

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Програмні засоби захисту інформації»

Освітня програма	<i>Кіберзахист інформаційних ресурсів</i>
Рівень вищої освіти	<i>перший (бакалаврський)</i>
Форма навчання	<i>денна</i>
Статус навчальної дисципліни	<i>обов'язкова</i>
Мова викладання	<i>українська</i>

Робочу програму навчальної дисципліни розглянуто та схвалено на засіданні кафедри Безпеки інформаційно-комунікаційних систем від 01.09.2024 року, протокол № 1.

1. Опис навчальної дисципліни

Показник	Значення показника
Курс	2
Семестр	4
Обсяг (кредити ЄКТС/години)	4 / 120
Кількість змістових модулів	3
Розподіл годин за видами навчальної діяльності:	
лекції (Л)	18
практичні заняття (ПЗ)	38
самостійна робота (СР)	64
Форма підсумкового контролю (семестр 4)	Екзамен

Передумови для вивчення навчальної дисципліни:

1. Мережеві технології та протоколи.

2. Мета та завдання навчальної дисципліни

2.1. Мета та основні завдання вивчення навчальної дисципліни

допомогти здобувачам вищої освіти опанувати знання та навички щодо питання забезпечення безпеки інформації в інформаційно-комунікаційних системах за рахунок використання програмних засобів захисту інформації, ознайомити з особливостями їх майбутньої професії.

Завдання:

- здатність застосовувати знання державної та іноземних мов, інформаційно-комунікаційних технологій, комп'ютерної техніки для забезпечення професійної комунікації;

- здатність здійснювати запобіжні заходи для запобігання витоку інформації.

- здатність обґрунтовувати застосування різних програмних засобів для захисту інформації з метою забезпечення безпеки та захисту інформації в мережах та системах всередині організації, між організаціями, між організаціями і користувачами;

- вміння обґрунтовувати застосування методів та засобів захисту програмних засобів, оцінки забезпечення якості програмного забезпечення а також інформаційно-програмних ресурсів і процесів, що беруть участь в життєвому циклі застосунків.

2.2. Результати навчання

Обов'язкова навчальна дисципліна «Програмні засоби захисту інформації» спрямована на досягнення програмних результатів навчання, які в інтегрованому (синтезованому) вигляді визначені у профілі освітньо-професійної / освітньо-наукової програми «Кіберзахист інформаційних ресурсів» (від 11.09.2024 №29/3/1/3-1277ві), а саме:

ПРН 5.	Адаптуватись до нових викликів та дій у певних ситуаціях, застосовувати знання державної та іноземних мов, інформаційно – комунікаційних технологій, комп'ютерної техніки для забезпечення професійної комунікації.
ПРН 17.	Здійснювати заходи щодо запобігання розголошення секретної інформації, випадкам втрат матеріальних носіїв цієї інформації, заволодіння цією інформацією іноземними державами, іноземними юридичними особами, іноземцями, особами без громадянства та громадянами України, яким не надано допуск та доступ до неї
ПРН 22.	Обґрунтовувати застосування методів та засобів захисту програмних засобів, оцінки забезпечення якості програмного забезпечення а також інформаційно-програмних ресурсів і процесів, що беруть участь в життєвому циклі застосунків

3. Програма та структура навчальної дисципліни

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	ЛЗ	СР
<i>I</i>	2	3	4	5	6	7
Семестр 4						
Змістовий модуль 1. Загальносистемні програмні засоби захисту інформації в інформаційно-комунікаційних системах						
Тема 1. Програмне забезпечення систем захисту інформації	26	4		8		14
Лекція 1. Основні поняття програмного забезпечення систем захисту інформації в інформаційно-комунікаційних системах		2				
Самостійна робота 1. Програмні засоби захисту інформації в інформаційно-комунікаційних системах						2
Практичне заняття 1. Структура та організація захисту інформації в ІТС програмними засобами				2		
Самостійна робота 2. Захист інформації в інформаційно-комунікаційних системах						2
Практичне заняття 2. Методи і засоби несанкціонованого отримання інформації в інформаційно-комунікаційних системах				2		
Самостійна робота 3. Протоколи аутентифікації та ідентифікації.						2
Самостійна робота 4. Класифікація порушників інформаційної безпеці						2
Лекція 2. Захист інформації на рівні операційної системи		2				
Самостійна робота 5. Способи захисту інформації на рівні операційної системи						2
Практичне заняття 3. Механізми захисту операційних систем сімейства MS Windows				2		
Самостійна робота 6. Механізми захисту операційних систем сімейства MS Windows						2
Практичне заняття 4. Використання сервісів безпеки				2		

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	ЛЗ	СР
<i>I</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>
операційної системи MS Windows						
Самостійна робота 7. Сервіси безпеки операційної системи MS Windows						2
Тема 2. Альтернативні механізми захисту інформації в операційних системах	28	4		10		14
Лекція 3. Захист інформації засобами операційних систем		2				
Самостійна робота 8. Засоби операційних систем для захисту інформації						2
Практичне заняття 5. Блокування портів та пристроїв виведення інформації на зовнішні носії				2		
Самостійна робота 9. Блокування портів вводу/виведення.						2
Практичне заняття 6. Резервне копіювання даних засобами операційних систем.				2		
Самостійна робота 10. Резервне копіювання даних в операційних системах						2
Лекція 4. Віртуалізовані операційні системи		2				
Самостійна робота 11. Віртуалізація.						2
Практичне заняття 7. Налаштування віртуальної операційної системи				2		
Самостійна робота 12. Види віртуальних операційних систем.						2
Практичне заняття 8. Безпека операційних систем мобільних пристроїв				2		
Самостійна робота 13. Загрози для операційних систем мобільних пристроїв.						2
Самостійна робота 14. Підготовка до проходження модульної контрольної роботи 1						2
Практичне заняття 9. Модульна контрольна робота 1.				2		
Всього годин за змістовий модуль 1.	54	8	-	18	-	28
Змістовий модуль 2. Зовнішні засоби захисту інформації в інформаційно-комунікаційних системах						
Тема 3. Захист від шкідливого програмного забезпечення	12	2	-	4	-	6
Лекція 5. Антивірусний захист інформаційно-комунікаційних систем		2				
Самостійна робота 15. Класифікація вірусів та шкідливого програмного забезпечення.						2
Практичне заняття 10. Програмні засоби антивірусного захисту інформації.				2		
Самостійна робота 16. Сучасні програмні засоби антивірусного захисту інформації.						2
Практичне заняття 11. Аналіз хмарних рішень для виявлення шкідливого програмного забезпечення.				2		
Самостійна робота 17. Хмарні антивірусні програми.						2
Тема 4. Несанкціонованих доступ до даних	18	4		4		10
Лекція 6. Основні принципи та методи забезпечення інформаційної безпеки		2				
Самостійна робота 18. Несанкціонований доступ до даних.						2
Практичне заняття 12. Аналізатор мережевих протоколів Wireshark				2		
Самостійна робота 19. Аналізатори мережевого трафіку						2
Лекція 7. Програмні засоби виявлення і запобігання вторгненням		2				
Самостійна робота 20. Засоби виявлення та запобігання вторгненням.						2

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	ЛЗ	СР
<i>I</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>
Практичне заняття 13. Аналіз систем виявлення вторгнень				2		
Самостійна робота 21. Системи виявлення вторгнень.						2
Самостійна робота 22. Системи запобігання вторгненням						2
Тема 5. Альтернативні засоби захисту інформації	20	2		6		12
Лекція 8. Протоколи автентифікації. Алгоритми електронного цифрового підпису.		2				
Самостійна робота 23. Протоколи аутентифікації та ідентифікації.						2
Самостійна робота 24. Загрози протоколів аутентифікації.						2
Практичне заняття 14. Програмні засоби створення та збереження надійних паролів				2		
Самостійна робота 25. Вимоги до створення надійного пароля.						2
Самостійна робота 26. Менеджери паролів.						2
Практичне заняття 15. Створення електронного цифрового підпису.				2		
Самостійна робота 27. Алгоритми електронного цифрового підпису.						2
Практичне заняття 16. Хмарні сервіси для резервного зберігання інформації				2		
Самостійна робота 28. Види хмарних сервісів для резервного зберігання інформації.						2
Тема 6. Криптографічних захист інформації	16	2		6		8
Лекція 9. Програмні засоби криптографічного захисту інформації. Характеристика алгоритмів шифрування.		2				
Самостійна робота 29. Характеристика алгоритмів шифрування						2
Практичне заняття 17. Шифрування та розшифрування інформації				2		
Самостійна робота 30. Шифрування інформації способами простої та складної заміни.						2
Практичне заняття 18. Асиметричний алгоритм шифрування				2		
Самостійна робота 31. Асиметричний алгоритм шифрування RSA						2
Самостійна робота 32. Підготовка до проходження модульної контрольної роботи 2.						2
Практичне заняття 19. Модульна контрольна робота 2.				2		
Всього годин за змістовий модуль 2.	66	10		20		36
Підсумковий контроль (екзамен)						
Всього годин за навчальну дисципліну	120	18		38		64

4. Основні методи навчання

Під час викладання навчальної дисципліни використовуються такі методи навчання як індуктивний, дедуктивний, продуктивний, дослідницький та метод стимулювання.

Індуктивний метод полягає в тому, що викладач спершу викладає факти, проводить досліди, поступово підводить слухачів до узагальнень, визначення понять. Дедуктивний метод полягає в тому, що викладач повідомляє загальне положення, закон, а потім роблячи висновки поступово підводить до конкретних висновків, ставить конкретні завдання. Продуктивний метод пов'язаний з опануванням нових знань у процесі творчої роботи.

5. Оцінювання результатів навчання

5.1 Результати навчання здобувача вищої освіти з навчальної дисципліни оцінюються за 100-бальною шкалою як сума балів поточного та підсумкового контролю із застосуванням наступних вагових коефіцієнтів, загальна сума яких дорівнює 1:

Вид контролю	Ваговий коефіцієнт
Поточний контроль (К)	0,8
Підсумковий контроль (ПК)	0,2

Підсумкова семестрова оцінка (ПСО) обчислюється за формулою: $ПСО=К+ПК$

5.2. Складниками для обчислення балу поточного контролю здобувача вищої освіти є:

Види навчальної діяльності	Кількість балів (максимальна за одиницю)	Кількість одиниць	Максимальна кількість балів*
Виконання завдань під час практичних занять	5	17	80
Виконання модульної контрольної роботи	20	2	40
Максимальна кількість балів (середнє арифметичне)			120

Мінімальна кількість балів для допуску до підсумкового контролю 50

Для переведення балів підсумкового контролю в 100-бальну систему необхідно отримані бали поділити на 1,5

5.3. Шкала оцінювання здобувача вищої освіти

Оцінка за шкалою ЄКТС	Оцінка за 100-бальною шкалою	Значення оцінки
A	90-100	<i>Відмінно – відмінне виконання лише з незначною кількістю помилок.</i> 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.
B	84-89	<i>Дуже добре – вище середнього рівня, але з кількома помилками.</i> Здобувач вищої освіти вільно володіє вивченим обсягом матеріалу, застосовує його на практиці, вільно розв'язує справи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна.
C	75-83	<i>Добре – загалом правильна робота, але з певною кількістю помилок.</i> 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.
D	65-74	<i>Задовільно – непогано, але зі значною кількістю недоліків.</i> 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.
E	60-64	<i>Достатньо – виконання задовольняє мінімальні вимоги.</i> Здобувач вищої освіти володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні.
FX	35-59	<i>Незадовільно – потрібна додаткова робота.</i> Здобувач вищої освіти володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу
F	1-34	<i>Незадовільно – потрібна значна додаткова робота.</i> Здобувач вищої освіти володіє матеріалом на рівні елементарного розпізнання і відтворення окремих фактів, елементів, об'єктів.

6. Ресурсне забезпечення навчальної дисципліни

Рекомендовані джерела інформації

Основна література:

1. Микитишин А.Г. Операційні системи: консп. лекц. / укл. А.Г. Микитишин, І.В. Чихіра. – Тернопіль: ТНТУ імені Івана Пулюя, 2016. – 107 с.
2. Операційні системи: [Електронний ресурс]: навч. посіб. для студ. / В. Г. Зайцев, І. П. Дробязко; КПІ ім. Ігоря Сікорського. – Електронні текстові дані – Київ: КПІ ім. Ігоря Сікорського, 2019. – 240 с.
3. Авраменко В. С., Авраменко А. С. Основи операційних систем. Навчальний посібник. – Черкаси: ЧНУ імені Богдана Хмельницького, 2018. – 524 с.: іл. ISBN 966-552-157-8
4. Шеховцов В. А. Операційні системи / В.А. Шеховцов. – Київ: Видавнича група ВНУ, 2005. – 576 с.: іл.
5. Погребняк Б. І. Операційні системи : навч. посібник / Б. І. Погребняк, М. В. Булаєнко ; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків: ХНУМГ ім. О. М. Бекетова, 2018. – 104 с.
6. Федотова-Півень І.М. Операційні системи: навчальний посібник. [за ред. В.М.
7. Рудницького] / І.М. Федотова-Півень, І.В. Миронець, О.Б. Півень, С.В. Сисоєнко, Т.В. Миронюк; Черкаський державний технологічний університет. – Харків: ТОВ «ДІСА ПЛЮС», 2019. – 216 с.
8. Бондаренко М.Ф. Операційні системи: навчальний посібник. / М.Ф. Бондаренко, О.Г. Качко - Харків: Компанія СМІТ, 2008 - 432 с.
9. Захарченко М.В. Інформаційна безпека інформаційно-комунікаційних систем. Захист інформації від НСД у каналах зв'язку: навч. посіб. / М.В. Захарченко, В.В. Топалов, М.С. Русляченко // За ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2014. – 228 с.
10. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група ВНУ, 2009. – 608 с.
11. Захист інформації в комп'ютерних системах та мережах : навч. посібник / С. Г. Семенов [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". – Харків : НТУ "ХПІ", 2014. – 251 с.
12. Кібербезпека: сучасні технології захисту. Навчальний посібник для вищих навчальних закладів. / Остапов С.Е., Євсєєв С.П., Король О.Г. – Львів: «Новий світ-2000», 2019. – 678 с.
13. Тарнавський Ю. А. Технології захисту інформації / Ю. А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
14. Мнушка, О.В. Безпека програм і даних : конспект лекцій для студентів за спеціальністю 121 «Інженерія програмного забезпечення» / Мнушка О.В. - Харків, ХНАДУ, 2020.
15. Захист інформації в автоматизованих системах управління : навч. посібник / Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

16. Каплун, В. А. Захист програмного забезпечення [Текст] : навчальний посібник. Ч. 2 / В. А. Каплун, О. В. Дмитришин, Ю. В. Барішев ; ВНТУ. – Вінниця : ВНТУ, 2016. – 106 с.

17. Дудатьєв А.В. Захист програмного забезпечення. Ч.1 : навчальний посібник / Андрій Дудатьєв, Валентина Каплун, Василь Семеренко – Вінниця: ВНТУ, 2005. – 140 с.

Допоміжна література:

18. Andrew S. Tanenbaum. Modern Operating Systems, 3rd Edition. – Pearson, 2007. – 1104 p. ISBN-10: 0136006639, ISBN-13: 978-0136006633.

19. Pavel Yosifovich, Mark Russinovich, David Solomon, Alex Ionescu. Windows Internals, Part 1: System architecture, processes, threads, memory management, and more, 7th Edition – Microsoft Press, 2017. – 800 p. ISBN-10: 9780735684188, ISBN-13: 978-0735684188.

20. Evi Nemeth. UNIX and Linux System Administration Handbook, 5th Edition / Evi Nemeth, Garth Snyder, Trent Hein, Ben Whaley, Dan Mackin. – Addison-Wesley Professional, 2017. – 1232 p. ISBN-10: 0134277554, ISBN-13: 978-0134277554.

21. Kevin Wilson. MacOS Fundamentals: Catalina Edition: The Step-by-step Guide to Using your Mac. – Independently published, 2019. – 335 p. ISBN-10: 1708721118, ISBN-13: 978-1708721114.

22. Алгоритми і структури даних: посібник / Н. Б. Шаховська, Р. О. Голощук ; за заг. ред. В. В.Пасічника. - К.: Магнолія 2006, 2010. - 215 с.: рис., схеми. - (Комп'ютинг). - Бібліогр.: с. 200

23. Інформатики. Комп'ютерна техніка. Комп'ютерні технології: Підручник для студентів вищих навчальних закладів / В.А.Баженов , П.С.Угорський , В.М.Горлач та інш . – К.: Каравела, 2003,2004. - 464с.

24. Комп'ютерні мережі: [навчальний посібник] / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. — Львів: «Магнолія 2006», 2013

Адреса розміщення робочої програми навчальної дисципліни:

(офіційний вебсайт НА СБУ / платформа дистанційного навчання / електронний ресурс навчально-наукового інституту, кафедри, бібліотеки тощо)

7. Дані про перегляд робочої програми навчальної дисципліни

№ п/п	Дата, номер протоколу засідання кафедри (спільного засідання кафедр)	Рішення за результатами перегляду	Підпис керівника кафедри
1.			
2.			

29/3/12 - 17/10/16

25.10.24