Міністерство освіти і науки України

Харківський національний університет імені В. Н. Каразіна

Кафедра безпеки інформаційних систем і технологій

"ЗАТВЕРДЖУЮ"

Проректор з науково-педагогічної роботи

Антон ПАНТЕЛЕЙМОНОВ

"____" _____ 2020 р.

Робоча програма навчальної дисципліни

Захист інформації в інформаційно-комунікаційних системах

рівень вищої освіти перший (бакалаврський)

галузь знань 12 «Інформаційні технології»

спеціальність 125 – «Кібербезпека»

освітня програма Кібербезпека

спеціалізація

вид дисципліни обов'язкова

факультет комп'ютерних наук

2020 / 2021 навчальний рік

2

Програму рекомендовано до затвердження вченою радою факультету (інституту, центру)

"31" серпня 2020 року, протокол № 12

РОЗРОБНИКИ ПРОГРАМИ:

Єсін Віталій Іванович , доктор технічних наук, доцент, професор кафедри безпеки інформаційних систем і технологій;

Сватовський Ігор Іванович, кандидат технічних наук, старший науковий співробітник, доцент кафедри безпеки інформаційних систем і технологій.

Програму схвалено на засіданні кафедри безпеки інформаційних систем і технологій

Протокол від "31" серпня 2020 року № 1

Завідувач кафедри безпеки інформаційних систем і технологій

(підпис) Рассомахін С.Г.
(прізвище та ініціали)

Програму погоджено з гарантом освітньої (професійної/наукової) програми (керівником проектної групи) Кібербезпека
назва освітньої програми

Гарант освітньої (професійної/наукової) програми
(керівник проектної групи) Рассомахін Сергій Геннадійович

(підпис) Рассомахін С. Г.
(прізвище та ініціали)

Програму погоджено методичною комісією факультету комп'ютерних наук

Протокол від "31" серпня 2020 року № 1

Голова методичної комісії факультету комп'ютерних наук

Бердніков А. Г.

Додаток до робочої програми навчальної дисципліни «Захист інформації в інформаційно-комунікаційних системах».
Дію робочої програми продовжено: на 2021/2022 н. р.

Заступник декана факультету з навчальної роботи

_____ Євгенія КОЛОВАНОВА

« » серпня 2021 р.

Голова методичної комісії факультету комп'ютерних наук

_____ Анатолій БЕРДНІКОВ

« » серпня 2021 р.

Програму погоджено з гарантом освітньої програми 125 «Кібербезпека»
Гарант освітньої програми 125 «Кібербезпека»

_____ Сергій РАССОМАХІН

ВСТУП

Програма навчальної дисципліни «Захист інформації в інформаційно-комунікаційних системах» складена відповідно до освітньї програми підготовки фахівця першого (бакалаврського) рівня вищої освіти за спеціальністю 125 – «Кібербезпека».

1. Опис навчальної дисципліни

1.1. Мета викладання навчальної дисципліни

Метою викладання навчальної дисципліни є закладення у студентів термінологічного фундаменту сучасних принципів організації захисту інформації в інформаційно-комунікаційних системах (ІКСМ), забезпечення безпеки процесів обробки, зберігання та поширення інформації в електричних, радіо і оптичних інформаційних і комунікаційних мережах з урахуванням сучасного стану та прогнозу розвитку методів, систем і засобів здійснення загроз з боку потенційних порушників.

1.2. Основні завдання вивчення дисципліни

Основними завданнями вивчення дисципліни є формування у студентів певних знань та вмінь з теорії та практики організації захисту інформації в інформаційно-комунікаційних системах.

Загальні компетентності (КЗ):

- знання та розуміння предметної області та розуміння професії (КЗ2);
- вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням (КЗ4).

Фахові компетентності (КФ):

- здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки (КФ2);
- здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах (КФ3);
- здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки (КФ4);
- здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки (КФ5);
- здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження (КФ6);
- здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки (КФ11).

1.3. Кількість кредитів – 13

1.4. Загальна кількість годин – 390

1.5. Характеристика навчальної дисципліни	
Нормативна / за вибором	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
3-й	
Семестр	
6-й	

Лекції
48 год.
Практичні, семінарські заняття
16 год.
Лабораторні заняття
32 год.
Самостійна робота
54 год.
Індивідуальні завдання
У т.ч. індивідуальні завдання (курсова робота) 20год.
Рік підготовки
4-й
Семестр
7-й
Лекції
48 год.
Практичні, семінарські заняття
24 год.
Лабораторні заняття
24 год.
Самостійна робота
54 год.
Індивідуальні завдання
Рік підготовки
4-й
Семестр
8-й
Лекції
24 год.
Практичні, семінарські заняття
12 год.
Лабораторні заняття
12 год.
Самостійна робота
42 год.
Індивідуальні завдання
У т.ч. індивідуальні завдання (курсова робота) 20год.

1.6. Заплановані результати навчання

ЗНАТИ:

– моделі даних, архітектуру побудови СУБД;
– основні положення, підходи та етапи проектування баз даних;
– основи проектування реляційних БД з використанням моделі «сутність-зв'язок»;
– основи мови SQL;
– основи паралельної обробки транзакцій в БД, які розраховані на багато користувачів;
– основи безпеки БД та методи адміністрування безпеки БД;
– механізми захисту інформації, які реалізовані засобами СУБД;
– організацію здійснення захисту інформації в операційних системах, мережах та системах управління базами даних відповідно до стандартів з оцінки захищених систем;

–основи захисту авторського права і інтелектуальної власності;

–основи авторського право на комп'ютерні програми;

–основні механізми інформаційної безпеки в програмному забезпеченні, локальних та глобальних мережах, системах передачі даних та зв’язку.

ВМІТИ:

– організовувати застосування ПК у будь-якій інформаційно-комунікаційній системі;

– виявляти несправність в елементах та пристроях інформаційно-комунікаційних систем під час експлуатації, вибирати оптимальні режими експлуатації;

– реалізовувати системи захисту інформації в ІКСМ відповідно до стандартів з оцінки захищеності систем;

– проектувати бази даних та ІКСМ, що мають необхідні характеристики безпеки даних відповідно до вимог міжнародних і вітчизняних стандартів інформаційної безпеки, з урахуванням можливостей різних ОС;

– виявляти дії вірусів та іншого шкідливого програмного забезпечення.

2. Тематичний план навчальної дисципліни

Розділ 1. Вступ до баз даних.

Переваги і недоліки СУБД. Основні сфери застосування систем з базами даних. Трирівнева архітектура ANSI-SPARC. Моделі даних. Функції, що реалізовуються в СУБД. Компоненти СУБД. Технологія «клієнт/сервер».

Розділ 2. Реляційні СУБД.

Реляційна модель. Підходи до проектування бази даних. Проектування реляційних баз даних з використанням моделі ″сутність-зв'язок″. Методологія концептуального і логічного проектування баз даних. Фізичне проектування бази даних. Нормалізація як метод проектування баз даних. Призначення і структура мови SQL. Основні оператори мови визначення даних. Основні оператори мови маніпулювання даними.

Розділ 3. Основи NoSQL баз даних.

Основні класи NoSQL, NewSQL баз даних, їх характеристика, особливості, можливості, переваги та недоліки.

Розділ 4. Основи побудови та особливості експлуатації сучасних СУБД, які розраховані на багато користувачів.

Управління транзакціями в БД, які розраховані на багато користувачів. Паралельна обробка транзакцій. Відновлення бази даних. Основи СУБД Oracle.

Розділ 5. Основи захисту в СУБД.

Основи безпеки БД. Основи системи захисту Microsoft Access. Забезпечення безпеки даних засобами СУБД Microsoft Access останніх версій. Основні механізми захисту даних, які використовуються в СУБД Oracle. Методи автентифікації, які використовуються в СУБД Oracle. Методи авторизації в СУБД Oracle. Адміністрування безпеки СУБД Oracle. Основи шифрування в СУБД Oracle.

Розділ 6. Захист програм та даних.

Загрози безпеці програмному забезпеченню інформаційних систем. Методи і засоби захисту від шкідливого програмного забезпечення. Організація системи антивірусного захисту. Захист авторського права і інтелектуальної власності в світі і в Україні. Авторське право на комп'ютерні програми. Комп'ютерне піратство і основні методи боротьби з ним. Контроль життєвого циклу програмного забезпечення.

Особливості побудови і функціонування програмних продуктів з точки зору безпечного програмування. Уразливість переповнювання буфера, рядка формату, цілечисельного переповнювання.

Розділ 7. Захист в операційних системах.

Тема 1. Моделі безпеки основних операційних систем.

Розглядаються основні моделі безпеки операційних систем (ОС), їх вразливості; основні поняття захищеності ОС та механізми забезпечення контролю доступу до них.

Тема 2. Аналіз захищеності сучасних операційних систем.

Розглядаються основні терміни та поняття в області захищених ОС; аналізуються функції безпеки ОС на прикладі однієї з них та засоби підвищення захищеності сучасних ОС.

Тема 3.Принципи побудови захисних механізмів операційної системи Linux.

Розглядаються облікові записи користувачів, процедура реєстрації, права доступу до файлів, розмежування доступу, використання механізму SUDO, поводження з об'єктами файлової системи, монтування файлової системи, копіювання та запис даних, файлові посилання, безпека файлових систем ext*fs, безпечне управління процесами, способи автоматичного запуску і зупинки програм, засоби взаємодії між процесами, приховування процесів, консольні атаки, аудит подій і його безпека,мережеві можливості операційних систем Linux.

Розділ 8. Захист інформації в мережах та компонентах мереж.

Тема 1. Засоби забезпечення безпеки в обчислювальних мережах.

Розглядаються загальні принципи побудови обчислювальних мереж, їх класифікація, моделі та основні протоколи взаємодії, поняття мережевої операційної системи, принципи забезпечення структурної та функціональної безпеки мереж, переваги і недоліки основних методів комутації, маршрутизації та доступу.

Тема 2. Засоби захисту локальних мереж.

Розглядаються принципи побудови локальних мереж, їх основні компоненти для сегментної організації мереж, методи доступу та стеки комунікаційних протоколів, особливості побудови бездротових мереж та їх стандарти, основні вразливості та заходи по забезпеченню безпеки в бездротових мережах.

Тема 3.Методи забезпечення безпеки мереж при їх приєднанні до мережі Інтернет.

Розглядаються традиційні методи захисту мереж від типових атак, аналізуються типові загрози в мережах і методи їх нейтралізації, розглядаються методи міжмережевого екранування на різних рівнях взаємодії мереж та переваги і недоліки різних схем брандмауерів, а також методи підвищення ефективності захисту з використанням stealth-режиму, міжмережевих екранів нового покоління NGFW, бастіонних вузлів та методів інтеграції міжмережевих екранів в розподілені мережеві інфраструктури.

Тема 4. Основи технології віртуальних приватних мереж VPN.

Розглядаються принципи організації та класифікація VPN, основи їх побудови та використання, основні протоколи, що застосовуються при побудові VPN, і особливості їх реалізації на канальному, мережевому, транспортному та прикладному рівнях.

Розділ 9. Методи та технології захисту інформації в інформаційно-комунікаційних системах.

Тема 1. Мережеві атаки.

Розглядаються сучасний стан та тенденції розвитку мережевих атак, типові сценарії їх організації та етапи реалізації, онтологія мережевих атак та можливих їх наслідків.

Тема 2. Основи побудови систем виявлення атак і вторгнень.

Розглядаються моделі систем виявлення атак і вторгнень та класифікація таких систем, особливості реалізації сигнатурного аналізу та систем виявлення аномалій, альтернативні методи виявлення атак і вторгнень з використанням технологій штучного

інтелекту, системи аналізу захищеності, обманні системи (paddingcells) і хости-приманки (honeypot), реалізація комерційних систем виявлення вторгнень на прикладі рішень компанії Symantec.

Розділ 10. Управління мережевою безпекою.

Тема 1. Забезпечення захисту інформації при використанні хмарних технологій.

Розглядаються особливості застосування методів забезпечення захисту інформації при використанні хмарних технологій і сервісів та тенденції їх розвитку.

Тема 2. Управління системою мережевої безпеки.

Розглядаються основні завдання побудови і управління комплексною системою мережевої безпеки, інтеграції засобів мережевого або системного управління з механізмами управління засобами захисту.

3. Структура навчальної дисципліни

Назви розділів	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб.	інд.	с. р.		л	п	лаб.	інд.	с. р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Розділ 1. Вступ до баз даних												
Разом за розділом 1	8	6				2						
Розділ 2. Реляційні СУБД												
Разом за розділом 2	66	18	8	22		18						
Розділ 3. Основи NoSQL баз даних												
Разом за розділом 3	10	4				6						
Розділ 4. Основи побудови та особливості експлуатації сучасних СУБД, які розраховані на багато користувачів												
Разом за розділом 4	22	8	6			8						
Розділ 5. Основи захисту в СУБД												
Разом за розділом 5	44	12	2	10		20						
Розділ 6. Захист програм та даних												
Разом за розділом 6	34	14	6	2		12						
Розділ 7. Захист в операційних системах												
Разом за розділом 7	116	34	18	22		42						
Розділ 8. Захист інформації в мережах та компонентах мереж												
Разом за розділом 8	62	18	6	12		26						
Розділ 9. Методи та технології захисту інформації в інформаційно-комунікаційних системах												
Разом за розділом 9	18	4	4			10						
Розділ 10. Управління мережевою безпекою												
Разом за розділом 10	10	2	2			6						
Усього годин	**390**	**12**	**52**	**68**		**150**						

		0										

4. Теми семінарських (практичних, лабораторних) занять

№ з/п	Назва теми	Кількість годин
1	Концептуальне і логічне проектування бази даних	6
2	Основи роботи в середовищі СУБД Microsoft Access	2
3	Проектування бази даних на основі принципів нормалізації	4
4	Використання операторів мови визначення даних мови SQL	2
5	Використання операторів мови маніпулювання даними мови SQL.	4
6	Розробка екранних форм для роботи з базою даних в середовищі Microsoft Access	4
7	Розробка звітів у середовищі Microsoft Access	4
8	Установка Oracle Server і Oracle Client на ОС Windows	2
9	Основи роботи з PL/SQL Developer	4
10	Система безпеки Microsoft Access	4
11	Адміністрування безпеки СУБД Oracle	4
12	Шифрування в СУБД Oracle за допомогою стандартних пакетів	4
13	Способи виявлення вірусів	2
14	Моделі безпеки основних операційних систем	4
15	Аналіз захищеності сучасних операційних систем	6
16	Принципи побудови захисних механізмів операційної системи Linux	36
17	Засоби забезпечення безпеки в обчислювальних мережах	2
18	Засоби захисту локальних мереж	2
19	Методи забезпечення безпеки мереж при їх приєднанні до мережі Інтернет	10
20	Основи технології віртуальних приватних мереж -VPN	4
21	Мережеві атаки	2
22	Основи побудови систем виявлення атак і вторгнень	2
23	Забезпечення захисту інформації при використанні хмарних технологій	1
24	Управління системою мережевої безпеки	1
	Разом:	120

5. Завдання для самостійної робота

№ з/п	Види, зміст самостійної роботи	Кількість годин
1	Вступ до баз даних	2
2	Основи проектування баз даних	5
3	Основи мови SQL	8
4	Вступ до NoSQL баз даних	6
5	Основи побудови та особливості експлуатації сучасних СУБД, які розраховані на багато користувачів	8
6	Основи захисту в СУБД	5
7	Курсова робота	20
8	Захист програм та даних	12
9	Моделі безпеки основних операційних систем	8
10	Аналіз захищеності сучасних операційних систем	8
11	Принципи побудови захисних механізмів операційної системи Linux	6

12	Засоби забезпечення безпеки в обчислювальних мережах	6
13	Засоби захисту локальних мереж	6
14	Методи забезпечення безпеки мереж при їх приєднанні до мережі Інтернет	6
15	Основи технології віртуальних приватних мереж VPN	8
16	Мережеві атаки	4
17	Основи побудови систем виявлення атак і вторгнень	6
18	Забезпечення захисту інформації при використанні хмарних технологій	3
19	Управління системою мережевої безпеки	3
20	Курсова робота	20
	Разом:	150

6. Індивідуальні завдання

Індивідуальне завдання – 2 курсові роботи з дисципліни у 6, 8 семестрах.

У 6 семестрі курсова робота, пов’язана з тематикою «Розробки бази даних компанії (організації, установи) із забезпеченням захисту її даних».

Суть завдання, що виконується в курсовій роботі, полягає у розробці БД для потреб компанії (організації, установи), дослідженні змісту елементів системи захисту даних бази і обґрунтуванні вимог до їх використання в конкретних умовах функціонування.

У 8 семестрі курсова робота, пов’язана з тематикою «Методи і засоби забезпечення безпеки при передачі даних в локальних і глобальних мережах».

Суть завдання, що виконується в курсовій роботі, полягає у проведенні аналізу, систематизуванні та узагальненні інформації за обраною тематикою, обґрунтуванні та формулюванні пропозицій з найкращого вирішення задачі, що розглядається.

7. Методи навчання

Як правило лекційні та практичні заняття проводяться аудиторне. В умовах дії карантину заняття проводяться відповідно до Наказу ректора Харківського національного університету імені В.Н. Каразіна (аудиторне або дистанційно за допомогою платформ Google Meet або Zoom).

8. Методи контролю

Контроль засвоєння студентами навчального матеріалу на лекційному зайнятті здійснюється шляхом концентрації уваги студентів постановкою питань за раніше вивченим матеріалом, пов'язаним з тематикою лекції.

На лабораторних та практичних заняттях контроль засвоєння студентами навчального матеріалу здійснюється шляхом оцінки якості оформлення звіту і його захисту. Рівень знань, продемонстрований студентами при оформленні і захисті звітів з лабораторних та практичних занять оцінюється окремо для кожного заняття кількістю балів відповідно до наведеної нижче таблиці.

Контроль засвоєння студентами навчального матеріалу здійснюється на 3-х контрольних роботах, що передбачені навчальним планом. Рівень знань, продемонстрований студентами на кожної контрольній роботі оцінюється кількістю балів відповідно до наведеної нижче таблиці.

При виконанні курсових робіт контролюється рівень засвоєння студентами системного розуміння проблеми. Бали за кожну курсову роботу складаються з розрахунку: 12 балів за зміст і акуратність оформлення розрахунково-пояснювальної записки (відповідно до вимог методичних вказівок по оформленню курсової роботи) і 8

балів за захист курсової роботи. Максимальна кількість балів за кожну курсову роботу складає 20 балів.

Максимальна кількість балів за результатами контролю поточної успішності складає 60 балів.

Таблиця 8.1 – Розподіл балів, які отримують студенти за результатами контролю поточної успішності

Вид заняття / контрольний захід	**Оцінка** $O_{сем}$
6 семестр	
Практичні заняття	
Концептуальне і логічне проектування бази даних	6
Лабораторні заняття	
Основи роботи в середовищі СУБД Microsoft Access	2
Проектування бази даних на основі принципів нормалізації	4
Використання операторів мови визначення даних мови SQL	3
Використання операторів мови маніпулювання даними мови SQL.	3
Розробка екранних форм для роботи з базою даних в середовищі Microsoft Access	3
Розробка звітів у середовищі Microsoft Access	3
Система безпеки Microsoft Access	2
Адміністрування безпеки СУБД Oracle	3
Шифрування в СУБД Oracle за допомогою стандартних пакетів	3
Контрольна робота	
Контрольна робота 1	8
Курсова робота	
Курсова робота 1	20
Всього за семестр	60
7 семестр	
Практичні заняття	
Способи виявлення вірусів	10
Моделі безпеки основних операційних систем	10
Аналіз захищеності сучасних операційних систем	10
Лабораторні заняття	
Принципи побудови захисних механізмів операційної системи Linux	60
Контрольна робота	
Контрольна робота 2	10
Всього за семестр	100
8 семестр	
Практичні заняття	
Засоби забезпечення безпеки в обчислювальних мережах	6
Засоби захисту локальних мереж	6
Основи технології віртуальних приватних мереж VPN	6
Основи побудови систем виявлення атак і вторгнень	4
Забезпечення захисту інформації при використанні хмарних технологій	1
Управління системою мережевої безпеки	1
Лабораторні заняття	
Методи забезпечення безпеки мереж при їх приєднанні до мережі Інтернет	16
Курсова робота	
Курсова робота 2	20
Всього за семестр	60

Згідно рішенню кафедри безпеки інформаційних систем і технологій до іспиту не допускаються студенти, що не захистили звіти з практичних, лабораторних занять, не брали участь у виконанні контрольних робіт і не захистили курсову роботу.

Підсумковий контроль здійснюється шляхом проведення іспиту.

Екзаменаційний білет включає два теоретичних і одне практичне питання. Теоретичні питання оцінюються в 13 балів кожне, практичний – в 14 балів.

Максимальна кількість балів за результатами іспиту складає 40 балів.

Максимальна кількість балів за результатами вивчення дисципліни складає 100 балів.

6 семестр

Бали за поточний контроль знань по розділам протягом семестру		Контрольна робота, передбачена навчальним планом	Курсова робота	Разом сума балів у семестрі	Іспит	Загальна сума балів
Розділ 1,2	Розділ 3, 4, 5	8	20	60	40	100
24	8					

7 семестр

Бали за поточний контроль знань по розділам протягом семестру		Контрольна робота, передбачена навчальним планом	Курсова робота	Разом сума балів у семестрі	Загальна сума балів
Розділ 6	Розділ 7	10		100	100
10	80				

8 семестр

Бали за поточний контроль знань по розділам протягом семестру			Контрольна робота, передбачена навчальним планом	Курсова робота	Разом сума балів у семестрі	Іспит	Загальна сума балів
Розділ 8	Розділ 9	Розділ 10	8	20	60	40	100
18	10	4					

Критерії оцінювання

Критерії оцінювання знань студентів за виконання практичних, лабораторних занять

Визначення	Кількість балів*
Завдання з практичного, лабораторного заняття виконано самостійно в повному обсязі. Звіт оформлений акуратно відповідно до вимог методичних вказівок. При захисті звіту показано розуміння суті і змісту проведених досліджень	N_{max}
Завдання з практичного, лабораторного заняття виконано самостійно в повному обсязі. Звіт оформлений достатньо акуратно відповідно до вимог методичних вказівок. При захисті звіту були виявлені незначні помилки у знанні теоретичного матеріалу	$N_{max} - \frac{N_{max}}{4}$
Завдання з практичного, лабораторного заняття виконано в повному обсязі. Звіт оформлений достатньо акуратно, в оформленні звіту є незначні недоліки. При захисті звіту були виявлені незначні помилки у знанні теоретичного матеріалу	$N_{max} - 2 \times \frac{N_{max}}{4}$
Завдання з практичного, лабораторного заняття виконано. Звіт оформлений з помилками і недоліками. При захисті звіту були	$N_{max} - 3 \times \frac{N_{max}}{4}$

виявлені суттєві помилки у знанні теоретичного матеріалу	

$*$ N_{max} – максимальна кількість балів для відповідного заняття відповідно до таблиці 7.1.

Критерії оцінювання знань студентів за виконання контрольній роботи

Визначення	Кількість балів		
	Контрольна робота 1	Контрольна робота 2	Контрольна робота 3
Дані повні відповіді на кожне питання показано тверде знання навчального матеріалу, розуміння суті поставлених питань, зроблені повні і правильні висновки	8	10	8
У відповідях на поставлені питання показано знання навчального матеріалу, розуміння суті поставлених питань за наявності незначних помилок зроблені достатньо повні і правильні висновки	5-7	7-9	5-7
У відповідях на поставлені питання показано достатньо знання навчального матеріалу при наявності суттєвих помилок, зроблені висновки	2-4	4-6	2-4
У відповідях показано розуміння суті поставлених питань за наявності принципових помилок при рішенні практичних завдань, відсутні висновки	1	2-3	1
У відповідях на поставлені питання показано слабкі знання навчального матеріалу при наявності принципових помилок, відсутні висновки	0,5	0,5-1	0,5

Критерії оцінювання знань студентів за виконання курсової роботі

Визначення	Кількість балів
Завдання на курсову роботу виконано акуратно в повній відповідності з вимог методичних вказівок. Студентом показано тверді знання навчального матеріалу, вміння чітко і стисло викладати основні результати дослідження.	20
Завдання на курсову роботу виконано досить акуратно, але не в повній відповідності з вимогами методичних вказівок. Студентом показано достатньо тверді знання навчального матеріалу і вміння стисло викладати основні результати дослідження.	12-19
Завдання на курсову роботу виконано не в повній відповідності з вимогами методичних вказівок. Студентом показано не достатньо тверді знання навчального матеріалу і вміння викладати основні результати дослідження.	4-11
Завдання на курсову роботу виконано не в повній відповідності з вимогами методичних вказівок. Студентом показано слабкі знання навчального матеріалу і невміння викладати основні результати дослідження. У розрахунково-пояснювальній записці є суттєві помилки	1-4

Критерії оцінювання екзаменаційних робіт студентів

Визначення	Кількість балів

При відповіді на екзаменаційний білет питання висвітлені повністю, завдання вирішено правильно, зроблені висновки	40
При відповіді на екзаменаційний білет питання достатньо висвітлені, завдання вирішено правильно з незначними помилками, зроблені висновки	35-39
При відповіді на екзаменаційний білет питання висвітлені з помилками, завдання вирішено правильно з незначними помилками. Зроблені неповні висновки	25-34
При відповіді на екзаменаційний білет питання висвітлені з суттєвими помилками, завдання вирішено з помилками. Зроблені неповні висновки	15-24
При відповіді на екзаменаційний білет питання висвітлені з суттєвими помилками, завдання вирішено частково або не повністю. Висновки неповні або відсутні	1-14

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка
	для чотирьохрівневої шкали оцінювання (іспит)
90 – 100	відмінно
70-89	добре
50-69	задовільно
1-49	незадовільно

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка для дворівневої шкали оцінювання
50 – 100	задовільно
1-49	незадовільно

10. Рекомендованалітература

Основна література

1. Єсін В. І., Кузнецов О. О., Сорока Л. С. Безпека інформаційних систем і технологій. Х.: ХНУ імені В. Н. Каразіна, 2013. 632 с.
2. Pfleeger C. P., Pfleeger S. L., Margulies J. Security in Computing, 5th ed. Pearson Education Inc.: New York, NY, USA, 2015.
3. Пасічник В. В. Організація баз даних та знань / В. В. Пасічник, В. Л. Резніченко. – К.: Видавнича група BHV, 2006. 384 с.
4. Connolly T. M., Begg C. E. Database systems: a practical approach to design, implementation, and management. Sixth edition. Harlow, Essex, England: Pearson Education Limited, 2015. 1329 p.
5. Date C. J. An Introduction to Database Systems. 8th ed. Pearson Education Inc.: New York, NY, USA, 2004.
6. Garcia-Molina H., Ullman J. D., Widom J. Database Systems. The Complete Book, 2th ed.; Pearson Prentice Hall: Upper Saddle River, NJ, USA, 2009.
7. Groff J., Weinberg P., Oppel A. SQL. The Complete Reference, 3rd ed.; McGraw-Hill Inc.: New York, NY, USA, 2010.
8. Kroenke D. M., Auer D. J. Database Processing. Fundamentals, Design, and

Implementation. 14th. ed. Pearson Education Inc.: New York, NY, USA, 2016. 637 p.
9. Sadalage P. J., Fowler M. NoSQL Distilled A Brief Guide to the Emerging World of Polyglot Persistence. Addison-Wesley Professional, 2012. 188 p.
10. Monnappa K. A. Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware. Packt Publishing Ltd, 2018.
11. Tanenbaum A. S., Bos H. Modern operating systems. Pearson Education Inc.: New York, NY, USA, 2015. 1136 p.
12. William Stallings Operating Systems: Internals and Design Principles, 9th Edition. Pearson Education Limited, 2018. 732 p.
13. Wetherall D. J., Tanenbaum A. S. Computer networks. Pearson Education, 2011. 933 p.
14. William “Bo” Rothwel, Denise Kinsey Linux Essentials for Cybersecurity. Pearson Education, Inc., 2019. (e-book)
15. Applied Network Security / Arthur Salmon, Warun Levesque, Michael McLafferty - Packt Publishing, 2017.
16. William Stallings Cryptography and network security. Principles and practice. Eighth edition. Pearson Education Limited, 2023. 832 p.

Допоміжна література

1. Wright P. Protecting Oracle Database 12c. Apress, 2014. 308 p.
2. Feuerstein S., Pribyl B. Oracle PL/SQL Programming. 6th ed. O'Reilly Media: Sebastopol, CA, USA, 2014.
3. Greenwald R., Stackowiak R., Stern J. Oracle essentials: Oracle database 12c. Gravenstein Highway North, Sebastopol, CA: O'Reilly Media, Inc., 2013.
4. Alapati S. R. Expert Oracle Database 11g Administration. Apress, 2009.
5. Nanda A., Feuerstein S. Oracle PL/SQL for DBAs: Security, Scheduling, Performance & More. O'Reilly Media, Inc., 2005. 454 p.
6. Litchfield D. The Database Hacker’s Handbook: Defending Database Servers / David Litchfield, Chris Anley, John Heasman, Bill Grindlay. Wiley Publishing, Inc., 2005. 532 p.
7. Basic Security Testing with Kali Linux 2 (e-book) Copyright 2016 by Daniel W. Dieterle. 323 p.
8. Network Security PRIVATE Communication in a PUBLIC World. Third Edition. Pearson Education, Inc., 2023. 677 p.
9. Ali Sadiqui Computer Network Security. John Wiley & Sons, Inc., 2020. 246 p.
10. Joseph Migga Kizza Guide to Computer Network Security. Fifth Edition. Springer Nature Switzerland AG, 2020. 595 p.

10. Посилання на інформаційні ресурси в Інтернеті, відео-лекції, інше методичне забезпечення

1. Закон України від 05.07.94 № 80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах».
2. Система стандартів з баз даних. Структура системи словників інформаційних ресурсів : ДСТУ 3302-96. – [Чинний від 1997-01-01]. – К. : Держстандарт України 1996. – 29 с. – (Національний стандарт України).
3. American National Standards Institute (1975). ANSI/X3/SPARC Study Group on Data Base Management Systems. Interim Report, FDT. ACM SIGMOD Bulletin, 7(2).
4. Інформаційні технології. Еталонна модель керування даними (ISO/IECTR 10032:2003, IDT) : ДСТУ ISO/IECTR 10032:2012. – [Чинний від 2013-03-01]. – К. : Держспоживстандарт України 2012. – 48 с. – (Національний стандарт України).
5. ISO/IEC 27000:2018 Information technology. Security techniques. Information security management systems. Overview and vocabulary.

6. ISO/IEC 27032:2012 Information technology. Security techniques. Guidelines for cybersecurity.
7. ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model.
8. ISO/IEC 15408-2:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components.
9. ISO/IEC 15408-3:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components.
10. http://cert.gov.ua/
11. https://www.owasp.org/index.php/Main_Page
12. https://www.intel.com/content/www/us/en/security/hardware/hardware-security-overview.html
13. https://www.mcafee.com/
14. https://www.symantec.com/
15. https://www.trendmicro.com/
16. https://attack.mitre.org/
17. http://www.computersciencestudent.com/
18. http://jrnl.nau.edu.ua/index.php/Infosecurity/index
19. https://www.offensive-security.com/
20. https://csrc.nist.gov/groups/computer-security-division/cryptographic-technology
21. **https://ocw.mit.edu/courses/6-858-computer-systems-security-fall-2014/**