

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

"ЗАТВЕРДЖУЮ"

Заступник керівника
(проректор з науково-педагогічної роботи)


Микола АФАНАСЬЄВ



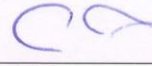
МЕРЕЖНЕ ПРОГРАМУВАННЯ

робоча програма навчальної дисципліни

| | |
|------------------|-----------------------------------|
| Галузь знань | <i>12 Інформаційні технології</i> |
| Спеціальність | <i>125 Кібербезпека</i> |
| Освітній рівень | <i>перший (бакалаврський)</i> |
| Освітня програма | <i>Кібербезпека</i> |

| | |
|---|-------------------|
| Статус дисципліни | <i>вибіркова</i> |
| Мова викладання, навчання та оцінювання | <i>українська</i> |

Завідувач кафедри
кібербезпеки та
інформаційних технологій



Сергій СВС

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

**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 "Мережне програмування" викладається студентам першого рівня навчання з метою набуття ними знань в області сучасних технологій розробки програмного забезпечення інформаційних мереж.

Успішне вивчення дисципліни можливо при наявності у студентів комп'ютерної грамотності та володіння основними поняттями та методами теорії систем, основами кіберзахисту, мовами програмування, принципами побудови баз даних.

Поставлена мета досягається вирішенням наступних завдань при вивченні дисципліни:

1. вивчення принципів організації і функціонування локальних і глобальних мереж;
2. вивчення принципів проектування програмного забезпечення в сучасній індустрії інформаційних технологій, сучасної термінології і методів автоматизації розробки програмного забезпечення;
3. вивчення сучасних моделей доступу до даних в глобальних інформаційних мережах на прикладі мережі Інтернет;
4. придбання практичних навичок роботи з конкретними технологіями мережевого програмування.

Характеристика навчальної дисципліни

| | |
|-----------------------------|---------|
| Курс | 4 |
| Семестр | 8 |
| Кількість кредитів ECTS | 5 |
| Форма підсумкового контролю | екзамен |

Структурно-логічна схема вивчення дисципліни

| Пререквізити | Постреквізити |
|----------------------|--------------------------|
| Вступ до фаху | Технології програмування |
| Основи програмування | |
| | |

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 |

| Фахові компетентності | Результати навчання |
|-----------------------|--|
| | <p>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</p> |

| Фахові компетентності | Результати навчання |
|-----------------------|---|
| | <p>загроз різних класів;</p> <p>РН–32. вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;</p> <p>РН–34. приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;</p> <p>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;</p> <p>РН–42. впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;</p> <p>РН–43. застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;</p> <p>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;</p> <p>РН–45. застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;</p> <p>РН–46. здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;</p> <p>РН–47. вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;</p> <p>РН–48. виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;</p> <p>РН–49. забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;</p> <p>РН–50. забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);</p> <p>РН–51. підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;</p> <p>РН–52. використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;</p> <p>РН–53. вирішувати задачі аналізу програмного коду на</p> |

| Фахові компетентності | Результати навчання |
|---|---|
| <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> | <p>наявність можливих загроз.</p> <p>РН–9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;</p> <p>РН–13 аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;</p> <p>РН–14 вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;</p> <p>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;</p> <p>РН–19 застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;</p> <p>РН–23 реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;</p> <p>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;</p> <p>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;</p> <p>РН–32 вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;</p> <p>РН–33 вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;</p> <p>РН–34 приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;</p> <p>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 та/або кібербезпеки;</p> |

| Фахові компетентності | Результати навчання |
|--|---|
| | <p>RH-41 забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;</p> <p>RH-42 впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;</p> <p>RH-43 застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;</p> <p>RH-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;</p> <p>RH-45 застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;</p> <p>RH-46 здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;</p> <p>RH-48 виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;</p> <p>RH-49 забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;</p> <p>RH-50 забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);</p> <p>RH-51 підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;</p> <p>RH-52 використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;</p> <p>RH-53 вирішувати задачі аналізу програмного коду на наявність можливих загроз.</p> |
| <p>КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.</p> | <p>RH-14 вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;</p> <p>RH-20 забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;</p> <p>RH-31 застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;</p> <p>RH-36 виявляти небезпечні сигнали технічних засобів;</p> <p>RH-37 вимірювати параметри небезпечних та заводових сигналів під час інструментального контролю процесів</p> |

| Фахові компетентності | Результати навчання |
|-----------------------|---|
| | <p>захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;</p> <p>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;</p> <p>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;</p> <p>РН–40 інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;</p> <p>РН–47 вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;</p> <p>РН–48 виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;</p> |

Програма навчальної дисципліни

Тема 1. Основні поняття і визначення. Сучасні інформаційні мережі. Локальні і глобальні інформаційні мережі. Глобальна мережа Internet. Розміщення даних в мережах. Проблеми управління даними в інформаційних мережах.

Тема 2. Мережеві архітектури. Модель OSI відкритих систем. Алгоритмічне забезпечення мереж. Протоколи передачі даних в мережах. Коротка характеристика протоколів. Мережеві рівні і модель OSI. Стек протоколів TCP / IP. Стандарти TCP / IP. Структура стека TCP / IP.

Тема 3. Структури даних в мережах. Документи і служби. Гіпертекстову документ. Web-сайт. Web-портал. Мережеві технології баз даних.

Тема 4. Основні завдання мережевого програмування. Технологія і моделі "клієнт-сервер". Завдання програмування на рівні клієнта. Завдання програмування на рівні сервера.

Тема 5. Мови мережевого програмування. Мова HTML. Мова JavaScript. Мова і технологія Java.

Тема 6. Технологія SYBASE мережевого програмування. Організація доступу до серверів баз даних. Сервери додатків. Підтримка компонентних моделей. Підтримка Web-серверів.

Тема 7. Мережеве програмування на стороні клієнта. Проектування і програмування Web-сторінок. Програмування доступу до баз даних.

Тема 8. Мережеве програмування в триланкової технології "клієнт-сервер". Проектування і програмування Web-сайту. Програмування доступу до серверів баз даних. Застосування композитних моделей в мережевому програмуванні.

Тема 9. Спеціальні програмні рішення в мережах. Програмування служб електронної пошти. Програмування служб доступу до файлів.

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 проекти, майстер-класи. Під час проведення лекцій застосовуються такі методи навчання як лекції (теми 1 – 9) та бесіди (теми 1, 3, 9).

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 різні 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 цей 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 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. Мінімумально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімумально 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

| 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 | незадовільно | не зараховано |
| 35 – 59 | FX | | |

Рейтинг-план навчальної дисципліни

| Тема | Форми та види навчання | | Форми оцінювання | Мак бал |
|--------|---|---|--------------------------------|---------|
| Тема 1 | Аудиторна робота | | | |
| | Лекція | Тема 1. Основні поняття і визначення. Сучасні інформаційні мережі. Локальні і глобальні інформаційні мережі. Глобальна мережа Internet. Розміщення даних в мережах. Проблеми управління даними в інформаційних мережах. | 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. Мережеві архітектури. Модель OSI відкритих систем. Алгоритмічне забезпечення мереж. Протоколи передачі даних в мережах. Коротка характеристика протоколів. Мережеві рівні і модель OSI. Стек протоколів TCP / IP. Стандарти TCP / IP. Структура стека TCP / IP. | Робота на лекції | 1 |
| | Лабораторне заняття | Лабораторна робота № 1 "Інтерфейси прикладного програмування WinSock і сокети UNIX, основні функції мережевого взаємодії, певні в стандарті POSIX " | 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 3 | Аудиторна робота | | | |
| | Лекція | Тема 3. Структури даних в мережах. Документи і служби. Гіпертекстову документ. Web - сайт. Web - портал. Мережеві технології баз даних. | 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 4 | Аудиторна робота | | | |
| | Лекція | Тема 4. Основні завдання мережевого програмування. Технологія і моделі "клієнт-сервер". Завдання програмування на рівні клієнта. Завдання програмування на рівні сервера. | Робота на лекції | 1 |
| | Лабораторне заняття | Лабораторна робота № 2. "Моделі мережевого вводу-виводу " | виконання лабораторної роботи | 4 |
| | | | 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 5 | Аудиторна робота | | | |
| | Лекція | Тема 5. Мови мережевого програмування. Мова HTML. Мова JavaScript. Мова і технологія Java. | 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 6 | Аудиторна робота | | | |
| | Лекція | Тема 6. Технологія SYBASE мережевого програмування. Організація доступу до серверів баз даних. Сервери додатків. Підтримка компонентних моделей. Підтримка Web - серверів. | Робота на лекції | 1 |
| | Лабораторне заняття | Лабораторна робота № 3. | виконання | 4 |

| | | | | |
|---------------|---|--|-------------------------------|---|
| | | "Багатоадресне і широкомовленне разилка" | лабораторної роботи | |
| | | 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 7 | | Аудиторна робота | | |
| | Лекція | Тема 7. Мережеве програмування на стороні клієнта. Проектування і програмування Web - сторінок. | 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 7 | | Аудиторна робота | | |
| | Лекція | Тема 7. Програмування доступу до баз даних. | Робота на лекції | 1 |
| | Лабораторне заняття | Лабораторна робота № 4. "Багатопотокові мережеві додатки". | 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 8 | | Аудиторна робота | | |
| | Лекція | Тема 8. Мережеве програмування в триланкової технології "клієнт-сервер". Проектування і програмування Web - сайту. | 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 | | |
| | | Аудиторна робота | | |
| Тема 8 | Лекція | Тема 8. Програмування доступу до серверів баз даних. Застосування композитних моделей в | Робота на лекції | 1 |

| | | | | |
|---------------|---|--|-------------------------------|----|
| | | мережевому програмуванні. | | |
| | Лабораторне заняття | <i>Лабораторна робота № 5. "Мережеве програмування з сокетами і каналами"</i> | виконання лабораторної роботи | 4 |
| | <i>Самостійна робота</i> | | | |
| | 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 9 | Лекція | <i>Тема 9. Спеціальні програмні рішення в мережах. Програмування служб електронної пошти.</i> | Робота на лекції | 1 |
| | <i>Самостійна робота</i> | | | |
| | 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 9 | Лекція | <i>Тема 9. Спеціальні програмні рішення в мережах. Програмування служб електронної пошти.</i> | Робота на лекції | 1 |
| | Лабораторне заняття | <i>Лабораторна робота № 5. "Віддалений виклик методу (RMI)".</i> | виконання лабораторної роботи | 4 |
| | | | Контрольна робота 2 | 12 |
| | <i>Самостійна робота</i> | | | |
| | 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. Кровчик Э. .Net сетевое программирование для профессионалов / Э. Кровчик, В. Кумар, Н. Лагари, А. Мунгале, К. Нагель, Т. Паркер, Ш. Шивакумар. - М.: Лори, 2005. – 400 с.
2. Кровчик Э. .Net сетевое программирование / Э. Кровчик, В.Кумар, Н. Лагари, А. Мунгале, К. Нагель, Т. Паркер, Ш. Шивакумар. - М.: Лори, 2007. – 420 с.
3. Cisco Systems, Inc. Руководство по технологиям объединенных сетей, 4-е издание / Cisco Systems, Inc - М.: Вильямс, 2005. - 1040с.
4. Шиндер, Д.Л. Основы компьютерных сетей / Д.Л. Шиндер. - М.: Вильямс, 2002. - 615с.

Додаткова

5. Магда, Ю.С. Программирование последовательных интерфейсов / Ю.С. Магда. - С-Пб.: БХВ-Петербург, 2009. - 304с.
6. Фейт, С. TCP/IP Архитектура, протоколы, реализация / С. Фейт. - М.: Лори, 2000. - 424с.
7. Джонс, Э. Программирование в сетях Microsoft Windows / Э. Джонс, Д. Оланд. - С-Пб.: Питер, 2002. - 594с.
8. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер. - С-Пб.: Питер, 2001. - 668с.
9. Найк, Д. Стандарты и протоколы Интернета / Д. Найк. - М.: Русская Редакция, 1999. - 384с.

Інформаційні ресурси.

10. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Розробка та аналіз алгоритмів" <https://pns.hneu.edu.ua/course/view.php?id=7452>.