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

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

ОСНОВИ ПЛАНУВАННЯ ТА АДМІНІСТРУВАННЯ СЛУЖБ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ

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:
Алексієв В. О., д.т.н., проф. кафедри кібербезпеки та інформаційних технологій.

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

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

Анотація навчальної дисципліни

Сучасні підприємства й організації різної форми власності та за розміром мають розвинені інформаційні ресурси, що надають користувачам (клієнтам, співробітникам, ін.) необхідний рівень знань щодо продукції, технологічних особливостей виробництва, послуг, що надаються, тощо. Існуючі інформаційно-комунікаційні технології дозволяють у найкоротший строк розгорнути відповідні служби доступу до інформаційних ресурсів. Технологічною базою таких служб є система керування вмістом (Content Management System, CMS). Тому, з точки зору конкурентоспроможності, для будь-якого підприємства чи організації зараз є актуальними задачі планування та адміністрування служб доступу до інформаційних ресурсів.

Метою викладання дисципліни є формування теоретичних знань з основ планування та адміністрування служб доступу до інформаційних ресурсів, до яких у більшості відносяться сучасні системи керування вмістом, за допомогою яких реалізовуються веб-ресурси та сервіси, а також формування практичних навичок із побудови та адміністрування відповідних серверних систем.

Результатами вивчення даної дисципліни є придбання навичок з проектування та створення інформаційного ресурсу для малого підприємства, а також комплексних практичних навичок щодо планування, адміністрування та забезпечення безпеки служб доступу до інформаційних ресурсів.

Характеристика навчальної дисципліни

Курс	**4**
Семестр	**7**
Кількість кредитів ECTS	**4**
Форма підсумкового контролю	залік

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Основи побудови та захисту сучасних операційних систем	Адміністрування Unix-подібних
Комплексні системи захисту інформації	Мережне програмування
Безпека в інформаційно-комунікаційних системах	Дипломне проектування

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; РН–18. використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;

Фахові компетентності	Результати навчання
	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;

Фахові компетентності	Результати навчання
	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;

Фахові компетентності	Результати навчання
	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;

Фахові компетентності	Результати навчання
	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. Загальні відомості з організації та планування служб доступу до інформаційних ресурсів

Тема 1. *Особливості сучасних CMS (Content Management System).*
Тема 2. *Настроювання веб-серверу на базі операційної системи Linux.*
Тема 3. *Засоби LDAP у рішенні завдань доступу до інформаційних ресурсів.*
Тема 4. *Налагодження WordPress. Плагіни, технологія мультисайт.*
Тема 5. *Особливості та можливості WordPress API.*
Тема 6. *Кібербезпека служб доступу до інформаційних ресурсів.*

Змістовий модуль 2. Адміністрування служб доступу до інформаційних ресурсів

Тема 7. *Налагодження доступу до інформаційних ресурсів на прикладі WordPress.*
Тема 8. *Програмування завдань із застосування API інформаційних ресурсів.*
Тема 9. *Особливості серверних рішень для забезпечення служб доступу до інформаційних ресурсів.*
Тема 10. *Перспективи розвитку служб доступу до інформаційних ресурсів.*

Перелік практичних (семінарських) / 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 (теми 1 – 10), бесіди (теми 1, 6, 10).

Порядок оцінювання результатів навчання

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 – 100 балів; мінімальна сума, що дозволяє студенту поставити залік – 60 балів);

2) підсумковий/семестровий контроль, що проводиться у формі накопичувальної оцінки за семестр.

Порядок здійснення поточного оцінювання знань студентів.

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

– аналізувати та декомпозувати служб доступу до інформаційних ресурсів;

– вміти розгорнути веб-сервер, що містить засоби організації доступу до інформаційних ресурсів підприємства чи організації;

– використовувати в професійній діяльності методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;

– вирішувати задачі адміністрування служб доступу до інформаційних ресурсів;

– проводити захист та підтримку функціонування інформаційних ресурсів на основі практик, навичок та знань, щодо залучення кращих практик та моделей захисту електронних інформаційних ресурсів;

– проводити заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів;

– оцінювати можливості масштабування служб доступу до інформаційних ресурсів;

– вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі підтримки надійних інформаційних потоків та стабільної роботи серверних систем.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі заліку на основі накопичувальної системи балів.

Лекційні заняття: максимальна кількість балів становить 30 (робота на лекціях – 10, експрес-опитування – 20), а мінімальна – 15.

Лабораторні заняття: максимальна кількість балів становить 70 (захист лабораторних робіт – 60, контрольні роботи – 10), а мінімальна – 45.

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

Результат заліку оцінюється в балах (максимальна кількість – 100 балів, мінімальна кількість, що зараховується – 60 балів) і проставляється у відповідній графі залікової "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 – 60.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час аудиторних занять, 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		
35 – 59	FX	незадовільно	не зараховано

Рейтинг-план навчальної дисципліни

Тема	Форми та види навчання		Форми оцінювання	Max бал
Тема 1	***Аудиторна робота***			
	Лекція	Проблемна лекція *"Особливості сучасних CMS (Content Management System)"*	Робота на лекції	1
Тема 2.	***Аудиторна робота***			
	Лекція	Лекція *"Настроювання веб-серверу на базі операційної системи Linux"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №1 *"Вивчення мережевих засобів доступу до інформаційних систем"*		
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт.		
Тема 3	***Аудиторна робота***			
	Лекція	Лекція *"Засоби LDAP у рішенні завдань доступу до інформаційних ресурсів"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №2 *"Розгортання віртуальної машини на базі Linux"*	Захист лабораторних робіт № 1, 2	10
	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	Лекція *"Налагодження WordPress. Плагіни, технологія мультисайт"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №3 *"Розгортання веб-серверу та засобів управління базами даних"*	Захист лабораторної роботи № 3	10
	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 5	***Аудиторна робота***			
	Лекція	Лекція *"Особливості та можливості WordPress API"*	Робота на лекції	1
			Експрес-	10

			опитування	
	Лабораторне заняття	Лабораторна робота №4. *"Packet Tracer. Навігація по IOS"*	Захист лабораторної роботи № 4	10
			Контрольна робота 1	5
Тема 6	***Аудиторна робота***			
	Лекція	Лекція"Кібербезпека служб доступу до інформаційних ресурсів"	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №5. *"Розгортання WordPress"*		
	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	Лекція *" Налагодження доступу до інформаційних ресурсів на прикладі WordPress "*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №6. *"Застосування засобів LDAP"*		
	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 8	***Аудиторна робота***			
	Лекція	Лекція *" Програмування завдань із застосування API інформаційних ресурсів "*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №7. "Взаємодія та обмін інформацією у системі на базі Wordpress".	Захист лабораторних робіт № 5, 6, 7	20
	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 9	***Аудиторна робота***			
	Лекція	Лекція *" Особливості серверних рішень для забезпечення служб доступу до інформаційних ресурсів."*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №8. "Програмування доступу до API"		
	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 10	***Аудиторна робота***			
	Лекція	Лекція *"Перспективи розвитку служб доступу до інформаційних ресурсів"*	Робота на лекції	1
			Експрес-опитування	10
	Лабораторне заняття	Лабораторна робота №9. "Засоби безпеки сайту на базі WordPress".	Захист лабораторної роботи № 8, 9	10
			Контрольна робота 2	5
	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		

Рекомендована література

Основна

1. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ-2000», 2020 . – 678 с.

2. Алексієв В. О. Застосування GRID-технології у транспортному ВНЗ: навч.-метод. посіб. / В. О. Алексієв.– Х. : ХНАДУ, 2008. – 208 с.

3. Microservices vs. Service-Oriented Architecture. Mark Richards. / O'Reilly Media. All., 2016., 57 p. [Electronic resource]. –Access mode: https://www.oreilly.com/radar/microservices-vs-service-oriented-architecture/

4. Unix и Linux. Руководство системного администратора / [Э. Немет, Г. Снайдер, Т. Хейн и др.] – М. : ИД "Вильямс", 2012. – 1312 с.

5. Уильямс Б., Дэмстра Д., Стэрн Х. WordPress для профессионалов. – СПб.: Питер, 2014. – 464 с.

Додаткова

6. Как установить Linux, Apache, MySQL, PHP (LAMP) в Ubuntu 18.04 [Электронный ресурс] / Mark Drake. DigitalOcean, 2018. – Режим доступа : https://www.digitalocean.com/community/tutorials/linux-apache-mysql-php-lamp-ubuntu-18-04-ru.

7. Куалман Э. Безопасная сеть. Правила сохранения репутации в эпоху социальных медиа и тотальной публичности. – М. : Альпина Паблишер, 2018. – 214 с.

Інформаційні ресурси.

8. WordPress Security Fundamentals [Электронный ресурс] / Wordfence. Defiant. – Режим доступа : https://www.wordfence.com/learn/.