МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ЗАТВЕРДЖУЮ
Заступник керівника
(проректор з науково-педагогічної роботи)
_____
Микола АФАНАСЬЄВ

ОРГАНІЗАЦІЯ І ЗБЕРЕЖЕННЯ БАЗ ДАНИХ

робоча програма навчальної дисципліни

Галузь знань ***12 Інформаційні технології***
Спеціальність ***125 Кібербезпека***
Освітній рівень ***перший (бакалаврський)***
Освітня програма ***Кібербезпека***

Статус дисципліни ***вибіркова***
Мова викладання, навчання та оцінювання ***українська***

Завідувач кафедри *кібербезпеки та інформаційних технологій* _____ *Сергій ЄВСЄЄВ*

Харків
2020

ЗАТВЕРДЖЕНО
на засіданні кафедри кібербезпеки
та інформаційних технологій
Протокол № 2 від 31.08.2020 р.

Розробник:
Мілевський С. В., к.е.н., доц. КІТ

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

Анотація навчальної дисципліни

Основною метою вивчення дисципліни є отримання студентами теоретичних знань та практичних навичок щодо проектування баз даних, застосування програмних систем для їх створення і ведення. Завдання дисципліни – Завданням дисципліни є математична та комп'ютерна підготовка студентів до засвоєння моделей, методів та інформаційних технологій баз даних, які є ядром інформаційних систем різного призначення.

Об'єктом вивчення дисципліни є бази даних, що складаються з великого числа взаємодіючих між собою елементів.

Предмет дисципліни – засоби побудови, організації та збереження баз даних.

Метою викладання дисципліни є розширення та поглиблення теоретичних знань і прикладних вмінь і навичок щодо проектування, організації та збереження баз даних.

Результатами вивчення даної дисципліни є придбання навичок з проектування та адміністрування баз даних, а також комплексних практичних навичок щодо управління безпекою баз даних.

Характеристика навчальної дисципліни

Курс	**3**
Семестр	**5**
Кількість кредитів ECTS	**7**
Форма підсумкового контролю	**екзамен**

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Основи технічного захисту інформації	Дипломний проект
Забезпечення інформаційної безпеки	
Комплексні системи захисту інформації	

Компетентності та результати навчання за дисципліною:

Компетентності	Результати навчання
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	РН–9. впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН–13. аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН–14. вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН–17. забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН–18. використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН–19. застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН–20 забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;

	РН–21. вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН–22. вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН–23. реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН–24. вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН–25. забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН–26. впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН–27. вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН–28. аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН–29. здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН–32. вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН–34. приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН–35. вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН–42. впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН–43. застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН–44. вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН–45. застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН–46. здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;

	РН–47. вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН–48. виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН–49. забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН–50. забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН–51. підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН–52. використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; РН–53. вирішувати задачі аналізу програмного коду на наявність можливих загроз.
КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.	РН–9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН–13 аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН–14 вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН–17 забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН–19 застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН–23 реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН–25 забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН–29 здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН–32 вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН–33 вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН–34 приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН–35 вирішувати задачі забезпечення та супроводу комплексних

	систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН–41 забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН–42 впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН–43 застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН–44 вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН–45 застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН–46 здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН–48 виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН–49 забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН–50 забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН–51 підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН–52 використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; РН–53 вирішувати задачі аналізу програмного коду на наявність можливих загроз.
КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.	РН–14 вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН–20 забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН–31застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН–36 виявляти небезпечні сигнали технічних засобів; РН–37 вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН–38 інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН–39 проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних

	документах; РН–40 інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; РН–47 вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН–48 виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;

Програма навчальної дисципліни

Змістовий модуль 1. Теоретичні основи і методологія проектування реляційних БД

Тема 1. *Еволюція пристроїв зовнішньої пам'яті й програмних систем управління даними*

Тема 2. *Проектування БД. Концептуальне проектування*

Тема 3. *Вступ в реляційну модель даних*

Тема 4. *Логічне проектування БД на основі принципів нормалізації*

Змістовий модуль 2. Засоби управління та забезпечення реляційних БД в СУБД MYSQL

Тема 5. *Мова баз даних SQL: загальний вступ і опис даних*

Тема 6. *Загальна характеристика оператора вибірки даних*

Тема 7. *Стандартні функції та підзапити*

Тема 8. *Засоби маніпулювання даними та адміністративні засоби мови SQL*

Перелік лабораторних занять, а також питань та завдань до самостійної роботи наведено у таблиці "Рейтинг-план навчальної дисципліни".

Методи навчання та викладання

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 проблемні лекції, презентації, бесіди, індивідуальні та групові проєкти, майстер-класи.

Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні та лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Контрольні заходи включають:

1) поточний контроль, що здійснюється протягом семестру під час проведення лекційних та лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що дозволяє студенту складати іспит, – 35 балів);

2) підсумковий/семестровий контроль, що проводиться у формі семестрового екзамену, відповідно до графіку навчального процесу.

Порядок здійснення поточного оцінювання знань студентів.

Оцінювання знань студента під час лекційних і лабораторних занять проводиться за такими критеріями:

- усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

- виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

- виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.

- аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.

- вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

- використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

- забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

- використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

- застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

- забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.

- застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

- вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі проведення семестрового екзамену, завданням якого є перевірка розуміння студентом програмного матеріалу в цілому, логіки та взаємозв'язків між окремими розділами, здатності творчого використання накопичених знань, вміння формулювати своє ставлення до певної проблеми навчальної дисципліни тощо.

Лекційні заняття: максимальна кількість балів становить 12 (робота на лекціях).

Лабораторні заняття: максимальна кількість балів становить 48 (активна участь у виконанні лабораторних робіт – 36, контрольні роботи – 12), а мінімальна – 29.

Самостійна робота: складається з часу, який здобувач витрачає на підготовку до виконання лабораторних робіт та на підготовку до екзамену з дисципліни, в технологічній карті бали на цій вид робіт не виділені.

Підсумковий контроль: проводиться з урахуванням іспиту.

Екзаменаційний білет охоплює програму дисципліни і передбачає визначення рівня знань та ступеня опанування студентами компетентностей.

Кожен екзаменаційний білет складається із 3 практичних ситуацій (одне стереотипне, одне діагностичне та одне евристичне завдання), які передбачають вирішення типових професійних завдань фахівця на робочому місці та дозволяють діагностувати рівень теоретичної підготовки студента і рівень його компетентності з навчальної дисципліни. Оцінювання кожного завдання екзаменаційного білету наступне: перше завдання – це виконання початкового логічного проектування у вигляді ER-діаграми, оцінюється 16 балами; друге завдання – присвячене створенню бази даних, виконання його оцінюється 18 балами; третє завдання – забезпечення безпеки розробленої бази даних, виконання його оцінюється 6 балами.

Результат семестрового екзамену оцінюється в балах (максимальна кількість – 40

балів, мінімальна кількість, що зараховується, – 25 балів) і проставляється у відповідній графі екзаменаційної "Відомості обліку успішності".

Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімально можлива кількість балів, набраних на екзамені, – 25.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: "60 і більше балів – зараховано", "59 і менше балів – не зараховано" та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано

Рейтинг-план навчальної дисципліни

Тема	Форми та види навчання		Форми оцінювання	Max бал
Тема 1	***Аудиторна робота***			
	Лекція	Тема 1. *Еволюція пристроїв зовнішньої пам'яті й програмних систем управління даними*	Робота на лекції	1,5
	Лабораторне заняття	Л/р №1. *Бази даних в середовищі Microsoft Excel*	Активна участь у виконанні лабораторних завдань Поточна КР	4,5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою Виконання індивідуальних завдань щодо елементів БД в середовищі MS Excel	Перевірка індивідуальних завдань	
Тема 2	***Аудиторна робота***			
	Лекція	Тема 2. *Проектування БД. Концептуальне проектування*	Робота на лекції	1,5
	Лабораторне заняття	Л/р №2. *Концептуальне проектування БД в середовищі MySQL Workbench*	Активна участь у виконанні лабораторних	4,5

			завдань Поточна КР	
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою Виконання індивідуальних завдань щодо елементів БД в середовищі MS Excel	Перевірка індивідуальних завдань	
Тема 3	***Аудиторна робота***			
	Лекція	Тема 3. *Вступ в реляційну модель даних*	Робота на лекції	1,5
	Лабораторне заняття	Л/р №3. *Операції реляційної алгебри*	Активна участь у виконанні лабораторних завдань Поточна КР	4,5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою	Перевірка індивідуальних завдань	
Тема 4	***Аудиторна робота***			
	Лекція	Тема 4. *Логічне проектування БД на основі принципів нормалізації*	Робота на лекції	1,5
	Лабораторне заняття	Л/р №4. *Логічне проектування БД і нормалізація*	Активна участь у виконанні лабораторних завдань Поточна КР	4,5
		Контрольна робота за змістовим модулем	Контрольна робота	6
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою Виконання індивідуальних завдань з логічного проектування БД		
Тема 5	***Аудиторна робота***			
	Лекція	Тема 5. *Мова баз даних SQL: загальний вступ і опис даних*	Робота на лекції	1,5
	Лабораторне заняття	Л/р №5. *Фізичне проектування БД в СУБД MySQL*	Активна участь у виконанні лабораторних завдань Поточна КР	4,5
	Самостійна робота			

	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою	Перевірка індивідуальних завдань	
Тема 6	***Аудиторна робота***			
	Лекція	Тема 6. *Загальна характеристика оператора вибірки даних*	Робота на лекції	1,5
	Лабораторне заняття	Л/р №6. *Добавлення даних в БД. Експорт-імпорт БД*	Активна участь у виконанні лабораторних завдань Поточна КР	4,5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою Виконання індивідуальних завдань з фізичного проектування БД	Перевірка індивідуальних завдань	
Тема 7	***Аудиторна робота***			
	Лекція	Тема 7. *Стандартні функції та підзапити*	Робота на лекції	1,5
	Лабораторне заняття	Л/р №7. *Вибірка даних. Запити на об'єднання таблиць*	Активна участь у виконанні лабораторних завдань Поточна КР	4,5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою Виконання індивідуальних завдань щодо створення запитів на вибірку даних	Перевірка індивідуальних завдань	
Тема 8	***Аудиторна робота***			
	Лекція	Тема 8. *Засоби маніпулювання даними та адміністративні засоби мови SQL*	Робота на лекції	1,5
	Лабораторне заняття	Л/р №8. *Запити на групування даних Безпекові аспекти адміністрування баз даних*	Активна участь у виконанні лабораторних завдань	4,5
		Контрольна робота за змістовим модулем	Контрольна робота	6
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою Виконання індивідуальних завдань щодо створення запитів на вибірку даних	Перевірка індивідуальних завдань	

Екзамен	40

Рекомендована література

Основна

1. Атре Ш. Структурный подход к организации баз данных. – М.: Финансы и статистика, 1983. – 320 с.
2. Боуман Джудит С., Эмерсон Сандра Л., Дарновски Марси. Практическое руководство по SQL. 3-е издание. : Пер. с англ. – Диалектика, 1997. – 320с.
3. Гайджарги В.І., Дацюк О.А. Основи проектування та використання баз даних: Навч. посібн. – 2-е вид.,¬ – К.: ІВЦ "Видавництво "Політехніка", ТОВ Фірма "Періодика", 2004. – 256 с.
4. Гарсіа-Молина Гектор, Ульман Джеффри Д., Уидом Дженифер. Системы баз данных. Полный курс. : Пер. с англ. – М.: "Вильямс", 2003. – 1088 с.
5. Дейт К. Введение в системы баз данных (седьмое издание) – СПб: Вильямс, Питер 2001, 1072 с.
6. Зайцева Т.В. Вступ до інформаційних технологій. - Херсон: Айлант. – 2000. – 196с.
7. Пасічник В.В., Резниченко В.А. Організація баз даних та знань. – К.: Видавнича група BHV, 2006. –384 с.
8. Теория и практика построения баз данных. 8-изд. / Д. Крёнке. СПб.: Питер, 2003. – 800 с.

Додаткова

9. Бекаревич Ю.Б., Пушкина Н.В. Самоучитель Microsoft* Access 2002. – СПб.: БХВ-Петербург, 2004. – 720 с. (або інший підручник з СКБД Access)
10. Дейт К. Руководство по реляционной СУБД DB2. – М.: Финансы и статистика, 1988. – 320 с.
11. ДСТУ 2874-94. ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ. Системи оброблення інформації. Бази даних. Терміни та визначення
12. Коннолли Т. Бегг К., Страчан А. Базы даних: проектирование, реализация и сопровождение. Теорія и практика, 2-е издание : Пер. с англ. – М.: Вильямс, 2001. – 1120 с. : ил.
13. Фісун М.Т., Ніколенко С.Г. Створення та ведення баз даних засобами мови Jet SQL:методичні вказівки до виконання робіт з дисципліни "Організація баз даних". – Миколаїв: Вид-во ЧДУ, 2009. – 83 с.

Інформаційні ресурси

14. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Організація і збереження баз даних" https://pns.hneu.edu.ua/course/view.php?id=4927