МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”

Кафедра _____*кібербезпеки*_____
(назва кафедри, яка забезпечує викладання дисципліни)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КОМПЛЕКСНИЙ ТРЕНІНГ “БЕЗПЕКА ВЕБ-ЗАСТОСУНКІВ”

(назва навчальної дисципліни)

рівень вищої освіти_____*другий (магістерський)*_____
перший (бакалаврський) / другий (магістерський)

галузь знань_____*12 Інформаційні технології*_____
(шифр і назва)

спеціальність _____*125 Кібербезпека*_____
(шифр і назва)

освітня програма _____*Кібербезпека*_____
(назви освітньої програми)

вид дисципліни _____*спеціальна (фахова) підготовка, вибіркова*_____
(загальна підготовка /спеціальна (фахова) підготовка; обов’язкова/вибіркова)

форма навчання _____*денна*_____
(денна / заочна/дистанційна)

Харків – 2022 рік

ЛИСТ ЗАТВЕРДЖЕННЯ

Робоча програма з навчальної дисципліни КОМПЛЕКСНИЙ ТРЕНІНГ “БЕЗПЕКА ВЕБ-ЗАСТОСУНКІВ”
(назва дисципліни)

Розробники:

доц, к.т.н., доц.		*Ольга КОРОЛЬ*
(посада, науковий ступінь та вчене звання)	(підпис)	(ім’я та прізвище)

Робоча програма розглянута та затверджена на засіданні кафедри

кібербезпеки
(назва кафедри, яка забезпечує викладання дисципліни)

Протокол від “_22_”__серпня___2022 року № 1

Завідувач кафедри _кібербезпеки__		*Сергій ЄВСЕЄВ*
(назва кафедри)	(підпис)	(ініціали та прізвище)

ЛИСТ ПОГОДЖЕННЯ

Шифр та назва освітньої програми_____125 “Кібербезпека”_____

_____

Кафедра _____кібербезпеки_____
(назва кафедри на якій викладається дисципліна)

Гарант ОП _____ 22.08.2022р _____ *Олександр МІЛОВ*
(Підпис, дата) (ім’я та прізвище)

Завідувач кафедрою _____ 22.08.2022р _____ *Сергій ЄВСЕЄВ*
(Підпис, дата) (ім’я та прізвище)

ЛИСТ ПЕРЕЗАТВЕРДЖЕННЯ РОБОЧОЇ НАВЧАЛЬНОЇ ПРОГРАМИ

№ зп	Дата засідання кафедри-розробника РПНД	Номер протоколу	Підпис завідувача кафедри (яка викладає)	Підпис завідувача кафедри (на якій викладається)	Підпис гаранта освітньої програми
1					
2					
3					
4					
5					

МЕТА, КОМПЕТЕНТНОСТІ, РЕЗУЛЬТАТИ НАВЧАННЯ ТА СТРУКТУРНО-ЛОГІЧНА СХЕМА ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета навчальної дисципліни “Комплексний тренінг“Безпека веб-застосунків” – формування практичних навичок щодо виявлення та протидії сучасним загрозам в кіберпросторі на основі відпрацювання практичних завдань.

Компетентності та результати навчання

Компетентності	Результати навчання
КЗ-1. Здатність застосовувати знання у практичних ситуаціях.	РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури. РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної

Компетентності	Результати навчання
	безпеки та/або кібербезпеки організації. РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому. РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації	РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до

Компетентності	Результати навчання
щодо попередження та аналізу кіберінцидентів в цілому.	встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

Структурно-логічна схема вивчення навчальної дисципліни

Вивчення цієї дисципліни безпосередньо спирається на:	На результати вивчення цієї дисципліни безпосередньо спираються:
Веб-безпека	Практика
Бездротова та мобільна безпека	Атестація
Тестування на проникнення та етичний хакінг	

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

(розподіл навчального часу за семестрами та видами навчальних занять)

Семестр	Всього (годин) / кредитів ECTS	З них		За видами аудиторних занять (годин)			Індивідуальні завдання студентів (КП, КР, РГ, Р, РЕ)	Поточний контроль	Семестровий контроль	
		Аудиторні заняття (годин)	Самостійна робота (годин)	Лекції	Лабораторні заняття	Практичні заняття, семінари		Контрольні роботи (кількість робіт)	Залік	Екзамен
1	2	3	4	5	6	7	8	9	10	11
2	**150/5**	**64**	**86**	**32**	**32**	**–**	**–**	**2**	**+**	**–**

Співвідношення кількості годин аудиторних занять до загального обсягу складає 21 (%).

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
1	Л СР	2 2	**Тема 1. Впровадження коду.** Виявлення ін'єкцій, таких як SQL, NoSQL, ОС та ін'єкція LDAP, які виникають, коли ненадійні дані надсилаються інтерпретатору як частина команди чи запиту.	**1, 3-6**
	ЛЗ СР	2 4	**Лабораторна робота №1** Впровадження коду.	
2	Л СР	2 2	**Тема 2. Некоректна автентифікація і управління сесією.** Виявлення функцій іплікації, які пов'язані з автентифікацією та керуванням сеансом, що дозволяє зловмисникам компрометувати паролі, ключі або скельні маркери або використовувати інші недоліки впровадження, щоб тимчасово або назавжди припустити особистість інших користувачів.	**1, 3-6**
	ЛЗ СР	2 3	**Лабораторна робота №2** Некоректна автентифікація і управління сесією.	
3	Л СР	2 2	**Тема 3. Міжсайтовий скриптинг (XSS).** Виявлення веб-додатків та API, які не захищені належним чином. Зловмисники можуть вкрасти або змінити такі слабко захищені дані, щоб вчинити шахрайство з кредитною карткою, крадіжку особи або інші злочини.	**1-4**
	ЛЗ СР	2 3	**Лабораторна робота №3.** Міжсайтовий скриптинг (XSS).	
4	Л СР	2 2	**Тема 4. Небезпечні прямі посилання на об'єкти.** Аналіз старих або погано налаштованих процесорів XML оцінюють посилання зовнішніх об'єктів у документах XML. Зовнішні об'єкти можуть використовуватися для розкриття внутрішніх файлів за допомогою обробника URI файлів, обміну внутрішніми файлами, сканування внутрішніх портів, віддаленого виконання коду та відмови в атаці служби.	**1-4**
	ЛЗ СР	2 3	**Лабораторна робота №4.** Небезпечні прямі посилання на об'єкти.	
5	Л СР	2 2	**Тема 5. Небезпечна конфігурація.** Аналіз обмеження щодо дозволених користувачів, які дозволено робити, часто не виконуються належним чином. Зловмисники можуть використовувати ці недоліки для доступу до несанкціонованих функціональних можливостей та / або даних, таких	**1-4**

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
			як доступ до облікових записів інших користувачів, перегляд конфіденційних файлів, зміна даних інших користувачів, зміна прав доступу тощо.	
	ЛЗ СР	2 4	**Лабораторна робота №5.** Небезпечна конфігурація.	
6	Л СР	2 2	**<u>Тема 5.</u> Небезпечна конфігурація.** Аналіз обмеження щодо дозволених користувачів, які дозволено робити, часто не виконуються належним чином. Зловмисники можуть використовувати ці недоліки для доступу до несанкціонованих функціональних можливостей та / або даних, таких як доступ до облікових записів інших користувачів, перегляд конфіденційних файлів, зміна даних інших користувачів, зміна прав доступу тощо.	**1-4**
	ЛЗ СР	2 3	**Лабораторна робота №5.** Небезпечна конфігурація.	
7	Л СР	2 2	**<u>Тема 6.</u> Витік чутливих даних – оцінка конфігурації безпеки.** Зазвичай це результат небезпечних конфігурацій за замовчуванням, неповних або спеціальних конфігурацій, відкритого хмарного сховища, неправильно налаштованих заголовків HTTP та багатослівних повідомлень про помилки, що містять конфіденційну інформацію. Не тільки всі операційні системи, рамки, бібліотеки та додатки повинні бути надійно налаштовані, але вони повинні бути виправлені / модернізовані своєчасно.	**1-4**
	ЛЗ СР	2 3	**Лабораторна робота №6.** Витік чутливих даних – оцінка конфігурації безпеки.	
8	Л СР	2 2	**<u>Тема 6.</u> Витік чутливих даних – оцінка конфігурації безпеки.** Зазвичай це результат небезпечних конфігурацій за замовчуванням, неповних або спеціальних конфігурацій, відкритого хмарного сховища, неправильно налаштованих заголовків HTTP та багатослівних повідомлень про помилки, що містять конфіденційну інформацію. Не тільки всі операційні системи, рамки, бібліотеки та додатки повинні бути надійно налаштовані, але вони повинні бути виправлені / модернізовані своєчасно.	**1-4**
	ЛЗ СР	2 3	**Лабораторна робота №6.** Витік чутливих даних – оцінка конфігурації безпеки.	
9	Л СР	2 2	**<u>Тема 7.</u> Відсутність контролю доступу до функціонального рівня.** Визначення недоліків XSS, які виникають щоразу, коли програма включає недовірені дані на новій веб-сторінці без належної валідації або не відкриття, або оновлює наявну веб-	**1-4**

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
			сторінку за допомогою наданих користувачем даних за допомогою API браузера, який може створювати HTML або JavaScript. XSS дозволяє зловмисникам виконувати скрипти в браузері жертви, які можуть захоплювати сеанси користувачів, знищувати веб-сайти або перенаправляти користувача на шкідливі сайти	
	ЛЗ СР	2 4	**Лабораторна робота №7.** Відсутність контролю доступу до функціонального рівня.	
10	Л СР	2 2	**<u>Тема 7.</u> Відсутність контролю доступу до функціонального рівня.** Визначення недоліків XSS, які виникають щоразу, коли програма включає недовірені дані на новій веб-сторінці без належної валідації або не відкриття, або оновлює наявну веб-сторінку за допомогою наданих користувачем даних за допомогою API браузера, який може створювати HTML або JavaScript. XSS дозволяє зловмисникам виконувати скрипти в браузері жертви, які можуть захоплювати сеанси користувачів, знищувати веб-сайти або перенаправляти користувача на шкідливі сайти	**1-4**
	ЛЗ СР	2 4	**Лабораторна робота №7.** Відсутність контролю доступу до функціонального рівня.	
11	Л СР	2 2	**<u>Тема 8.</u> Підробка міжсайтових запитів (CSRF).** Оцінка небезпечної десеріалізації, яка часто призводить до віддаленого виконання коду. Навіть якщо дефери дезаріалізації не призводять до віддаленого виконання коду, їх можна використовувати для виконання атак, включаючи атаки відтворення, атаки ін'єкції та напади ескалації привілеїв.	**1-4**
	ЛЗ СР	2 3	**Лабораторна робота №8.** Підробка міжсайтових запитів (CSRF).	
12	Л СР	2 2	**<u>Тема 8.</u> Підробка міжсайтових запитів (CSRF).** Оцінка небезпечної десеріалізації, яка часто призводить до віддаленого виконання коду. Навіть якщо дефери дезаріалізації не призводять до віддаленого виконання коду, їх можна використовувати для виконання атак, включаючи атаки відтворення, атаки ін'єкції та напади ескалації привілеїв.	**1-4**
	ЛЗ СР	2 3	**Лабораторна робота №8.** Підробка міжсайтових запитів (CSRF).	
13	Л СР	2 2	**<u>Тема 9.</u> Використання компонентів з відомими уразливостями.** Аналіз компонент, таких як	**1-4**

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
			бібліотеки, рамки та інші програмні модулі, які працюють із тими ж привілеями, що і додаток. Якщо використовується вразливий компонент, така атака може полегшити серйозні втрати даних або захоплення сервера. Програми та API, що використовують компоненти з відомою вразливістю, можуть підірвати захисні програми та включити різні атаки та впливи.	
	ЛЗ СР	2 4	**Лабораторна робота №9.** Використання компонентів з відомими уразливостями.	
14	Л СР	2 2	**<u>Тема 9.</u> Використання компонентів з відомими уразливостями.** Аналіз компонент, таких як бібліотеки, рамки та інші програмні модулі, які працюють із тими ж привілеями, що і додаток. Якщо використовується вразливий компонент, така атака може полегшити серйозні втрати даних або захоплення сервера. Програми та API, що використовують компоненти з відомою вразливістю, можуть підірвати захисні програми та включити різні атаки та впливи.	**1-4**
	ЛЗ СР	2 4	**Лабораторна робота №9.** Використання компонентів з відомими уразливостями.	
15	Л СР	2 2	**<u>Тема 10.</u> Невалідовані редіректи.** Виявлення недостатнього обліку та моніторингу у поєднанні з відсутньою або неефективною інтеграцією з реакцією на інцидент дозволяє зловмисникам надалі атакувати системи, підтримувати стійкість, перетворювати на більші кількості систем, а також підробляти, витягувати або знищувати дані. Більшість досліджень щодо порушення виявляють час виявлення порушення понад 200 днів, як правило, виявляються зовнішніми сторонами, а не внутрішніми процесами чи моніторингом.	**1-4**
	ЛЗ СР	2 3	**Лабораторна робота №10.** Невалідовані редіректи.	
16	Л СР	2 2	**<u>Тема 10.</u> Невалідовані редіректи.** Виявлення недостатнього обліку та моніторингу у поєднанні з відсутньою або неефективною інтеграцією з реакцією на інцидент дозволяє зловмисникам надалі атакувати системи, підтримувати стійкість, перетворювати на більші кількості систем, а також підробляти, витягувати або знищувати дані. Більшість досліджень щодо порушення виявляють час виявлення порушення понад 200 днів, як правило, виявляються зовнішніми сторонами, а не	**1-4**

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
			внутрішніми процесами чи моніторингом.	
	ЛЗ СР	2 3	**Лабораторна робота №10.** Невалідовані редіректи.	
Разом (годин)		**150**		

САМОСТІЙНА РОБОТА

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час.

№ з/п	Назва видів самостійної роботи	Кількість годин
1	Опрацьовування лекційного матеріалу	32
2	Підготовка до лабораторних занять	54
	Разом	**86**

ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Не передбачено навчальним планом

МЕТОДИ НАВЧАННЯ

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

МЕТОДИ КОНТРОЛЮ

Поточний контроль при вивченні дисципліни реалізується у формі опитувань на лекційних заняттях, захисту лабораторних робіт та проведення контрольних робіт.

Контроль складової робочої програми, яка освоюється під час самостійної роботи студента, проводиться:

- з лекційного матеріалу – шляхом проведення тестування, презентацій докладів за темами лекційних занять;
- з лабораторних завдань – за допомогою перевірки виконаних завдань.

Семестровий контроль проводиться у формі заліку (з оцінкою) відповідно до навчального плану в обсязі навчального матеріалу, визначеного навчальною програмою та у терміни, встановлені навчальним планом.

Семестровий контроль проводиться в письмовій формі за контрольними завданнями, а також шляхом тестування з використанням технічних засобів.

Результати поточного контролю враховуються як допоміжна інформація для виставлення оцінки з даної дисципліни.

Студент вважається атестованим з навчальної дисципліни за умови повного відпрацювання усіх лабораторних робіт, виконання контрольних робіт та тестових опитувань, що передбачено навчальною програмою з дисципліни.

РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ, ТА ШКАЛА ОЦІНЮВАННЯ ЗНАНЬ ТА УМІНЬ (НАЦІОНАЛЬНА ТА ECTS)

Таблиця 1 – Розподіл балів для оцінювання успішності студента для заліку

Контрольні роботи	Лабораторні роботи	КП	РГЗ	Індивідуальні завдання	Тощо	Залік	Сума
20	50	–	–	–	–	30	100

Критерії та система оцінювання знань та вмінь студентів.

Згідно основних положень ЄКТС, під **системою оцінювання** розуміють сукупність методів (письмові, усні і практичні тести, екзамени, проєкти, тощо), що використовуються при оцінюванні досягнень особами, що навчаються, очікуваних результатів навчання.

Успішне оцінювання результатів навчання є передумовою присвоєння кредитів особі, що навчається. Тому твердження про результати вивчення компонентів програм завжди повинні супроводжуватися зрозумілими та відповідними **критеріями оцінювання** для присвоєння кредитів. Це дає можливість стверджувати, чи отримала особа, що навчається, необхідні знання, розуміння, компетенції.

Критерії оцінювання – це описи того, що як очікується, має зробити особа, яка навчається, щоб продемонструвати досягнення результату навчання.

Основними концептуальними положеннями системи оцінювання знань та вмінь студентів є:

1. Підвищення якості підготовки і конкурентоспроможності фахівців за рахунок стимулювання самостійної та систематичної роботи студентів протягом навчального семестру, встановлення постійного зворотного зв'язку викладачів з кожним студентом та своєчасного коригування його навчальної діяльності.

2. Підвищення об'єктивності оцінювання знань студентів відбувається за рахунок контролю протягом семестру із використанням 100 бальної шкали (табл. 2). Оцінки обов'язково переводять у національну шкалу (з виставленням державної семестрової оцінки "відмінно", "добре", "задовільно" чи "незадовільно") та у шкалу ECTS (A, B, C, D, E, FX, F).

Таблиця 2 – Шкала оцінювання знань та умінь: національна та ЄКТС

Рейтингова Оцінка, бали	**Оцінка ECTS та її визначення**	**Національна оцінка**	**Критерії оцінювання**	
			позитивні	**негативні**
1	**2**	**3**	**4**	**5**
90-100	A	Відмінно	- **Глибоке знання** навчального матеріалу, що містяться в **основних і додаткових літературних джерелах;** - **вміння аналізувати** явища, які вивчаються, в їхньому взаємозв'язку і розвитку; - **вміння** проводити **теоретичні розрахунки**; - **відповіді** на запитання **чіткі, лаконічні, логічно послідовні;** - **вміння вирішувати складні практичні задачі.**	Відповіді на запитання можуть містити **незначні неточності**
82-89	B	Добре	- **Глибокий рівень знань** в обсязі **обов'язкового матеріалу**, - вміння давати **аргументовані відповіді** на запитання і проводити **теоретичні розрахунки**; - вміння вирішувати **складні практичні задачі.**	Відповіді на запитання містять **певні неточності;**
			- **Міцні знання** матеріалу, що вивчається,	- невміння використовуват

Рейтингова Оцінка, бали	Оцінка ECTS та її визначення	Національна оцінка	Критерії оцінювання	
			позитивні	негативні
1	**2**	**3**	**4**	**5**
75-81	С	Добре	та його **практичного застосування;** - вміння давати **аргументовані відповіді** на запитання і проводити **теоретичні розрахунки**; - вміння вирішувати **практичні задачі.**	и теоретичні знання для вирішення **складних практичних задач.**
64-74	Д	Задовільно	- Знання **основних фундаментальних положень** матеріалу, що вивчається, та їх **практичного застосування**; - вміння вирішувати прості **практичні задачі**.	Невміння давати **аргументовані відповіді** на запитання; - невміння **аналізувати** викладений матеріал і **виконувати розрахунки;** - невміння вирішувати **складні практичні задачі.**
60-63	Е	Задовільно	- Знання **основних фундаментальних положень** - вміння вирішувати найпростіші **практичні задачі**.	Незнання **окремих (непринципових) питань** з матеріалу модуля; - невміння **послідовно і аргументовано** висловлювати думку; - невміння застосовувати теоретичні положення при розвязанні **практичних задач**

Рейтингова Оцінка, бали	**Оцінка ECTS та її визначення**	**Національна оцінка**	**Критерії оцінювання**	
			позитивні	**негативні**
1	**2**	**3**	**4**	**5**
35-59	FX (потрібне додаткове вивчення)	Незадовільно	**Додаткове вивчення** матеріалу може бути виконане **в терміни, що передбачені навчальним планом**.	Незнання **основних фундаменталь них положень** навчального матеріалу модуля; - **істотні помилки** у відповідях на запитання; - невміння розв’язувати **прості практичні задачі.**
1-34	F (потрібне повторне вивчення)	Незадовільно	-	- Повна **відсутність знань** значної частини навчального матеріалу модуля; - **істотні помилки** у відповідях на запитання; -незнання основних фундаментальн их положень; - невміння орієнтуватися під час розв’язання **простих практичних задач**

НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Стандарт вищої освіти галузі знань 12 “Інформаційні технології” для другого (магістерського) рівня вищої освіти, який затверджено наказом Міністерства освіти і науки України від 18.03.2021 р. № 332 та введено в дію з 2021/2022 навчального року.

2. Робоча програма навчальної дисципліни.

3. Силабус навчальної дисципліни

4. Персональні навчальні системи кафедри кібербезпеки НТУ “ХПІ”: https://iiiii-my.sharepoint.com/personal/serhii_yevseiev_khpi_edu_ua1/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fserhii%5Fyevseiev%5Fkhpi%5Fedu%5Fua1%2FDocuments%2F%D0%9F%D0%9D%D0%A1%20%D0%BA%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B8

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова література

1	Kali Linux Web Penetration Testing Cookbook, Second Edition (Packt Publishing) URL: https://www.packtpub.com/product/kali-linux-web-penetration-testing-cookbook-second-edition/9781788991513
2	Зразок звіту з тестування на проникнення URL: https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf
3	Зразок технічного звіту з проникнення URL: https://tbgsecurity
4	OWASP Top 10: issues in the 10 most critical security risk categories in your web applications URL: https://www.sonarqube.org/features/security/owasp/?gads_campaign=Europe-1-Generic&gads_ad_group=OWASP&gads_keyword=owasp%20top%2010&gclid=CjwKCAiAsNKQBhAPEiwAB-I5zQywzTKai6fcrilMphlAn21CRehrI0q9DEjUZNpHUoDt5V_bVpLm4RoClIkQAvD_BwE

Допоміжна література

5	Встановлення Metasploitable 2 URL: https://metasploit.help.rapid7.com/docs/metasploitable-2
6	Збірка Metasploitable 3 URL: https://github.com/rapid7/metasploitable3.

ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ

1. Додаткова інформація про встановлення Kali Linux URL: https://docs.kali.org/category/installation (https://docs.kali.org/installation/dual-boot-kali-with-windows)

2. Shodan для випробувачів на проникнення URL: https://www.defcon.org/images/defcon-18/dc-18-presentations/Schearer/DEFCON-18-Schearer-SHODAN.pdf

3. Персональні навчальні системи кафедри кібербезпеки НТУ “ХПІ”: https://iiiii-my.sharepoint.com/personal/serhii_yevseiev_khpi_edu_ua1/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fserhii%5Fyevseiev%5Fkhpi%5Fedu%5Fua1%2FDocuments%2F%D0%9F%D0%9D%D0%A1%20%D0%BA%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B8