Київський університет імені Бориса Грінченка

Факультет інформаційних технологій та управління

Кафедра інформаційної та кібернетичної безпеки

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ О.Б.Жильцов
«31» 01 2019 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ЗАХИСТ БАЗ ТА СХОВИЩ ДАНИХ»

для студентів денної форми

спеціальності	125 Кібербезпека
освітнього рівня	першого (бакалаврського)
освітньої програми	125.00.01 Безпека інформаційних і комунікаційних систем

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
Начальник відділу
моніторингу якості освіти
Програма № 2070/19
(підпис) (прізвище, ініціали)
«___» _____ 20 19 р.

Київ – 2019

Розробник:

Платоненко Артем Вадимович, старший викладач кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Викладач:

Платоненко Артем Вадимович, старший викладач кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки

Протокол від 16.01.2019 р. № 1

Завідувач кафедри _____ (підпис) В.Л. Бурячок

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем)

___.___. 20___ р.

Керівник освітньої програми _____ (підпис) В.В. Семко

Робочу програму перевірено

___.___. 20___ р.

Заступник директора/декана _____ (підпис) І.Ю. Мельник

Пролонговано:

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	обов'язкова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	4 / 120	
Курс	1 (3)	
Семестр	2 (6)	
Кількість змістових модулів з розподілом:	2	
Обсяг кредитів	4	
Обсяг годин, в тому числі:	120	
Аудиторні	42	
Модульний контроль	6	
Семестровий контроль	30	
Самостійна робота	42	
Форма семестрового контролю	Екзамен	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Захист баз та сховищ даних» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки на основі освітньо-професійної програми підготовки здобувачів першого (бакалаврського) рівня відповідно до навчальних планів спеціальності 125 Кібербезпека.

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач першого (бакалаврського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Захист баз та сховищ даних» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Захист баз та сховищ даних» складається з двох змістових модулів: Основи захисту баз даних, Засоби захисту сховищ даних. Обсяг дисципліни – 120 год (4 кредити).

Метою викладання навчальної дисципліни «Прикладні аспекти аналізу та синтезу політик безпеки» є отримання компетентностей в області практичного використання засобів захисту баз та сховищ даних.

Завдання:

- надання студентам теоретичних знань про основи захисту баз даних;
- формування у студентів категоріальних понять безпечного використання баз даних;
- формування у студентів уміння управління захистом баз та сховищ даних;
- стимулювання студентів до активної аналітико-пошукової роботи, що спрямована на визначення ефективних шляхів застосування засобів захисту баз та сховищ даних.

У результаті вивчення навчальної дисципліни формуються загальні компетентності:

- ***компетентності у сфері навчання:***
  - здатність до організації самостійної навчальної, практичної та науково-дослідної діяльності;
- ***компетентності у сфері застосування знань в практичних ситуаціях***
  - вміння застосовувати здобуті теоретико-концептуальні професійні знання у процесі практичної роботи;

фахові компетентності:

- ***компетентності у сфері проектування політик безпеки:***
  - глибокі знання та розуміння принципів застосування захищених баз та сховищ даних, необхідного апаратного і програмного забезпечення для їх впровадження;
  - уміння аналізувати створені параметри захищеності баз та сховищ даних;
  - здатність до самостійного налаштування параметрів захисту;
- **компетентності у сфері науково-дослідної діяльності:**
  - уміння вивчати і систематизувати знання у галузі збереження баз даних;
  - вивчати, узагальнювати й упроваджувати на практиці організаційні засоби захисту баз та сховищ даних.
- **компетентності у сфері вмінь працювати в групі:**
  - здатність використовувати навички взаємодії в роботі, компетентності у сфері навичок міжособистісного спілкування
  - здатність до продуктивного використання комунікації як складової професійної діяльності.

3. Результати навчання за дисципліною

При вивченні курсу «Захист баз та сховищ даних» студенти повинні

знати:

– історію та особливості розвитку баз та сховищ даних;

– основні процеси що вимагаються при впровадженні безпеки для баз та сховищ даних;

– класифікацію та характеристики апаратних і програмних засобів для ефективного впровадження захисту баз та сховищ даних;

– основні чинники, що визначають надійність і ефективність сховищ даних;

– понятійно-термінологічний апарат в області баз та сховищ даних;

уміти:

– визначати тип баз та сховищ даних;

– аналізувати ефективність обраної системи захисту баз та сховищ даних,

– виявляти особливості баз та сховищ даних;

– обґрунтовувати вибір технічних і програмних засобів для ефективного впровадження захисту баз та сховищ даних;

– визначати ресурси, необхідні для забезпечення надійності функціонування баз та сховищ даних, з врахуванням факторів помилки користувачів.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1. Основи захисту баз даних							
Тема 1. Поняття бази даних, їх призначення та функції	14	4		4			6
Тема 2. Класифікація баз даних та їх функціональні компоненти	14	4		4			6
Тема 3. Аналіз баз даних та їх особливості	14	2		4			8
Модульний контроль	2						
Разом	44	10		12			20
Змістовий модуль 2. Засоби захисту сховищ даних							
Тема 4. Розподіл типів сховищ даних	14	4		4			6
Тема 5. Методи та засоби захисту сховищ даних	14	2		4			8
Тема 6. Особливості підтримки безпеки сховищ даних	14	2		4			8
Модульний контроль	4						
Разом	46	8		12			22
Підготовка та проходження контрольних заходів	30						
Усього	120	18		24			42

5. Програма навчальної дисципліни

Змістовий модуль 1. Основи захисту баз даних.

Основні питання:

- Поняття бази даних, їх призначення та функції
- Класифікація баз даних та їх функціональні компоненти
- Аналіз баз даних та їх особливості

Змістовий модуль 2. Засоби захисту сховищ даних.

Основні питання:

- Розподіл типів сховищ даних
- Методи та засоби захисту сховищ даних
- Особливості підтримки безпеки сховищ даних

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип пооперaційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних заняттях та семінарах, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, екзамен.
- *Комп'ютерного контролю:* тестові програми.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних та індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних та індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	5	5	4	4
Відвідування практичних занять	1	6	6	6	6
Робота на практичному занятті	10	6	60	6	60
Виконання завдань для самостійної роботи	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25
Виконання ІНДЗ	30				
	Разом	-	101	-	100
Максимальна кількість балів: 201					
Розрахунок коефіцієнта: 201/60=3,35					

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1. Основи захисту баз даних		**20**	**5**
1	Поняття бази даних, їх призначення та функції	6	1
2	Класифікація баз даних та їх функціональні компоненти	6	2
3	Аналіз баз даних та їх особливості	8	2
Змістовий модуль 2. Засоби захисту сховищ даних		**22**	**5**
4	Розподіл типів сховищ даних	6	2
5	Методи та засоби захисту сховищ даних	8	1
6	Особливості підтримки безпеки сховищ даних	8	2
	Разом	**42**	**10**

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв’язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – комп’ютерний тест, що складається 15 запитань закритої та відкритої форм.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі екзамену, умовою допуску до якого є отриманням студентом 35 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Форма проведення екзамену – комбінована. Екзамен оцінюється у 40 балів за розподілом: 10 балів – комплексний комп’ютерний тест з дисципліни; 30 балів – виконання практико-орієнтованого завдання.

Виконання практичного завдання передбачає перевірку рівня оволодіння студентом теоретичними знаннями та практичними вміннями здійснювати інтерактивного контенту за спеціальністю.

Оцінювання практичного завдання відбувається в межах від 0 до 30 балів, згідно критеріїв оцінювання, й здійснюється з урахуванням: рівнів сформованості аналітико-синтетичних, творчих та методичних умінь.

Бали за виконання тесту та бали за виконання практичного завдання додаються. Оцінювання результатів засвоєння теоретичних знань та оцінювання сформованості практичних навичок володіння цифровими технологіями студентами, продемонстровані на

екзамені, представлене у таблиці.

Підсумкова кількість балів (max – 40)	Оцінка за 4-бальною шкалою
1 – 23	«незадовільно»
24 – 29	«задовільно»
30 – 35	«добре»
36 – 40	«відмінно»

Орієнтовний перелік питань для семестрового контролю

1. Що таке база даних?
2. Що таке сховище даних?
3. Як класифікують бази даних?
4. Як класифікують сховища даних?
5. Для чого необхідний аналіз баз даних?
6. Які основні вимоги до захисту сховищ даних?
7. Методи впровадження захисту сховищ даних.
8. Важливість підтримки безпеки сховища даних.
9. Які основні функції сховища даних?
10. Чому важливо дотримуватись безпечного налаштування сховища даних?

Шкала відповідності оцінок

Рейтингова оцінка	**Сума балів за всі види навчальної діяльності**	**Значення оцінки**
A	90-100	Відмінно — відмінний рівень знань (умінь) в межах обов’язкового матеріалу з, можливими, незначними недоліками
B	82-89	Дуже добре - достатньо високий рівень знань (умінь) в межах обов’язкового матеріалу без суттєвих (грубих) помилок
C	75-81	Добре - в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	Задовільно - посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68	Достатньо - мінімально можливий допустимий рівень знань (умінь)
FX	35-59	Незадовільно з можливістю повторного складання - незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	Незадовільно з обов’язковим повторним вивченням курсу - досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична картка дисципліни

Разом: 120 год., лекції – 18 год., практичні заняття – 24 год., модульний контроль – 6 год., самостійна робота – 42 год.

Модулі (назви, бали)	**Змістовий модуль 1. Основи захисту баз даних (101 бал)**			**Змістовий модуль 2. Засоби захисту сховищ даних (100 балів)**		
Лекції (теми, бали)	№ 1 Поняття бази даних, їх призначення та функції (2 бали)	№ 2 Класифікація баз даних та їх функціональні компоненти (2 бали)	№ 3 Аналіз баз даних та їх особливості (1 бал)	№ 4 Розподіл типів сховищ даних (2 бали)	№ 5 Методи та засоби захисту сховищ даних (1 бал)	№ 6 Особливості підтримки безпеки сховищ даних (1 бал)
Практичні, заняття (теми, бали)	№ 1 Створення та управління базою даних (22 бали)	№ 2 Порівняння баз даних відповідно до їх функцій (22 бали)	№ 3 Порівняння особливостей баз даних (22 бали)	№ 4 Порівняння різних типів сховищ даних (22 бали)	№ 5 Порівняння методів та засобів захисту сховищ даних (22 бали)	№ 6 Налаштування безпеки сховища даних та її перевірка (22 бали)
Самостійна робота	Самостійна робота (5 балів)			Самостійна робота (5 балів)		
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)			Модульна контрольна робота 2 (25 балів)		
Підсумковий контроль (вид, бали)	Екзамен (40 балів)					

8. Рекомендовані джерела

Основна (базова):

1. ДСТУ 3918-1999 (ISO / IEC 1207:1995) "Інформаційні технології. Процеси життєвого циклу програмного забезпечення".
2. ДСТУ ISO / IEC TR 13335-1:2003 "Інформаційні технології. Керівництво з управління безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій.".
3. ДСТУ ISO / IEC TR 13335-2:2003 "Інформаційні технології. Керівництво з управління безпекою інформаційних технологій. Частина 2. Управління та планування безпеки інформаційних технологій.".
4. ДСТУ ISO / IEC TR 13335-3:2003 "Інформаційні технології. Керівництво з управління безпекою інформаційних технологій. Частина 3. Методи управління захистом інформаційних технологій".
5. ДСТУ ISO / IEC TR 13335-4:2005 ''Інформаційні технології. Керівництво з управління безпекою інформаційних технологій. Частина 4. Вибір засобівзахисту".
6. ДСТУ ISO / IEC TR 13335-5:2005 "Інформаційні технології. Керівництво з управління безпекою інформаційних технологій. Частина 5. Керівництво з управління мережею безпеки".

9. Додаткові ресурси

1. MVA Microsoft https://mva.microsoft.com Віртуальна академія компанії «Microsoft»
2. ITVDN https://itvdn.com/ Відео курси з програмування
3. ITC.UA http://itc.ua/ Інформаційний портал сучасних технологій