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

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

ЕКСПЕРТНІ СИСТЕМИ

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(-и):
Мілов О.В., д.т.н., проф. кафедри КІТ
Мілевський С.В., к.е.н., доц. кафедри КІТ

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри
2020/2021	31.08.2020	2	

Анотація навчальної дисципліни

Дисципліна "Експертні системи" викладається студентам першого рівня навчання з метою набуття ними знань в області сучасних технологій побудови та використання експертних систем.

Успішне вивчення дисципліни можливо при наявності у студентів комп'ютерної грамотності та володіння основними поняттями та методами теорії систем, основ математичного моделювання, вищої математики.

Поставлена мета досягається вирішенням наступних завдань при вивченні дисципліни:

1. вивчення моделей та організації експертних систем;
2. вивчення принципів проектування експетних систем в сучасній індустрії інформаційних технологій, сучасної термінології і методів вирішення завдань за допомогою експертних систем;
3. вивчення сучасних моделей обробки та інтерпретації експертних оцінок;
4. придбання практичних навичок роботи з конкретними технологіями експертних систем.

Характеристика навчальної дисципліни

Курс	**4**
Семестр	**7**
Кількість кредитів ECTS	**5**
Форма підсумкового контролю	**екзамен**

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Вступ до фаху	дипломний проєкт
Основи програмування	
Вища математика	

Компетентності та результати навчання за дисципліною

Фахові 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;

Фахові компетентності	Результати навчання
	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;

Фахові компетентності	Результати навчання
	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.

Фахові компетентності	Результати навчання
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

Фахові компетентності	Результати навчання
	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

Фахові компетентності	Результати навчання
	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

Тема 1. Введення.
Тема 2. Моделі представлення знань
Тема 3. Архітектура і технологія розробки експертних систем
Тема 4. Застосування нечіткої логіки в експертних системах
Тема 5. Генетичний алгоритм в задачах оптимізації
Тема 6. Штучні нейронні мережі в обробці інформації

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. Під час проведення лекцій застосовуються такі методи навчання як проблемні лекції (теми 1 – 6) та бесіди (теми 1, 5). Індивідуальні та групові проєкти застосовуються під час проведення лабораторних занять (теми 1 – 6).

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:

впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;

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;

вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);

вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;

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;

вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;

вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;

приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;

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;

впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;

застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;

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;

застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;

здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;

вирішувати задачі аналізу програмного коду на наявність можливих загроз.

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 – 12).

Лабораторні заняття: максимальна кількість балів становить 48 (захист лабораторних робіт – 24, контрольні роботи – 24), 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 екзамену.

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 20 тестових завдань закритої форми, виконання його оцінюється 20 балами; друге завдання – присвячене розробленню структурної схеми побудови корпоративної мережі компанії, виконання його оцінюється 10 балами; третє завдання – розрахункове, виконання його оцінюється 10 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.

Виставлення підсумкової оцінки здійснюється за шкалою, наведено в таблиці "Шкала оцінювання: національна та ЄКТС".

Форми оцінювання та розподіл балів наведено у таблиці "Рейтинг-план навчальної дисципліни".

Шкала оцінювання: національна та ЄКТС

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Оцінка ЄКТС</td><td colspan="2">Оцінка за національною шкалою</td></tr>
<tr><td>для екзамену, курсового проекту (роботи), практики</td><td>для заліку</td></tr>
<tr><td>90 – 100</td><td>A</td><td>відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>82 – 89</td><td>B</td><td rowspan="2">добре</td></tr>
<tr><td>74 – 81</td><td>C</td></tr>
<tr><td>64 – 73</td><td>D</td><td rowspan="2">задовільно</td></tr>
<tr><td>60 – 63</td><td>E</td></tr>
<tr><td>35 – 59</td><td>FX</td><td>незадовільно</td><td>не зараховано</td></tr>
</table>

Рейтинг-план навчальної дисципліни

Тема	Форми та види навчання		Форми оцінювання	Max бал
Тема 1	***Аудиторна робота***			
	Лекція	*Введення*. Мета і завдання дисципліни, її роль і місце в загальній системі підготовки фахівця. Подання знань в інформаційних системах як елемент штучного інтелекту і нових інформаційних технологій.	Робота на лекції	1
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 1	***Аудиторна робота***			
	Лекція	*Введення*. Етапи створення штучного інтелекту. Процес мислення. Основні поняття і класифікація систем, заснованих на знаннях. Принципи придбання знань.	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота № 1 *"Вивчення пакету Text Analyst"*	виконання лабораторних завдань	4
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 2	***Аудиторна робота***			
	Лекція	*Моделі представлення знань*. Логічна модель представлення знань і правила виводу. Продукційна модель і правила їх обробки. Висновки, засновані на продукційних правилах.	Робота на лекції	1
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 2	***Аудиторна робота***			
	Лекція	*Тема 2. Моделі представлення знань*. Теорія фреймів і фреймових систем. Об'єкти з фреймами. Основні атрибути (слоти) об'єкта.	Робота на лекції	1

		Процедурні фрейми і слоти. Подання знань у вигляді семантичної мережі. Модель дошки оголошень. Модель представлення знань у вигляді сценарію.		
	Лабораторне заняття	Лабораторна робота № 2. *"Мова декларативного програмування Prolog"*	виконання лабораторної роботи	4
			Поточна контрольна робота 1	12
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань. Підготовка до екзамену		
Тема 3	***Аудиторна робота***			
	Лекція	*Архітектура і технологія розробки експертних систем.* Введення в експертні системи. Ролі експерта, інженера знань і користувача. Загальний опис архітектури експертних систем. База знань, правила, машина виведення, інтерфейс користувача, засоби роботи з файлами.	Робота на лекції	1
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань. Підготовка до екзамену		
Тема 3	***Аудиторна робота***			
	Лекція	*Тема 3. Архітектура і технологія розробки експертних систем.* Технологія розробки експертних систем. Логічне програмування та експертні системи. Мови штучного інтелекту. Підсистема аналізу і синтезу вхідних і вихідних повідомлень. Діалогова підсистема. Пояснювальні здатності експертних систем.	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота № 3. *"Проектування простішої експертної системи"*	виконання лабораторної роботи	4
	Самостійна робота			
	Питання та завдання	Пошук, підбір та огляд		

	до самостійного опрацювання	літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань.		
Тема 4	***Аудиторна робота***			
	Лекція	*Тема 4. Застосування нечіткої логіки в експертних системах.* Поняття про нечітких множинах і їх зв'язок з теорією побудови експертних систем. Коефіцієнти впевненості. Зважування свідоцтв. Ставлення правдоподібності гіпотез.	Робота на лекції	1
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань. Підготовка до екзамену		
Тема 4	***Аудиторна робота***			
	Лекція	*Тема 4. Застосування нечіткої логіки в експертних системах.* Функція приналежності елемента підмножині. Операції над нечіткими множинами. Дефазифікації нечіткої множини. Нечіткі правила виведення в експертних системах.	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота № 4. *"Робота з нечіткими множинами та нечіткими правилами виведення в експертних системах"*.	виконання лабораторної роботи	4
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань. Підготовка до екзамену: виконання типових завдань за теорією		
Тема 5	***Аудиторна робота***			
	Лекція	*Тема 5. Генетичний алгоритм в задачах оптимізації* Поняття про генетичний алгоритм. Етапи роботи генетичного алгоритму. Кодування інформації та формування популяції. Оцінювання популяції. Селекція. Схрещування і формування нового покоління. Мутація. Налаштування параметрів	Робота на лекції	1

		генетичного алгоритму.		
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань. Підготовка до екзамену: виконання типових завдань за практичною складовою		
	Аудиторна робота			
Тема 5	Лекція	*Тема 5. Генетичний алгоритм в задачах оптимізації* Канонічний генетичний алгоритм. Приклад роботи генетичного алгоритму. Рекомендації до програмної реалізації генетичного алгоритму. Застосування генетичного алгоритму для вирішення завдань оптимізації та апроксимації.	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота № 5. *"Програмування та використання генетичного алгоритму для задач оптимізації та апроксимації"*	виконання лабораторної роботи	4
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань. Підготовка до екзамену: виконання типових завдань за практичною складовою		
Тема 6	Лекція	*Тема 6. Штучні нейронні мережі в обробці інформації* Поняття про нейромережевих системах. Біологічні нейронні мережі. Формальний нейрон. Штучні нейронні мережі. Навчання нейронної мережі. Алгоритм зворотного поширення помилки. Приклад роботи і навчання нейронної мережі. Програмна реалізація.	Робота на лекції	1
	Самостійна робота			

	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань. Підготовка до екзамену: виконання типових завдань за практичною складовою		
Тема 6	Лекція	*Тема 6. Штучні нейронні мережі в обробці інформації* Застосування нейронних мереж для вирішення задач апроксимації, класифікації, автоматичного управління, розпізнавання і прогнозування. Мультиагентні системи.	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота № 6. *"Робота з пакетом NeuroNet". Задачі прогнозування та класифікації.*	виконання лабораторної роботи	4
			Поточна контрольна робота 2	12
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань. Підготовка до екзамену: виконання типових завдань за практичною складовою		
	Екзамен			40

Рекомендована література

Основна

1. Джаратано Дж., Райли Г. Экспертные системы: принципы разработки и программирование. – М.: ООО “И.Д. Вильямс”, 2007. – 1152 с.
2. Люгер Д.Ф. Искусственный интеллект: стратегии и методы решения сложных проблем. – М.: Издательский дом “Вильямс”, 2003. – 864 с.
3. Спицын В.Г., Цой Ю.Р. Представление знаний в информационных системах: Учебное пособие. – Томск: Изд-во ТПУ, 2008. – 152 с.
4. Гаврилова Т.А. , Хорошевский В.Ф. Базы знаний интеллектуальных систем. Санкт-Петербург: Питер, 2000. - 382 с.
5. Змитрович А.И. Интеллектуальные информационные системы. Минск: Тетра Системс, 1997. – 367 с.
6. Осовский С. Нейронные сети для обработки информации – М.: Финансы и статистика ”, 2007. – 345 с.
7. Спицын В.Г., Цой Ю.Р. Применение искусственных нейронных сетей для обработки информации: Методические указания. – Томск: Изд-во ТПУ, 2008. – 31 с.
8. Джексон П. Введение в экспертные системы: Пер.с англ.- М.: Издательский дом “Вильямс”, 2001. - 624 с.

9. Попов Э.В. Экспертные системы. – М.: Наука, 1987, -288 с.

10. Спицын В.Г. Базы знаний и экспертные системы: Учебное пособие – Томск: Изд-во ТПУ, 2001. – 88 с.

11. Экспертные системы. Принцип работы и примеры. / Под ред. Р. Форсайда: Пер.с англ. – М.: Радио и связь, 1987. - 221 с.

Додаткова

12. Искусственный интеллект: Кн. 1. Системы общения и экспертные системы. Справочник. / Под ред. Э.В. Попова.-М.: Радио и связь, 1990. – 464 с.

13. Нейлор К. Как построить свою экспертную систему: Пер.с англ.- М.: Энергоатомиздат. 1991.- 288 с.

14. Элти Дж., Кумбо М. Экспертные системы: концепции и примеры: Пер.с англ. -М.: Финансы и статистика, 1987.- 191 с.

15. Горбань А.Н., Дунин-Барковский В.Л., Кирдин А.Н., и др. Нейроинформатика. – Новосибирск: Наука. Сибирское отделение РАН, 1998. – 296 с.

16. Нечеткие множества в моделях управления и искусственного интеллекта./ Под ред. Д.А. Поспелова- М.: Наука, 1986. – 311 с

17. Осуга С. Обработка знаний: Пер. с японск. – М.: Мир, 1989.- 293 с.

18. Уэно Х., Коямо Т., Окамото Т. и др. Представление и использование знаний: Пер. с японск. – М.: Мир, 1989.- 220 с.

19. Таунсенд К., Фохт Д. Проектирование и программная реализация экспертных систем на персональных ЭВМ: Пер.с англ.- М.: Финансы и статистика, 1990.- 320 с.

20. Марселлус Д. Программирование экспертных систем на Турбо Прологе: Пер.с англ.- М.: Финансы и статистика, 1994.- 256 с.

21. Ин Ц., Соломон Д. Использование Турбо – Пролога: Пер. с англ. – М.: Мир, 1993.- 608 с.

Інформаційні ресурси.

22. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Розробка та аналіз алгоритмів" https://pns.hneu.edu.ua/course/view.php?id=7453.