проводити у формі екзамену.

2. Опис навчальної дисципліни «Кібербезпека у фінансових технологіях»

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Рівень вищої освіти, галузь знань, спеціальність</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td rowspan="2">Кількість кредитів 4</td><td>Рівень вищої освіти: другий (магістерський) рівень</td><td colspan="2" rowspan="2">Обов’язкова</td></tr>
<tr><td rowspan="6">Галузь знань:
07 «Управління та адміністрування»</td></tr>
<tr><td>Модулів 2</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів 2</td><td colspan="2">1-й</td></tr>
<tr><td rowspan="3">Загальна кількість годин 120</td><td colspan="2">Семестр</td></tr>
<tr><td colspan="2">2-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="8"></td><td rowspan="8">Спеціальність:
072 «Фінанси, банківська справа, страхування та фондовий ринок»

Освітньо-професійна програма «Фінансові технології»</td><td colspan="2">22/8 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td colspan="2">18/8год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td colspan="2">75/102 год.</td></tr>
<tr><td colspan="2">Індивід.-консультаційна робота: 5/2 год.</td></tr>
<tr><td colspan="2" rowspan="2">Вид контролю: екзамен</td></tr>
<tr></tr>
</table>

2.1.КОМПЕТЕНТНОСТІ ТА РЕЗУЛЬТАТИ НАВЧАННЯ

Після вивчення курсу “Кібербезпека у фінансових технологіях” здобувачі вищої освіти повинні володіти такими компетентностями та результатами навчання:

Компетентності	Результати навчання
ІК Здатність розв’язувати складні задачі і проблеми у професійній діяльності або у процесі навчання у сфері фінансів, банківської справи, страхування та фондового ринку, зокрема фінансових технологій, що передбачає проведення досліджень та\або здійснення інновацій та характеризується невизначеністю умов і вимог.	ПР 03. Здійснювати адаптацію та модифікацію існуючих наукових підходів і методів до конкретних ситуацій професійної діяльності.
ЗК2. Здатність спілкуватися іноземною мовою.	ПР 05. Вільно спілкуватись іноземною мовою усно і письмово з професійних та наукових питань, презентувати і обговорювати результати досліджень.
ЗК8. Здатність працювати в міжнародному контексті.	ПР 08. Вміти застосовувати інноваційні підходи у сфері фінансів, банківської справи, страхування та фондового ринку та управляти ними.
СК5. Здатність оцінювати межі власної фахової компетентності та підвищувати професійну кваліфікацію.	ПР 11. Застосовувати поглибленні знання в сфері фінансового, банківського та страхового менеджменту для прийняття рішень.
СК6. Здатність застосовувати міждисциплінарні підходи при розв’язані складних задач і проблем у сфері фінансів, банківської справи, страхування та фондового ринку.	ПР 12. Обґрунтувати вибір варіантів управлінських рішень у сфері фінансів, банківської справи, страхування та фондового ринку та оцінювати їх ефективність з урахуваннях цілей, наявних обмежень, законодавчих та етичних аспектів.
СК12. Здатність застосовувати управлінські навички у сфері ризик-менеджменту у фінансовій і страховій сфері, кібербезпеки у фінансових технологіях .	ПР16. Застосовувати інноваційні фінансові інструменти та технології у сфері фінансів, банківської справи, страхування та фондового ринку.

2.2. ПРЕРЕКВІЗИТИ ТА ПОСТРЕКВІЗИТИ ВИВЧЕННЯ ДИСЦИПЛІНИ.

Пререквізити: передумовами для вивчення дисципліни: “Фінансові технології”, “Ризик-менеджмент у фінансовій сфері”, “Сучасні платіжні системи” та інші дисципліни.

Постреквізити: на основі дисципліни “Фінансова аналітика”, “Фінансове моделювання та прогнозування” тощо.

2.3. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

"Кібербезпека у фінансових технологіях"
Спеціальність 072 "Фінанси, банківська справа, страхування та фондовий ринок"
денна форма навчання

Змістові модулі	Кількість годин				
	Лекції	Лабор.	Індивід-консул. робота	СРС	Всього
Модуль 1. АРХІТЕКТУРА ВЕБ-СИСТЕМ І ВЕБ-ДОДАТКІВ ТА ТИПИ АТАК НА НИХ. (2 залікових кредити (60 год.))					
Т. 1. Впровадження методів захисту у протоколах обміну інформацією	4	2		9	15
Т 2. Архітектура Веб-систем	2	2		10	14
Т 3. Аутентифікація	2	2	2	9	15
Т 4. Авторизація	4	2		10	16
Форма контролю – модульна контрольна робота					
Всього по модулю 1 Підсумкова атестація за 1-м модулем	**12**	**8**	**2**	**38**	**60**
Модуль 2. ПРОТИДІЯ КІБЕРЗАГРОЗАМ ПРИ ЗДІЙСНЕННІ ФІНАНСОВИХ ОПЕРАЦІЙ (2 залікових кредитів (60 год.))					
Т.5. Client-side Attacks (атаки на стороні клієнта)	4	4		10	18
Т. 6. Атаки перехоплення, поділу HTTP відповіді та міжсайтової підробки запиту	2	2		10	14
Т. 7. Виконання команд	2	2		10	14
Т. 8. Розробка захищених сайтів. OWASP проекти	2	2		10	14
Форма контролю – модульна контрольна робота					
Всього за модулем Підсумкова атестація за 2-м модулем	**10**	**10**		**40**	**60**
Разом годин з курсу	**22**	**18**	**2**	**78**	**120**
ФОРМА ПІДСУМКОВОГО КОНТРОЛЮ – екзамен					

2.4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ "Кібербезпека у фінансових технологіях"
Спеціальність 072 "Фінанси, банківська справа, страхування та фондовий ринок"
Заочна форма навчання

Змістові модулі	Кількість годин				
	Лекції	Лабор.	Індивід-консул. робота	СРС	Всього
Модуль 1. АРХІТЕКТУРА ВЕБ-СИСТЕМ І ВЕБ-ДОДАТКІВ ТА ТИПИ АТАК НА НИХ. (2 залікових кредити (60 год.))					
Т. 1. Впровадження методів захисту у протоколах обміну інформацією	1			13	14
Т 2. Архітектура Веб-систем		1		14	15
Т 3. Аутентифікація	1		2	13	16

Т 4. Авторизація		1		14	15
Форма контролю – модульна контрольна робота					
Всього по модулю 1 Підсумкова атестація за 1-м модулем	**2**	**2**	**2**	**54**	**60**
Модуль 2. ПРОТИДІЯ КІБЕРЗАГРОЗАМ ПРИ ЗДІЙСНЕННІ ФІНАНСОВИХ ОПЕРАЦІЙ **(2 залікових кредитів (60 год.))**					
Т.5. Client-side Attacks (атаки на стороні клієнта)	1			14	15
Т. 6. Атаки перехоплення, поділу HTTP відповіді та міжсайтової підробки запиту		1		14	15
Т. 7. Виконання команд				14	14
Т. 8. Розробка захищених сайтів. OWASP проекти	1	1		14	16
Форма контролю – модульна контрольна робота					
Всього за модулем Підсумкова атестація за 2-м модулем	**2**	**2**		**56**	**60**
Разом годин з курсу	**4**	**4**	**2**	**110**	**120**
ФОРМА ПІДСУМКОВОГО КОНТРОЛЮ – екзамен					

РЕЙТИНГ – ПЛАН

Денна форма навчання

Години	Тема	Форма заняття та заняття (лекція, семінар, лабораторна робота, практична робота, самостійна робота здобувача, контрольний захід, підсумкове тестування, індивідуальна робота)	Результати навчання	Вага оцінки кількість балів
4	Т1. Впровадження методів захисту у протоколах обміну інформацією	Лекція		0
2	Т1. Впровадження методів захисту у протоколах обміну інформацією	Лабораторна робота	ПР 03 ПР 05	2
2	Т2. Архітектура Веб-систем	Лекція		0
2	Т2. Архітектура Веб-систем	Лабораторна робота	ПР 08 ПР 11	2
2	Т3. Аутентифікація	Лекція		0
2	Т3. Аутентифікація	Лабораторна робота	ПР 12	2
	Т3. Аутентифікація	Індивідуальна робота		7
4	Т4. Авторизація	Лекція		0
2	Т4. Авторизація	Лабораторна робота	ПР 12 ПР16	2
		Проміжний модульний контроль		10
	Усього за модулем 1			**25**
	Модуль 2			
4	Т5. Client-side Attacks (атаки на стороні клієнта)	Лекція		0
4	Т5. Client-side Attacks (атаки на стороні клієнта)	Лабораторна робота	ПР16	4
2	Т6. Атаки перехоплення, поділу HTTP відповіді та міжсайтової підробки запиту	Лекція		
2	Т6. Атаки перехоплення, поділу HTTP відповіді та міжсайтової підробки запиту	Лабораторна робота	ПР 03	2
2	Т7. Виконання команд	Лекція		
2	Т7. Виконання команд	Лабораторна робота	ПР 03	2
2	Т8. Розробка захищених сайтів. OWASP проекти	Лекція		
2	Т8. Розробка захищених сайтів. OWASP проекти	Лабораторна робота	ПР 08	2
	Т5-8	Проміжний модульний контроль		10
	Усього за модулем 2			**20**
	Комп'ютерне тестування на платформі дистаниійного навчання ДПУ MOODLE			5
		Екзамен		50
	Усього за курсом			100

РЕЙТИНГ – ПЛАН

Заочна форма навчання

Години	Тема	Форма заняття та заняття (лекція, семінар, лабораторна робота, практична робота, самостійна робота здобувача, контрольний захід, підсумкове тестування, індивідуальна робота)	Результати навчання	Вага оцінки кількість балів
1	Т1. Впровадження методів захисту у протоколах обміну інформацією	Лекція		0
	Т1. Впровадження методів захисту у протоколах обміну інформацією	Лабораторна робота	ПР 03 ПР 05	2
0	Т2. Архітектура Веб-систем	Самостійна робота		0
0	Т2. Архітектура Веб-систем	Самостійна робота	ПР 08 ПР 11	
1	Т3. Аутентифікація	Лекція		0
0	Т3. Аутентифікація	Самостійна робота	ПР 12	2
	Т3. Аутентифікація	Індивідуальна робота		17
0	Т4. Авторизація	Самостійна робота		0
1	Т4. Авторизація	Лабораторна робота	ПР 12 ПР16	2
	Усього за модулем 1			**21**
	Модуль 2			
1	Т5. Client-side Attacks (атаки на стороні клієнта)	Лекція		0
0	Т5. Client-side Attacks (атаки на стороні клієнта)	Самостійна робота	ПР16	2
0	Т6. Атаки перехоплення, поділу HTTP відповіді та міжсайтової підробки запиту	Самостійна робота		
1	Т6. Атаки перехоплення, поділу HTTP відповіді та міжсайтової підробки запиту	Лабораторна робота	ПР 03	2
0	Т7. Виконання команд	Самостійна робота я		
0	Т7. Виконання команд	Самостійна робота	ПР 03	
1	Т8. Розробка захищених сайтів. OWASP проекти	Лекція		
1	Т8. Розробка захищених сайтів. OWASP проекти	Лабораторна робота	ПР 08	2
	Т5-8	Проміжний модульний контроль		20
	Усього за модулем 2			**24**
	Комп'ютерне тестування на платформі дистаниійного навчання ДПУ MOODLE			5
		Екзамен		50
	Усього за курсом			100

3.

4. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗМ 1. АРХІТЕКТУРА ВЕБ-СИСТЕМ І ВЕБ-ДОДАТКІВ ТА ТИПИ АТАК НА НИХ

Тема 1. Впровадження методів захисту у протоколах обміну інформацією

План лекційного заняття

1. Впровадження методів захисту у протоколах обміну інформацією
2. Протокол HTTP.
3. Протоколи HTTP/S, SOAP.
4. Захист персональних даних додатків клієнт-сервер завдяки поштовому протоколу, простому протоколу передачі пошти та протоколу доступу до міжмережевих повідомлень.

План лабораторного заняття

1. Основні помилки користувачів.
2. Чи можна мінімізувати ризики потрапити на гачок шахраїв, під час користування Інтернетом.
3. Як зловмисники отримують доступ до наших персональних даних і ноутбуків та мобільних пристроїв.
4. Які наслідки можуть мати кібератаки на користувачів.
5. Безпечне використання мобільних телефонів.

План самостійної роботи здобувачів вищої освіти

Питання для самостійного опрацювання:

1. Які є загрози для мобільних пристроїв.
2. Якої шкоди може завдати порушення правил безпеки під час використання смартфона.
3. Яких рекомендацій слід дотримуватися, щоб захистити мобільний пристрій від зловмисників.

Рекомендована література:

Основна [1, 4, 5].
Допоміжна [6, 7, 8].
Інформаційні ресурси Інтернет [12, 13].
Міжнародні видання [17, 18].

Тема 2. Архітектура Веб-систем

План лекційного заняття

1. Архітектура Веб-систем та Веб-додатків.
2. Об'єкти захисту / атак .
3. Класифікація веб-атак (уразливостей).

План лабораторного заняття.

1. Безпечне використання комп’ютерів.
2. Чим зумовлені поява й поширення комп’ютерної злочинності.
3. Якої шкоди може завдати порушення правил безпеки під час використання комп’ютера.
4. Яких рекомендацій слід дотримуватися, щоб захиститися від атак хакерів

План самостійної роботи здобувачів вищої освіти.

Питання для самостійного опрацювання:

1. Безпека в соціальних мережах
2. Безпечне використання Інтернету.

Рекомендована література:

Основна [1, 5].
Допоміжна [6, 7, 8].
Інформаційні ресурси Інтернет [12, 14].
Міжнародні видання [17, 18].

Тема 3. Аутентифікація

План лекційного заняття

1. “Груба сила” (Brute force).
2. Ненадійна аутентифікація.
3. Ненадійне відновлення пароля (Слабка перевірка відновлення пароля).

План лабораторного заняття.

1. Атаки методом «Грубої сили».
2. Відмінність автентифікацією та авторизацією.
3. Використання програми Hydra для підбору паролів зловмисниками.
4. Необхідність подвійної автентифікації.

План самостійної роботи здобувачів вищої освіти.

Питання для самостійного опрацювання:

1. Троян Lady Boyle.
2. Атака MITM (man in the middle) людина посередині.

Перелік питань для самоконтролю

1. Чим спричинена потреба дбати про захист власних комп’ютерів і мобільних пристроїв від небезпечних програм.
2. Які типи програм створюють хакери, та якої шкоди ці програми можуть завдати.
3. Яких рекомендацій слід дотримуватися, щоб вчасно розпізнати небезпечне ПЗ й уберегтися від атак хакерів.

План індивідуально-консультативної роботи

1. Типи шкідливого програмного забезпечення.
2. Атаки на Smart TV.
3. DDoS атаки.
4. Банківський троян Dyre Trojan.

Рекомендована література:
Основна [1, 2, 3, 4].
Допоміжна [6, 7, 8].
Інформаційні ресурси Інтернет [12, 13].
Міжнародні видання [17, 18].

Тема 4. Авторизація

План лекційного заняття

1. Прогнозування облікових даних/сесії .
2. Ненадійна авторизація..
3. Ненадійне завершення сесії.
4. Фіксація сесії.
5. Перехоплення сесії.

План лабораторного заняття

1. Випадок прогнозованих креденцій сесії.
2. Дії зловмисника по фіксації сесії.
3. Завершення сесії.
4. Запобігання перехопленню сесії.

План самостійної роботи здобувачів вищої освіти

Питання для самостійного опрацювання:

1. Безпечне використання електронної пошти.
2. Які атаки можуть здійснюватися через електронну пошту.
3. Яких заходів слід вживати, щоб убезпечити свій обліковий запис і повідомлення.

Перелік питань для самоконтролю

1. Слабкі паролі.
2..Перехоплення сесії.

Рекомендована література:

Основна [1, 2, 5].
Допоміжна [6, 7, 8].
Інформаційні ресурси Інтернет [12, 14].
Міжнародні видання [17, 18].

ЗМ 2. ПРОТИДІЯ КІБЕРЗАГРОЗАМ ПРИ ЗДІЙСНЕННІ ФІНАНСОВИХ ОПЕРАЦІЙ

Тема 5. Client-side Attacks (атаки на стороні клієнта)

План лекційного заняття

1. Спуфінг контенту.
2. Міжсайтовий скриптінг, XSS.
3. Міжфреймовий скриптінг (XFS) або Iframe ін'єкції.

План лабораторного заняття

1.Атаки типу «відбиті».
2. Атаки типу «збережені».
3. Атаки типу DOM-based.
4. Троянські програми.

План самостійної роботи здобувачів вищої освіти.

Теми рефератів та есе:

1. Атака типу TweetDeck
2. Інформація та комунікації у менеджменті.

Перелік питань для самоконтролю

1.Три види атак міжсайтового скриптингу.
2.Атаки типу Iframe ін'єкції.

Рекомендована література:

Основна [1, 2, 3].
Допоміжна [6, 7, 8].
Інформаційні ресурси Інтернет [12, 15].
Міжнародні видання [17, 18].

Тема 6. Атаки перехоплення, поділу HTTP відповіді та міжсайтової підробки запиту.

План лекційного заняття

1. Клікджекінг.
2. Поділ HTTP відповіді.
3. Міжсайтова підробка запиту, CSRF.

План лабораторного заняття

1.Виконання досліджень по оцінці захисту інформації в комп'ютерних системах від несанкціонованого доступу та організація служби захисту інформації в автоматизованій системі на об’єкті.
2. Організація контрольно-пропускного пункту на об’єкті .
3. Зчитувачі, проксіміті-картки.

4. Системи допуску та обліку відвідувачів.
5. Виконавчі пристрої.
6. Замки, турнікети.

План самостійної роботи здобувачів вищої освіти

1. Організація КПП об’єкту, в якому циркулює інформація з обмеженим доступом (ІзОД).
2. Положення про структурний підрозділ захисту інформації на об’єкті.
3. Штатний розпис підрозділу захисту інформації на підприємстві та посадові інструкції його співробітників.

Перелік питань для самоконтролю

1.Атака типу поділу HTTP відповіді.
2. Використання гостьової книги для проведення атак.
3. Перехоплення сесії при проведенні платежів.

Рекомендована література:
Основна [1, 5].
Допоміжна [6, 7, 8].
Інформаційні ресурси Інтернет [12, 15, 16].
Міжнародні видання [17, 18].

Тема 7. Виконання команд

План лекційного заняття

1. Переповнення буфера .
2. Формат атакуючого рядка.
3. LDAP ін'єкції.
4. Командні ОС.
5. SQL-ін'єкції .
6. SSI ін'єкції .
7. XPath ін'єкції.

План лабораторного заняття

1. Атаки ін’єкції.
2. Суть атак переповнення буфера.
3. Небезпека атак типу DROP для даних в системі.
4. Види можливих атак.

План самостійної роботи здобувачів вищої освіти

1. Використання стандартів ISO та COBIT для оцінки інформаційної безпеки.
2. Використання контролів безпеки в ISO.
3. Коли слід віддати перевагу COBIT для оцінки інформаційної безпеки.

Перелік питань для самоконтролю

1. Основні правила захисту інформації.
2. Використанням ліцензійного ПЗ, антивірусів та файрволів.
3. Резервне копіювання.

Рекомендована література:
Основна [1, 3, 4,].
Допоміжна [6, 7, 8].
Інформаційні ресурси Інтернет [12, 13, 14].
Міжнародні видання [17, 18].

Тема 8. Розробка захищених сайтів. OWASP проекти

План лекційного заняття

1. Методики розробки захищених сайтів.
2. Проекти OWASP.
3. Огляд інструкції тестування OWASP. Список топ 10.
4. Аудит безпеки веб-сайту.

План лабораторного заняття

1. Криптографічний захист.
2. Повноваження центрального банку у сфері грошово-кредитної політики.
3. DES шифрування.
4. Кейлоґери.
5. AES шифрування.
6. Атака типу Shellshock.
7. Криптографічний алгоритм RSA.
8.Атака типу Shamoon.

План самостійної роботи здобувачів вищої освіти

Питання для самостійного опрацювання:

1.Атака типу Heartbeat.
2. Атака типу Exploit W32/Wormlinks.
3. Атака типу Grub.

Перелік питань для самоконтролю

1.OWASP топ тен.
2. IT аудит кібербезпеки при роботі в інтернеті.

Рекомендована література:

Основна [1, 3, 5,].
Допоміжна [6, 7, 8, 10].
Інформаційні ресурси Інтернет [12, 13, 14].
Міжнародні видання [17, 18].

4. КРИТЕРІЇ ОЦІНЮВАННЯ РІВНЯ НАВЧАЛЬНИХ ДОСЯГНЕНЬ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Максимальна кількість балів отримана здобувачем вищої освіти за лабораторну роботу становить 4 бали.

Виконання самостійної роботи, як правило, оцінюється під час проведення лабораторного заняття у вигляді опитування в тому числі за питаннями, які виносяться на самостійну роботу.

Загальний розподіл балів, які здобувач вищої освіти може отримати в межах 100-бальної системи оцінювання, повинен включати обов'язкове комп'ютерне тестування на платформі дистанційного навчання ДПС MOODLE (максимально до 5 балів).

Таблиця 4.1

Шкала оцінювання роботи здобувачів вищої освіти лабораторних заняттях

Кількість балів	Критерії оцінювання
2(2)	В повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу.
1(1)	Не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час відповідей, недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності
0	Не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань та практичних завдань.

Критерії оцінювання контрольних робіт.

Формою проміжного поточного контролю є контрольні роботи, які проводяться у письмовій формі та кожна з яких оцінюється від 0 до 10 (20) балів.

Таблиця 4.2

Розподіл балів за різні види завдань в межах контрольної роботи

Вид завдання	Максимальна кількість балів за виконання
Теоретичні питання	4 (8)
Тестовий блок	6 (12)
Всього	10 (20)

Таблиця 4.3

Критерії оцінювання відповіді на теоретичне питання

Критерії оцінювання	Кількість балів
Оцінюється робота здобувача вищої освіти, який у повному обсязі дав відповіді на всі питання. При цьому використовував актуальну наукову термінологію, належним чином обґрунтовував свої думки та зробив узагальнені підсумки.	4 (8)

Оцінюється робота здобувача вищої освіти, який в основному розкрив зміст теоретичних питань. Проте, при висвітленні деяких питань не вистачало достатньої аргументації, допускалися при цьому окремі неістотні неточності та незначні помилки.	2 (4)
Оцінюється робота здобувача вищої освіти, який дав фрагментарні відповіді на теоретичні питання (без аргументації й обґрунтування, підсумків), у відповідях присутні неточності та помилки або відповідь дана лише на окремі питання.	1 (2)
Оцінюється робота здобувача вищої освіти, який дав неправильну відповідь на всі теоретичні питання, допустив істотні помилки, оперував неактуальною застарілою інформацією або відповіді на питання відсутні взагалі.	0

Таблиця 4.4

Критерії оцінювання тестового блоку

Критерії оцінювання	Кількість балів
Оцінюється робота здобувача вищої освіти, який повністю розкрив всі питання та використовував для цього наукову літературу та власну думку.	6 (12)
Оцінюється робота здобувача вищої освіти, який розкрив сутність лише окремих питань та використовував для цього наукову літературу та власну думку.	4 (6)
Оцінюється робота здобувача вищої освіти, який взагалі не розкрив сутність визначень.	0

Критерії оцінювання індивідуальної роботи.

У робочій програмі зазначається назва індивідуального завдання, його обсяг, структура, коротка характеристика змісту і вимог до виконання та оцінювання

Індивідуальна робота здійснюється у формі реферату, презентації, проєкту або інших формах описаних робочою програмою або методичною розробкою і оцінюється від 0 до 7 (17) балів.

Таблиця 4.5

Шкала оцінювання індивідуальної роботи здобувачів вищої освіти

Кількість балів	Критерії оцінювання
7 (17)	Послідовність, логічність написання реферату, а також підготовка презентації та, відповідно, його захист, а також виокремлення з різних джерел основних положень, які структурно об’єднанні, проаналізовані та узагальнені висновками.
3 (10)	Послідовність, логічність написання реферату, але без презентації.
0	Не написано реферат та не зроблено презентацію по ньому.

Підсумкове оцінювання знань здобувачів вищої освіти здійснюється за результатами поточного контролю (від 0 до 50 балів) та екзамену (від 0 до 50 балів). Критерієм успішного проходження здобувачем освіти підсумкового оцінювання є отримання не менше 25 балів за поточний контроль та 25 балів за підсумковий контроль у формі екзамену.

Переведення даних 100-бальної шкали оцінювання в національну шкалу та шкалу за системою ЄКТС здійснюється в такому порядку (табл.4.6):

Таблиця 4.6

Таблиця відповідності результатів контролю знань за різними шкалами й критеріями оцінювання

Сума балів за 100-бальною шкалою	Оцінка в ЄКТС	Значення оцінки ЄКТС	Критерії оцінювання	Рівень компетентності	Оцінка за національною Шкалою	
					Екзамен	Залік
90-100	A	Відмінно	Здобувач вищої освіти виявляє особливі творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить та опрацьовує необхідну інформацію, вміє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні обдарування і нахили.	високий (творчий)	відмінно	зараховано
80-89	B	дуже добре	Здобувач вищої освіти вільно володіє вивченим обсягом матеріалу, застосовує його на практиці, вільно розв'язує вправи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна.	достатній (конструктивно-варіативний)	добре	
70-79	C	Добре	Здобувач вищої освіти вміє зіставляти, узагальнювати, систематизувати інформацію під керівництвом викладача; в цілому самостійно застосовувати її на практиці; контролювати власну діяльність;			

			виправляти помилки, серед яких є суттєві, добирати аргументи для підтвердження думок.			
60-69	D	Задовільно	Здобувач вищої освіти відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень; з допомогою викладача може аналізувати навчальний матеріал, виправляти помилки, серед яких є значна кількість суттєвих.	середній (репродуктивний)	Задовільно	
50-59	E	Достатньо	Здобувач вищої освіти володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні.			
35-49	FX	Незадовільно з можливістю повторного складання семестрового контролю	Здобувач вищої освіти володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.	Низький (рецептивно-продуктивний)	незадовільно	Не зараховано
0-34	F	Незадовільно з обов'язковим повторним вивченням залікового кредиту	Здобувач вищої освіти володіє матеріалом на рівні елементарного розпізнання і відтворення окремих фактів, елементів, об'єктів.			

Результати складання екзамену оцінюються за чотирибальною шкалою («відмінно», «добре», «задовільно», «незадовільно») і вносяться у відомість обліку успішності здобувача вищої освіти, залікову книжку, індивідуальний навчальний план здобувача вищої освіти (крім «незадовільно» і «не зараховано»).

Критерієм успішного проходження здобувачем освіти підсумкового оцінювання може бути досягнення ним мінімальних порогових рівнів оцінок за кожним запланованим результатом навчання навчальної дисципліни.

5. ЗАСОБИ ДІАГНОСТИКИ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засобами оцінювання та методами демонстрування результатів навчання з навчальної дисципліни «Кібербезпека у фінансових технологіях» є:
- екзамен;
- стандартизовані тести;
- аналітичні звіти, реферати, есе;
- презентації результатів виконаних завдань та досліджень;
- презентації та виступи на наукових заходах;
- комп’ютерне тестування на платформі MOODLE ДПУ;
- інші види індивідуальних та групових завдань.

6. ФОРМИ ТА ПИТАННЯ ДО ПОТОЧНОГО ТА ПІДСУМКОВОГО КОНТРОЛЮ

Перелік питань до поточного контролю № 1

1. Веб-атаки та уразливості.
2. Функціонування / уразливості на стороні клієнта.
3. HTTP запит.
4. Протокол HTTP.
5. Протоколи HTTP/S, SOAP.
6. Поштові протоколи POP, SMTP та IMAP.
7. Клієнт-сервер протоколи.
8. HTTP відповідь.
9. Категоріювання уразливостей на стороні клієнта.
10. Функціонування на стороні сервера.
11. HTTP повідомлення для простої трансакції.
12. Статус коди.
13. Загрози та уразливості.
14. Категорії загроз: Spoofing.
15. Автентифікація та авторизація, їх відмінності.
16. Основи веб-безпеки.
17. Ненадійне завершення сесії.
18. Двошарова архітектура Веб-аплікацій.
19. Загрози, уразливості, атаки.
20. Атаки та контрміри.
21. Категорії загроз: . Information disclosure..
22. Основні Веб-безпекові організації.
23. Категорії загроз: Repudiation.
24. Реалізація загроз.
25. Категорії загроз: Denial of service.
26 Категорії загроз: Elevation of privilege.
27. Уразливості та слабкі місця.
28. Правила безпечного користування мережею.
29. HTTP заголовки (методи).
30. Ненадійна авторизація.
31. Уразливості клієнта.
32. Атака методом “Грубої сили” (Brute force).
33. Використання методів GET і POST.
34. DoS атаки.
35. Схема здійснення загрози.
36. Використання HTTP headers.
37. Використання заголовку trace.
38. WASC
39. Небезпеки блокування акаунта.
40. Компоненти архітектури Веб-аплікацій.
41. Отримання методом Грубої сили ідентифікатора сесії.
42. Отримання методом Грубої сили інформації банківської картки.
43. Отримання методом Грубої сили інформації директорій та файлів.
44. Відмінності автентифікації та авторизації.

Перелік питань до поточного контролю № 2

1.Протокол передачі гіпертексту.
2. Запити та відповіді HTTP, методи та повідомлення.
3. Куки.
4. HTTPS (протокол передачі гіпертексту через захищені сокети).
5. Протокол рівня захищених сокетів (SSL).
6. Перехоплення довірених осіб та HTTPS.
7. Простий протокол передачі пошти (SMTP).
8. Протокол поштового офісу (POP3).
9. Протокол доступу до Інтернет-повідомлень (IMAP).
10. Веб-системи та архітектура веб-додатків.
11. Об'єкти захисту / атаки.
12. Класифікація веб-атак (уразливостей).
13. Фіксація сесії.
14. Захист даних.
15. Автентифікація.
16. Оперування входом і виходом.
17. Конфігурація та операції.
18. Управління сесією.
19. Ненадійна авторизація..
20. Ненадійне завершення сесії.
21. Фіксація сесії.
22. Багатошарова архітектура Веб-аплікацій.
23. Безпека поведінки у соцмережах.
24. Види уразливостей веб аплікацій.
25. CWE.
26. Атака методом Brute force.
27. Три найтиповіші зразки архітектури Веб-аплікацій.
28. Слабкі місця.
29. SANS Top 25.
30. Додаток Web Goat.
31. Способи приховування даних.
32. Класифікація веб атак.
33. Фактори автентифікації.
34. Недостатня автентифікація.
35. Слабка валідація відновлення пароля.
36. Отримання методом Грубої сили інформації для логування.
37. Перехоплення сесії.

Перелік питань до підсумкового контролю контролю

1. Веб-атаки та уразливості.
2. Функціонування / уразливості на стороні клієнта.
3. HTTP запит.
4. Протокол HTTP.
5. Протоколи HTTP/S, SOAP.
6. Поштові протоколи POP, SMTP та IMAP.
7. Клієнт-сервер протоколи.

8. HTTP відповідь.
9. Категоріювання уразливостей на стороні клієнта.
10. Функціонування на стороні сервера.
11. HTTP повідомлення для простої трансакції.
12. Статус коди.
13. Загрози та уразливості.
14. Категорії загроз: Spoofing.
15. Автентифікація та авторизація, їх відмінності.
16. Основи веб-безпеки.
17. Ненадійне завершення сесії.
18. Двошарова архітектура Веб-аплікацій.
19. Загрози, уразливості, атаки.
20. Атаки та контрміри.
21. Категорії загроз: . Information disclosure..
22. Основні Веб-безпекові організації.
23. Категорії загроз: Repudiation.
24. Реалізація загроз.
25. Категорії загроз: Denial of service.
26. Категорії загроз: Elevation of privilege.
27. Уразливості та слабкі місця.
28. Правила безпечного користування мережею.
29. HTTP заголовки (методи).
30. Ненадійна авторизація.
31. Уразливості клієнта.
32. Атака методом “Грубої сили” (Brute force).
33. Використання методів GET і POST.
34. DoS атаки.
35. Схема здійснення загрози.
36. Використання HTTP headers.
37. Використання заголовку trace.
38. WASC
39. Небезпеки блокування акаунта.
40. Компоненти архітектури Веб-аплікацій.
41. Отримання методом Грубої сили ідентифікатора сесії.
42. Отримання методом Грубої сили інформації банківської картки.
43. Отримання методом Грубої сили інформації директорій та файлів.
44. Відмінності автентифікації та авторизації.
45. Протокол передачі гіпертексту.
46. Запити та відповіді HTTP, методи та повідомлення.
47. Куки.
48. HTTPS (протокол передачі гіпертексту через захищені сокети).
49. Протокол рівня захищених сокетів (SSL).
50. Перехоплення довірених осіб та HTTPS.
51. Простий протокол передачі пошти (SMTP).
52. Протокол поштового офісу (POP3).
53. Протокол доступу до Інтернет-повідомлень (IMAP).
54. Веб-системи та архітектура веб-додатків.
55. Об'єкти захисту / атаки.
56. Класифікація веб-атак (уразливостей).
57. Фіксація сесії.

58. Захист даних.
59. Автентифікація.
60. Оперування входом і виходом.
61. Конфігурація та операції.
62. Управління сесією.
63. Ненадійна авторизація..
64. Ненадійне завершення сесії.
65. Фіксація сесії.
66. Багатошарова архітектура Веб-аплікацій.
67. Безпека поведінки у соцмережах.
68. Види уразливостей веб аплікацій.
69. CWE.
70. Атака методом Brute force.
71. Три найтиповіші зразки архітектури Веб-аплікацій.
72. Слабкі місця.
73. SANS Top 25.
74. Додаток Web Goat.
75. Способи приховування даних.
76. Класифікація веб атак.
77. Фактори автентифікації.
78. Недостатня автентифікація.
79. Слабка валідація відновлення пароля.
80. Отримання методом Грубої сили інформації для логування.
81. Перехоплення сесії.

7. РЕКОМЕНДОВАНА ЛІТЕРАТУРА:

Основна

1. Гончар С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури : монографія / С. Ф. Гончар ; НАН України, Ін-т проблем моделювання в енергетиці ім. Г. Є. Пухова. - Київ : Альфа Реклама, 2019. - 175 с.

2. Гриценко К. Г. Шляхи підвищення ефективності забезпечення кібербезпеки банку / К. Г. Гриценко // Інфраструктура ринку. – 2020. – Вип. 45. – С. 274-279.

3. Даник Ю. Г. Основи кібербезпеки та кібероборони : підручник / Ю. Г. Даник, П. П. Воробієнко. - Одеса : ОНАЗ , 2019. - 320 с.

4. Дубина М. В. Роль кіберстрахування в системі ризик-менеджменту банківських установ / М. В. Дубина, І. О. Середюк, Н. В. Білоус // Проблеми і перспективи економіки та управління. – 2020. – № 1. – С. 183-196. – Режим доступу: http://ppeu.stu.cn.ua/article/view/211426.

5. Основи кіберпростору, кібербезпеки та кіберзахисту : навч. посіб. - Київ : Ліра-К, 2020. - 554 с.

Допоміжна

6. Євсеєв С. П. Кібербезпека: криптографія з Python : навч. посіб. / С. П. Євсеєв, О. В. Шматко, О. Г. Король ; відп. за вип. С. П. Євсеєв. – Львів : Новий Світ-2000, 2021. – 120 с

7. Кіберстрахування : можливості чи виклики? // Страхова справа. – 2019. – № 2. – С. 33.

8. Мазаракі А. А. FinTech : монографія / А. А. Мазаракі, С. В. Волосович. – Київ : КНТЕУ, 2019. – 308 с.

9. TechAmerica. 2017. Twenty-seventh Annual Survey of Federal Chief Information Officers (CIO), April 2017.

10. von Solms, B., and R. von Solms. 2018. "Cybersecurity and Information Security - What Goes Where?" Information and Computer Security 26: 2-9. doi:10.1108/ICS-01-2015-0001

11. Weber, S. (2017). Coercion in cybersecurity: What public health models reveal. Journal of Cybersecurity, 3(3), 173-183. https://doi.org/10.1093/cybsec/tyx005D. Gourley, B. Totty HTTP: The Definitive Guide. O'Reilly Media, Inc., 2002.

Інформаційні ресурси Інтернет

12. Web Application Security Consortium, "Web Security Threat Classification v2.0".URL: http://projects.webappsec.org/f/WASC-TC-v2_0.pdf

13. Web Application Security Consortium, "Web Security Threat Classification v1.0" URL: http://projects.webappsec.org/Threat-Classification

14. Synopsys Software Security. URL: https://www.whitehatsec.com/resource/glossary.html

15. Web Application Security Consortium. URL: http://projects.webappsec.org/w/page/13246995/Web-Hacking-Incident-Database

16. Web Application Security Services. URL: http://www.cgisecurity.com/lib/SessionIDs.pdf

Міжнародні видання

17. OWASP. Category:Access Control. URL: https://www.owasp.org/index.php/Guide_to_Authorization

18. Kaisler S., Armour F., Money W., Espinosa J. A. Big data issues and challenges // Encyclopedia of information science and technology, third edition. – IGI Global, 2023. – P. 363–370.

ЛИСТ МОНІТОРИНГУ

РОЗГЛЯНУТО ТА СХВАЛЕНО

на засіданні кафедри фінансових ринків та технологій

Протокол від _____2023 р. № ____.

Укладач: О.Береславська, д.е.н., професор, завідувач кафедри фінансових ринків та технологій

Навчальний рік	Дата засідання кафедри	Номер протоколу	Підпис завідувача кафедри	Підпис гаранта ОП

РЕЦЕНЗІЯ

на робочу програму навчальної дисципліни
«Кібербезпека у фінансових технологіях»
для підготовки здобувачів вищої освіти другого (магістерського) рівня
галузь знань 07 «Управління та адміністрування»
спеціальність «Фінанси, банківська справа, страхування та фондовий ринок»
освітньо-професійна програма “Фінансові технології”

Робоча програма навчальної дисципліни «Кібербезпека у фінансових технологіях» містить теми, які розташовані в логічній послідовності та розкривають зміст та методи забезпечення кібербезпеки у фінансових технологіях.

У робочій програмі навчальної дисципліни наведено опис структури дисципліни за модульною системою; теми лекційних та лабораторних занять; питання для підготовки до практичних занять та для самостійного опрацювання; індивідуальні завдання; перелік питань для поточного та семестрового контролю знань; форми та методи оцінювання; розподіл балів; рекомендовану літературу.

Тематика, зміст та погодинна структура лабораторних занять здатна забезпечити набуття студентами належних практичних навичок щодо кібербезпеки у фінансових технологіях.

В цілому робоча програма з курсу «Кібербезпека у фінансових технологіях» відповідає встановленим вимогам і може бути використана при організації навчального процесу.

Рецензент

РЕЦЕНЗІЯ

на робочу програму навчальної дисципліни
«Кібербезпека у фінансових технологіях»
для підготовки здобувачів вищої освіти другого (магістерського) рівня
галузь знань 07 «Управління та адміністрування»
спеціальність «Фінанси, банківська справа, страхування та фондовий ринок»
освітньо-професійна програма “Фінансові технології”

Структура курсу передбачає вивчення двох змістовних модулів, в яких розглядаються теоретичні та практичні засади кібербезпеки у фінансових технологіях.

Робоча програма дисципліни «Кібербезпека у фінансових технологіях» логічно структурована, містить розгорнутий перелік питань, що вивчаються під час лекційних та лабораторних занять, питань та завдань для самостійного опрацювання та індивідуальної роботи, контролю знань студентів. До кожного структурного елемента робочої програми визначено перелік рекомендованої літератури, присвяченої основним аспектам кібербезпеки у фінансових технологіях.

На підставі викладеного вважаю, що рецензована робоча програма навчальної дисципліни «Кібербезпека у фінансових технологіях» відповідає встановленим вимогам щодо забезпечення навчального процесу у вищих навчальних закладах України, ґрунтується на широкій джерельній базі вітчизняних та зарубіжних дослідників, тому рекомендується до використання в навчальному процесі.

Рецензент: