КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
Кафедра інженерії програмного забезпечення та кібербезпеки

СИЛАБУС

БЕЗПЕКА СИСТЕМ БАЗ ДАНИХ/
SECURITY OF DATABASE SYSTEMS
SYLLABUS

(ОП-2018)

освітній ступінь	**бакалавр /** bachelor
галузь знань	**12 Інформаційні технології /** Information Technology
спеціальності	**125 Кібербезпека /** Cybersecurity

Київ 2021

Розповсюдження і тиражування без офіційного дозволу КНТЕУ заборонено

Автор: С. Л. Рзаєва, к.т.н., доц.

Силабус розглянуто та затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки 27 серпня 2021 р., протокол № 1.

СИЛАБУС

БЕЗПЕКА СИСТЕМ БАЗ ДАНИХ/
SECURITY OF DATABASE SYSTEMS
SYLLABUS

освітній ступінь	**бакалавр /** bachelor
галузь знань	**12 Інформаційні технології /** Information Technology
спеціальності	**125 Кібербезпека /** Cybersecurity

Викладач: **Рзаєва Світлана Леонідіна**,

вчене звання та посада: кандидат техн. наук, доцент кафедри програмної, інженерії та кібербезпеки;

педагогічний стаж – 23 років;

контактиний телефон: (044)-531-49-57;

e-mail: rzaevasl@knute.edu.ua

наукові інтереси: бази даних, моделювання та аналіз ПЗ, програмування, системи захисту БД, інформаційні технології та системи

стажування та підвищення кваліфікації: Науково-практичний курс серії вебінарів компанії Linkos Group за темою «Інформаційні технології в економіці: інноваційні рішення захисту даних підприємства» (180 год.) Сертифікат № ITE010 виданий 25.05.2021. Навчальний вебінар «Головні метрики сучасної науки.Scopus та Web of Science», Сертифікат на 10 годин, №АА 1844 виданий 02.04.2021. Тренінг для підготовки експертів із забезпечення якості вищої освіти, Національне агентство із забезпечення якості вищої освіти, 18-19 січня 2021 р.проходила підвищення кваліфікації Корпорації «Парус» (м. Київ, сертифікати по різним модулях в період 2012-2017рр); Microsoft Україна сертифікат ДО751808 тема: «Використання хмарних сервісів Microsoft в освітньому процесі» (150 годин 5 кредитів), 09.11.2018; Група компаній «BGS Solutions» (м. Київ, курс підвищення кваліфікації по роботі з комп'ютерною програмою «1С: Підприємство» на тему «Технології програмування та конфігурування на платформі «1С: Підприємство 8». ТОВ «БІ ДЖІ ЕС КОНСАЛТИНГ» (м. Київ, Теоретико практичний курс по роботі з комп'ютерною програмою «1С: Підприємство» за модулем «Технології програмування та конфігурації на платформі «1С: Підприємство8»). Впровадження Microsoft Office 365 в освітній процес КНТЕУ.

1. Дисципліна: «БЕЗПЕКА СИСТЕМ БАЗ ДАНИХ»,

- рік навчання: ІІІ;
- семестр навчання: 6;
- кількість кредитів: 6;
- *кількість годин за семестр: 180 год.*
  - лекційних: *24 год.*
  - лабораторних: *24 год.*

- на самостійне опрацювання: *132 год.*

– *кількість аудиторних годин на тиждень:*
  - лекційних: *2 год.*
  - лабораторних: *2 год.*

2. Час та місце проведення:

– *аудиторні заняття* - відповідно до розкладу КНТЕУ з врахуванням специфіки дисципліни проведення останньої передбачено в аудиторіях: Б514;
– *поза аудиторна робота* - самостійна робота студента, результат виконання якої висвітлено засобами Office 365;
– *всі лабораторні завдання виконуються* на основі інтерактивних методів навчання у електронному середовищі. Передбачається можливість проведення лабораторних та лекційних занять на базах підприємств-партнерів.

3. Пререквізити та постреквізити навчальної дисципліни:

 пререквізити: дисципліна базується на знаннях та компетентностях, що набуває здобувач вищої освіти під час вивчення дисциплін «Бази даних», «Архітектура комп'ютера», «Операційні системи», «Безпека інформаційних систем», «Організація комп’ютерних мереж».

 постреквізити: дисципліна надає студентам необхідні знання та навички, які будуть корисні при вивченні дисциплін «Безпека телекомунікаційних мереж», при проходженні виробничої практики, підготовці до випускного кваліфікаційного проекту, у подальшій професійній діяльності.

4. Характеристика дисципліни:

4.1. <u>Призначення навчальної дисципліни:</u> дисципліна «Безпека систем баз даних» є вибірковою складовою підготовки сучасних фахівців з розробки інформаційних технологій. Її місце – на перетині традиційних фундаментальних дисциплін та дисциплін професійної підготовки бакалаврів.

4.2. <u>Мета вивчення дисципліни:</u> метою вивчення дисципліни «Безпека систем баз даних» є набуття теоретичних і практичних знань з механізмів

і засобів забезпечення захисту та цілісності даних, забезпечення конфіденційності систем баз даних.

4.3. <u>Задачі вивчення дисципліни:</u> Основними завданнями вивчення дисципліни «Безпека систем баз даних» є формування у студентів компетентностей, що набуває здобувач вищої освіти по закінченню вивчення даної дисципліни:

Номер в освітній програмі	**Зміст компетентності**	**Номер теми, що розкриває зміст компетентності**
Загальні компетентності за освітньою програмою		
КЗ 1	Здатність застосовувати знання у практичних ситуаціях	1-11
КЗ 4	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням	1-11
КЗ 5	Здатність до пошуку, оброблення та аналізу інформації	1-11
Спеціальні (фахові, предметні) компетентності за освітньою програмою		
КФ5	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	3, 7, 8, 11
КФ12	Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки	9, 10, 11
Програмні результати навчання за освітньою програмою		
14	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень	3-11

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
16	Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів	1
19	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах	1, 4-8, 11
20	Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах	1, 11
27	Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.	1, 11
34	Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації	1-6
41	Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур	3, 4, 10

4.5. <u>Зміст навчальної дисципліни:</u> відповідає навчальній та робочій програмі, яка відповідає запитам стейкхолдерів.

5. План вивчення дисципліни:

ТЕОРЕТИЧНИЙ БЛОК:

Навчальна діяльність	Робочий час студента (год.)
1	2
Лекція 1. Концепція безпеки баз даних і систем управління базами даних План лекції 1. Нормативно-правова база. 2. Поняття безпеки баз даних. 3. Основні загрози безпеки систем БД. 4. Джерела загроз інформації баз даних. 5. Заходи захисту БД. *Список рекомендованих джерел* *основний:* 1; 2; 5; додатковий *7, 12,14;* *Internet-ресурси 18.*	2
Лекція 2. Засоби забезпечення цілісності даних План лекції 1. Поняття цілісності даних. 2. Режими забезпечення цілісності. 3. Обмеження цілісності. 4. *Список рекомендованих джерел* *основний: 1, 2, 5;* *додатковий: 7, 12, 14;* *Internet-ресурси 18.*	2
Лекція 3. Транзакції та забезпечення цілісності даних План лекції 1. Файли і файлові групи бази даних. 2. Логічні та фізичні імена файлів. 3. Поняття транзакції та забезпечення цілісності даних. 4. Властивості транзакцій. *Список рекомендованих джерел*	2

1	2
основний: 3, 4, 6; *додатковий 9, 13, 14;* *Internet-ресурси 15, 16.*	
Лекція 4. Механізми транзакцій План лекції 1. Журнал транзакцій. Характеристики журналу транзакцій. 2. Логічна архітектура журналу транзакцій. 3. Фізична архітектура журналу транзакцій. 4. Підтримка реплікації транзакцій. 5. Конкурентні транзакції. Рівні ізольованості транзакцій. *Список рекомендованих джерел* *основний: 3, 4, 6;* *додатковий 9, 13, 14;* *Internet-ресурси 15, 16.*	2
Лекція 5. Механізми резервного копіювання баз даних План лекції 1. Створення резервних копій бази даних. 2. Критерії вибору стратегій резервного копіювання. 3. Типи резервних копій баз даних. 4. Журналізація створення резервних копій. *Список рекомендованих джерел* *основний: 3, 4, 6, 8;* *додатковий: 9, 10, 13;* *Internet-ресурси: 15, 16.*	2
Лекція 6. Відновлення систем баз даних *План лекції* 1. Моделі відновлення баз даних. 2. Відновлення бази даних до точки збою. 3. Відновлення транзакції. 4.Використання резервних копій журналу для відновлення до точки збою. *Список рекомендованих джерел* *основний: 3, 4, 6, 8;* *додатковий: 9, 10, 13;* *Internet-ресурси: 15, 16.*	2
Лекція 7. Засоби забезпечення конфіденційності систем баз даних План лекції	2

1	2
1. Аутентифікації користувачів. 2. Засоби аутентифікації об'єктів баз даних. 3. Режими аутентифікації. *Список рекомендованих джерел* *основний: 4, 5, 6;* *додатковий 9, 10, 11;* *Internet-ресурси 16, 17, 19.*	
Лекція 8. Методи забезпечення доступності систем баз даних *План лекції* 1. Авторізація користувачів. 2. Ролі та розмежування доступу на основі ролей. 3. Управління привілеями з допомогою ролей в СКБД. *Список рекомендованих джерел* *Основний:* 4, 5, 6; додатковий 9, 10, 11; Internet-ресурси 16, 17, 19.	2
Лекція 9. Аудит систем бази даних План лекції 1. Засоби і процеси підсистеми аудиту. 2. Специфікації аудиту. 3. Організація аудиту подій в системах управління базами даних. 4. Ведення журналу аудиту. *Список рекомендованих джерел* *основний: 4, 5, 6;* *додатковий: 9, 10, 11;* *Internet-ресурси: 16, 17, 19.*	2
Лекція 10. Методики оцінки вразливості СКБД План лекції 1. Методи і засоби верифікації баз даних. 2. Моніторинг активності на різних рівнях СКБД. 3. Моніторинг продуктивності з використанням сховища запитів. *Список рекомендованих джерел* *основний: 4, 5, 6;* *додатковий: 9, 10, 11;* *Internet-ресурси: 16, 17, 19.*	2

1	2
Лекція 11. Захист систем баз даних План лекції 1. Управління ключами безпеки. 2. Захист від несанкціонованого доступу користувачів. 3. Захист баз даних від «впровадження SQL-інєкцій». *Список рекомендованих джерел* *основний: 4, 5, 6;* *додатковий: 9, 10, 11;* *Internet-ресурси: 16, 17, 19.*	4

ЛАБОРАТОРНІ ЗАНЯТТЯ:

Навчальна діяльність	Робочий час студента (год.)	Оцінювання (бал)
1	2	3
Тема 3. Транзакції та забезпечення цілісності даних *Лабораторне заняття № 1* *Мета*: вивчити особливості обробки транзакцій та журналів транзакцій, які розміщуються у файлах. *Виконання*: в процесі виконання лабораторної роботи студент набуває практичних навичок щодо створення файлів і файлових груп за допомогою графічного сервісу СКБД Microsoft SQL Server та SQL-команд, а також механізмів підтримки цілісності даних при проведення транзакцій.	4	5
Тема 4. Механізми транзакцій *Лабораторне заняття № 2* *Мета*: вивчити механізми використання журналу транзакцій та відмінності Логічної і Фізичної архітектур журналу. *Виконання*: в процесі виконання лабораторної роботи студент набуває практичних навичок щодо: - розуміння процесів відкоту всіх незафіксованих транзакцій, одночасно з накатом змін, які зафіксовані в журналі, але не були записані на диск. -структури журналу транзакцій, - команди COMMIT і ROLLBACK	4	5
Тема 5. Механізми резервного копіювання баз даних	4	5

1	2	3
Лабораторне заняття № 3 *Мета*: вивчити особливості резервного копіювання баз даних у середовищі СКБД Microsoft SQL Server. *Виконання*: за допомогою графічного сервісу СКБД Microsoft SQL Server та команди BACKUP опанувати навичками повного або диференціального резервного копіювання баз даних, резервного копіювання журналу транзакцій.		
Тема 6. Відновлення систем баз даних **Засоби забезпечення конфіденційності систем баз даних** *Лабораторне заняття № 4* *Мета*: вивчити особливості відновлення баз даних у середовищі СКБД Microsoft SQL Server *Виконання*: за допомогою графічного сервісу СКБД Microsoft SQL Server та команди RESTORE опанувати навичками повного або диференціального відновлення баз даних, відновлення журналу транзакцій.	6	5
Тема 7. Засоби забезпечення конфіденційності систем баз даних *Лабораторне заняття № 5* *Мета*: вивчити режими аутентифікації користувачів та об'єктів баз даних. *Виконання*: за допомогою графічного сервісу СКБД Microsoft SQL Server Management Studio та команд CREATE LOGIN, CREATE USER опанувати навичками аутентифікації користувачів БД.	4	5
Тема 8. Методи забезпечення доступності систем баз даних *Лабораторне заняття № 6* *Мета*: вивчити особливості реалізації авторизації користувачів та надання їм привілеїв *Виконання*: за допомогою графічного сервісу СКБД Microsoft SQL Server Management Studio та команд CREATE ROLE, GRANT, DENY і REVOKE опанувати методами авторизації користувачів та надання їм привілеїв до об’єктів БД, створення ролей, проводити розмежування доступу до об’єктів БД на основі ролей.	6	5
Тема 9. Аудит систем бази даних *Лабораторне заняття № 7*	6	5

1	2	3
Мета: відпрацювання основних операцій з проведення аудиту бази даних. *Виконання*: за допомогою графічного сервісу СКБД Microsoft SQL Server опанувати навичками проведення аудиту бази даних та ведення журналу аудиту.		
Тема 10. Методики оцінки вразливості СКБД *Лабораторне заняття № 8* *Мета*: набути практичних навиків з моніторингу активності користувачів на рівні СКБД. *Виконання*: за допомогою графічного сервісу СКБД Microsoft SQL Server опанувати навичками проведення моніторингу активності користувачів. Параметри ALTER DATABASE SET	4	5
Тема 11. Захист систем баз даних *Лабораторне заняття № 9* *Мета*: відпрацювання основних операцій із захисту від несанкціонованого доступу користувачів до об'єктів баз даних та сервісів СКБД. *Виконання*: в процесі виконання лабораторної роботи студент набуває практичних навичок щодо: - стратегій шифрування даних: процедурної, декларативної; - захисту даних за допомогою функції *EncryptBy*(.), *DecryptBy*(.); - захисту від несанкціонованого доступу до об'єктів баз даних та сервісів СКБД від «впровадження SQL-ін’єкцій».	8	20

** всі лабораторні завдання виконуються на основі інтерактивних методів навчання у комп’ютерному середовищі*

САМОСТІЙНА РОБОТА:

Навчальна діяльність	Робочий час студента (год.)	Оцінювання (бал)
1	2	3
Тема 1. Концепція безпеки баз даних і систем управління базами даних *Самостійна робота студентів* Питання, що виносяться на самостійне опрацювання та підготовку есе: 1. Архітектура клієнт-сервер. 2. Основні задачі захисту даних.	10	3
Тема 2. Засоби забезпечення цілісності даних *Самостійна робота студентів* Питання, що виносяться на самостійне опрацювання та підготовку есе: **1**. Проблеми маніпулювання даними. 2. Обмеження цілісності даних. 3. Null-значення.	10	3
Тема 3. Транзакції та забезпечення цілісності даних *Самостійна робота студентів.* Питання, що виносяться на самостійне опрацювання та підготовку есе: 1. Введення в проблематику моделей TransRelational. Три рівня абстракції. Основний ідея. Таблиця значень полів. 2. Механізм тригерів і збережених процедур. 3. Встановлення та контроль цілісності даних на основі тригерів і збережених процедур.	10	3
Тема 4. Механізми транзакцій *Самостійна робота студентів* Питання, що виносяться на самостійне опрацювання та підготовку есе: 1.Робота з утилітами: msdb та db_ssisadmin. 2. Отримання дистрибутивів. Встановлення та налагодження Microsoft SQL Server. 3. Механізми ізоляції транзакцій.	10	3

1	2	3
Тема 5. Механізми резервного копіювання баз даних *Самостійна робота студентів* Питання, що виносяться на самостійне опрацювання та підготовку есе: 1. Резервування серверів СКБД. 2. Журналізація створення резервних копій.	12	3
Тема 6. Відновлення систем баз даних *Самостійна робота студентів* Питання, що виносяться на самостійне опрацювання та підготовку есе: 1. Точність відновлення або точка повернення. 2. Віддзеркалення баз даних. 3. Вимоги до відновлення резервних копій журналів транзакцій.	10	3
Тема 7. Засоби забезпечення конфіденційності систем баз даних *Самостійна робота студентів* Питання, що виносяться на самостійне опрацювання та підготовку есе. Забезпечення конфіденційності системи БД на основі рольової моделі доступу.	10	3
Тема 8. Методи забезпечення доступності систем баз даних *Самостійна робота студентів* Питання, що виносяться на самостійне опрацювання та підготовку есе. Методи дискреційного розмежування доступу.	10	3
Тема 9. Аудит систем бази даних *Самостійна робота студентів*. Питання, що виносяться на самостійне опрацювання та підготовку есе: 1. Тиражування та синхронізація в розподілених системах баз даних. 2. Тиражування даних. 3. Програма ISS Database Scanner.	5	3
Тема 10. Методики оцінки вразливості СКБД *Самостійна робота студентів* Питання, що виносяться на самостійне опрацювання та підготовку есе:	5	3

1	2	3
1. Програмування додатків в системі клієнт-сервер. 2. Підтримка технологій клієнт-сервер в стандарті мови SQL.		
Тема 11. Захист систем баз даних ***Самостійна робота студентів.*** Питання, що виносяться на самостійне опрацювання та підготовку есе: 1. Шифрування даних. 2. Стандарт шифрування даних. 3. Шифрування на основі відкритого ключа. 4.Двофазна фіксація.	10	10

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Нормативно-правова база

1.Положення про технічний захист інформації в Україні від 27 вересня 1999 року № 1229/99

2.Державний стандарт України ДСТУ 3396.0–96. Захист інформації. Технічний захист інформації. Основні положення.

3.Державний стандарт України ДСТУ 3396.2–97. Захист інформації. Технічний захист інформації. Терміни та визначення.

4.Концепція (основи державної політики) національної безпеки України від 21 грудня 2000 року №2171-111.

5.Концепція технічного захисту інформації в Україні від 8 жовтня 1997 року № 1126.

6.Положення про технічний захист інформації в Україні від 27 вересня 1999 року № 1229/9

Інтернет-ресурси

1. Захист баз даних – режим доступу: http://www.bseu.by/it/tohod/lekcii9_2.htm.

2. Захист інформаційних обєктів – режим доступу: http://www.warning.dp.ua/tel28.htm.

3.Адміністрування бази даних – режим доступу: http://ua-referat.com/%D0%90%D0%B4%D0%BC%D1%96%D0%BD%D1%96%D1%81%D1%82%D1%80%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D0%B1%D0%B0%D0%B7%D0%B8_%D0%B4%D0%B0%D0%BD%D0%B8%D1%85

4.Системи баз даних та знань – режим доступу: http://ism.lp.edu.ua/uk/content/systemy-baz-danyh-ta-znan-knyga-1-organizaciya-baz-danyh-ta-znan-0.

5.Технологія доступу, зберігання та адміністрування даних – режим доступу: http://posibniki.com.ua/post-tehnologiya-dostupu-zberigannya-ta-administruvannya-danih-u-kis.

7. Контроль та оцінювання результатів навчання:

Положення про оцінювання результатів навчання студентів і аспірантів наказ КНТЕУ №2891 від 16.09.2019р. (Електронний ресурс. Точка доступу: https://knute.edu.ua/file/NzU4MQ==/69da3a261374f213990591e6e9a812cd.pdf)

Під час вивчення дисципліни викладачем здійснюється поточний та підсумковий контроль. Поточний контроль та оцінювання передбачає:

- перевірку рівня засвоєння теоретичного матеріалу (тестування за матеріалами лекції, який здійснюється на початку кожної наступної лекції з використанням 365 Office);
- захист лабораторних робіт (проходить під час наступної лабораторної роботи);
- перевірка засвоєння матеріалу, що винесений на самостійне опрацювання під час фронтального опитування на лекції.

8. Політика навчальної дисципліни:

8.1. Відвідування лекційних та лабораторних занять: відвідування лекційних та лабораторних занять є обов'язковим. Допускаються пропуски занять з таких поважних причин, як хвороба (викладачу надається копія довідки від медичного закладу), участь в олімпіаді, творчому конкурсі тощо за попередньою домовленістю та згодою викладача за умови дозволу деканату (надаються документи чи інші матеріали, які підтверджують заявлену участь у діяльності студента).

8.2. Відпрацювання пропущених занять: відпрацювання пропущених занять є обов'язковим незалежно від причини пропущеного заняття. Лекційне заняття має бути відпрацьоване до наступної лекції на консультації викладача з використанням ПЗ 365 Office Teams. Відпрацювання лекційного матеріалу передбачає вивчення пропущеного теоретичного матеріалу та складання тесту за цим матеріалом. Лабораторне заняття відпрацьовується під час консультації викладача (розклад консультацій на сайті).

8.3. Правила поведінки під час занять: обов'язковим є дотримання техніки безпеки в комп'ютерних лабораторіях. Студенти повинні приймати активну участь в обговоренні навчально матеріалу ознайомившись з ним напередодні (навчальний матеріал надається

викладачем). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки практичних завдань в процесі заняття. Задля зручності, дозволяється використання ноутбуків та інших електронних пристроїв під час навчання в комп'ютерних аудиторіях (за взаємною згодою всіх учасників освітнього процесу)

8.4. **За порушення академічної доброчесності** студенти будуть притягнені до академічної відповідальності у відповідності до положення про дотримання академічної доброчесності педагогічними, науково-педагогічними, науковими працівниками та здобувачами вищої освіти КНТЕУ (Наказ КНТЕУ від 02.02.2018 №377. (Електронний ресурс. Точка доступу: https://knute.edu.ua/file/MTEyNDI=/f78c64a74cbbe5b4238729782d707efa.pdf)