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

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

Безпека в DevOps

робоча програма навчальної дисципліни

Галузь знань	**12 "ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ"**
Спеціальність	**125 "КІБЕРБЕЗПЕКА"**
Освітній рівень	**перший (бакалаврський)**
Освітня програма	**"КІБЕРБЕЗПЕКА / CYBERSECURITY"**

Вид 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.,
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

DevOps (Development and Operations) – методологія розробки програмного забезпечення, яка спрямована на покращення взаємодії розробників із фахівцями інформаційно-технологічного обслуговування (системних адміністраторів) та поєднання їх робочих процесів. DevOps застосовує у комплексі кращі практики гнучкого управління розробкою (Agile), засоби неперервної інтеграції (CI, Continuous Integration) програмного забезпечення, поруч із забезпеченням безперервної доставки (CD, Continuous Delivery) відповідних сервісів та застосунків користувачам. У свою чергу, для забезпечення кібербезпеки процесів розробки, розгортання та підтримки програмного продукту слід ретельно дотримуватися процесів забезпечення безпеки на протязі всього життєвого циклу програмного продукту (Security Development Lifecycle). Тому, зараз актуальною стає покращена методологія DevSecOps, що впроваджує практики забезпечення безпеки (Security) у обсязі неперервного циклу процесів DevOps.

Дисципліна «Безпека в DevOps» присвячена вивченню методології DevSecOps на практичних прикладах та спрямовує навчання студентів на розуміння й застосування кращих підходів до забезпечення безпеки життєвого циклу програмного продукту (у більшості розглядаються веб-застосунки та ресурси хмарних обчислень).

Мета навчальної дисципліни: формування системи теоретичних знань і набуття практичних умінь і навичок щодо забезпечення безпеки на протязі життєвого циклу існування веб-рішень, що виконуються на боці серверу. Оволодіння навичками застосування сучасного програмного забезпечення щодо рішень завдань DevSecOps і набуття компетенцій з використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

Характеристика навчальної дисципліни

Курс	**4**
Семестр	**7(1)**
Кількість кредитів ECTS	**5**
Форма підсумкового контролю	**Екзамен**

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Безпека в інформаційно-комунікаційних системах	Дипломна робота
Інформаційні системи та інтернет технології	Основи розробки децентралізованих застосувань (Decentralized Applications (DAPPS))
Технології програмування	Безпека банківських систем

Компетентності та результати навчання за дисципліною:

Компетентності	Результати навчання
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	РН–9. впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН–13. аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН–14. вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;

	РН–17. забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН–18. використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН–19. застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН–20 забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН–21. вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН–22. вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН–23. реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН–24. вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН–25. забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН–26. впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН–27. вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН–28. аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН–29. здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН–32. вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН–34. приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН–35. вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;

	РН–42. впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН–43. застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН–44. вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН–45. застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН–46. здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН–47. вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН–48. виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН–49. забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН–50. забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН–51. підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН–52. використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; РН–53. вирішувати задачі аналізу програмного коду на наявність можливих загроз.
КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.	РН–9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН–13 аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН–14 вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН–17 забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН–19 застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН–23 реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН–25 забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН–29 здійснювати оцінювання можливості реалізації потенційних

	загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН–32 вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН–33 вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН–34 приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН–35 вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН–41 забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН–42 впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН–43 застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН–44 вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН–45 застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН–46 здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН–48 виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН–49 забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН–50 забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН–51 підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН–52 використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; РН–53 вирішувати задачі аналізу програмного коду на наявність можливих загроз.
КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.	РН–14 вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН–20 забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН–31застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН–36 виявляти небезпечні сигнали технічних засобів; РН–37 вимірювати параметри небезпечних та завадових сигналів під

	час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН–38 інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН–39 проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; РН–40 інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; РН–47 вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН–48 виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;

Програма навчальної дисципліни

Змістовий модуль 1. Основи застосування методології DevOps.

Основні терміни та визначення. Побудова робочих процесів. Особливості застосування програмного забезпечення для виконання завдань CI/CD. Місце завдань забезпечення кібербезпеки у процесах DevOps.

Тема 1. Особливості сучасних мов програмування та розробки веб-орієнтованих застосунків.

Особливості розробки веб-застосунків. Налагодження середовища розробки. Відмінності платформ Windows, Linux та MacOS у якості середовища розробника. Поняття гнучкого (Agile) управління розробкою програмних продуктів.

Тема 2. Розгортання операційної системи Linux та Windows у якості платформи веб-сервера.

Застосування скриптів для автоматизації процесів розгортання програмного забезпечення. Знайомство з технологіями Chef, Puppet та Ansible. Особливості забезпечення безпеки рівня операційної системи та веб-серверу.

Тема 3. Особливості технологій серверної віртуалізації.

Визначення гіпервізору та контейнерної віртуалізації. Особливості роботи із системами управління віртуальними машинами. Особливості забезпечення безпеки рівня віртуальної машини.

Тема 4. Технології хмарних обчислень (Cloud Computing).

Засоби автоматизації DevOps у хмарних середовищах на прикладах: Amazon AWS, Microsoft Azure та рішень Red Hat OpenShift. Особливості забезпечення безпеки рівня хмарного середовища.

Тема 5. Основи застосування системи контролю версій Git.

Особливості застосування систем контролю версій. Огляд технологій: GitHub, Bitbucket та GitLab. Місце Git у процесах DevSecOps.

Змістовий модуль 2. Рішення комплексу завдань DevSecOps.

Застосування рішень забезпечення безпеки на протязі всього життєвого циклу веб-застосунку та/або сервісу. Особливості забезпечення безпеки на рівні управління розробкою програмного продукту.

Тема 6. Особливості застосування інструменту для безперервної інтеграції Jenkins.

Основи розгортання системи CI/CD. Аналоги, як сервіси хмарних обчислень. Розроблення сучасного веб-застосунку у разі залучення технології CI/CD. Значність забезпечення безпеки рівня систем CI/CD.

Тема 7. Основи технологій захисту веб-орієнтованих систем.

Особливості захисту програмних рішень. Технології Kali-Linux в завданнях тестування на вразливість, як на рівні операційної системи, так й хмарного середовища.

Тема 8. Основи розробки сучасних веб-застосувань у сенсі залучення засобів DevSecOps.

Основи розробки SPA (Single-Page Application); застосування архітектури REST (Representational State Transfer); втілення концепції мікросервісів у сенсі залучення засобів DevSecOps. Перспективи розвитку веб-технологій та рішення завдань побудови архітектури веб-орієнтованих систем у разі неперервного циклу залучення методики DevSecOps.

Методи навчання та викладання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються проблемні лекції, презентації, бесіди, індивідуальні та групові проєкти, майстер-класи.

Порядок оцінювання результатів навчання

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:

– знати особливості сучасних мов програмування та розробки веб-орієнтованих застосунків;

– вміти розгортати операційні системи Linux та Windows у якості платформи веб-сервера;

– орієнтуватися у виборі технологій серверної віртуалізації;

– володіти навичками застосування технологій хмарних обчислень (Cloud Computing).

– застосовувати на практиці системи контролю версій Git.

– розуміти особливості застосування інструменту для безперервної інтеграції Jenkins;

– проектувати базовий контур захисту веб-орієнтованих систем.

– вміти надати прогноз щодо перспектив розвитку систем розробки сучасних веб-застосувань у сенсі залучення засобів DevSecOps.

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.

Практичні (семінарські, лабораторні) заняття: максимальна кількість балів становить 40, а мінімальна – 25.

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

Підсумковий контроль: проводиться з урахуванням іспиту.

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

Кожен екзаменаційний білет складається із 3 практичних ситуацій (одне стереотипне, одне діагностичне та одне евристичне завдання), які передбачають вирішення типових професійних завдань фахівця на робочому місці та дозволяють діагностувати рівень теоретичної підготовки студента і рівень його компетентності з навчальної дисципліни.

Оцінювання кожного завдання екзаменаційного білету наступне: перше завдання – це 20 тестових завдань закритої форми, виконання його оцінюється 20 балами; друге завдання – присвячене розробленню структурної схеми побудови CI/CD процесів, виконання його оцінюється 10 балами; третє завдання – рішення евристичного завдання щодо планування розгортання контуру безпеки рівня DevOps сервісу, 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

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 мов програмування та розробки веб-орієнтованих застосунків."*	Робота на лекції	0,5
Тема 2.	***Аудиторна робота***			
	Лекція	Лекція *" Розгортання операційної системи Linux та Windows у якості платформи веб-сервера."*	Робота на лекції	0,5
	Лабораторне заняття	Лабораторна робота №1 *"Розгортання веб-серверу у середовищі віртуальної машини (налагодження середовища віртуалізації, налагодження веб-серверу та безпеки. Робота з системами автоматизації розгортання). "*	Робота на лабораторній роботі	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	Контрольна робота	5
Тема 3	***Аудиторна робота***			
	Лекція	Лекція *" Особливості технологій серверної віртуалізації."*	Робота на лекції	0,5
	Лабораторне заняття	Лабораторна робота №2 *" Розгортання та знайомство з GitLab (розробка он-лайн системи контролю версій та огляд технологій CI/CD). "*	Робота на лабораторній роботі	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	Захист лабораторної роботи № 1	10
Тема 4	***Аудиторна робота***			
	Лекція	Лекція *" Технології хмарних*	Робота на	0,5

		обчислень (Cloud Computing)."	лекції	
	Лабораторне заняття	Лабораторна робота №3 *" Створення веб-сайту у середовищі хмарних обчислень (знайомство із засобами безпеки рівня Cloud Computing)."*	Робота на лабораторній роботі	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	Захист лабораторної роботи № 2	10

Тема 5	***Аудиторна робота***			
	Лекція	Лекція *" Основи застосування системи контролю версій Git."*	Робота на лекції	0,5
	Лабораторне заняття	Лабораторна робота №4. *" Основи розробки веб-застосунку з залученням технологій DevSecOps (проектування та побудова у середовищі віртуальних машин рішення щодо забезпечення завдань DevSecOps). "*	Робота на лабораторній роботі	1,5
			Захист лабораторної роботи № 3	10
Тема 6	***Аудиторна робота***			
	Лекція	Лекція*" Особливості застосування інструменту для безперервної інтеграції Jenkins."*		1
	Лабораторне заняття	Лабораторна робота №4. *" Основи розробки веб-застосунку з залученням технологій DevSecOps (проектування та побудова у середовищі віртуальних машин рішення щодо забезпечення завдань DevSecOps)."*	Захист лабораторної роботи № 4	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. Підготовка до екзамену		
Тема 7	***Аудиторна робота***			
	Лекція	Лекція *" Основи технологій захисту веб-орієнтованих систем."*	Контрольна робота	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. Підготовка до екзамену		
Тема 8	***Аудиторна робота***			
	Лекція	Лекція *" Основи розробки сучасних веб-застосувань у сенсі залучення засобів DevSecOps."*		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		
Екзамен				40

Рекомендована література

Основна

1. Ушакова, І. О. Проектування інформаційних систем : практикум / Ушакова І.О. – Х. : ХНЕУ ім. С. Кузнеця, 2015. – 234 с.

2. Алешин Г.В. Информационные технологии и защита информации в информационно-коммуникационных системах : монография / Алешин Г.В., Белецкий А.Я., Биккузин К.В. и др. [под ред. В.С. Пономаренко]. – Х. : [Щедра садиба плюс], 2015. – 485 с.

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

4. Вехен Джульен. Безопасный DevOps. Эффективная эксплуатация систем. - СПб.: Питер, 2020. - 432 с.

5. Дэвис Дженнифер, Дэниелс Кэтрин. Философия DevOps. Искусство управления IT. - СПб.: Питер, 2017. - 416 с.

6. Вольф Эберхард. Continuous delivery. Практика непрерывных апдейтов. - СПб.: Питер, 2018. - 320 с.

7. Стеллман Эндрю. Постигая Agile. Ценности, принципы, методологии / Эндрю Стеллман, Дженни-фер Грин ; пер. сангл. С.Пасерба. - М.: Манн, Иванов и Фербер, 2017.— 448 с.

8. Ньюмен С. Создание микросервисов/ С.Ньюмен.–СПб.: Питер, 2016. – 304 с.

9. Таллоч Митч и команда Windows Azure. Знакомство с Windows Azure. Для ИТ-специалистов/ Таллоч М.; пер. с англ. – М.: ЭКОМ Паблишерз, 2014. — 154 с.

10. Риз Дж. Облачные вычисления: пер. с англ.- СПб.: БХВ-Петербург, 2011.- 288 с.

11. DevOps Revealed 3rd edition. International DevOps Certification Academy.- 94 p. [Electronic resource]. –Access mode https://www.devops-certification.org/

Додаткова та інформаційні ресурси

12. Страх и ненависть DevSecOps [Электронный ресурс] / Habr, 2019. – Режим доступа : https://habr.com/en/company/oleg-bunin/blog/448488/.

13. Настройка среды непрерывного развертывания с помощью Jenkins [Электронный ресурс] / На Лв, Чжао Чжо, Янь Чжэ, Чэнь Сяо Лун. IBM developerWorks, 2015. – Режим доступа : https://www.ibm.com/ developerworks/ru/library/d-continuous-delivery-framework-jenkins/.

14. Микрослужбы в действии: Введение в микрослужбы [Электронный ресурс] / Рик И. Осовский. IBM developerWorks, 2015. – Режим доступа : https://www.ibm.com/developerworks/ru/library/cl-bluemix-microservices-in-action-part-1-trs.

15. Распределенные базы и хранилища даннях : Электронный учебник / Н. Аносова, О. Бородин, Е. Гаврилов и др. – НОУ "ИНТУИТ" [Электронный ресурс]. – Режим доступа : http://www.intuit.ru/ studies/ courses/1145/214/info.

16. Разработка безопасных облачных приложений [Электронный ресурс] / Роби Сен. IBM developerWorks, 2016. – Режим доступа : http://www.ibm.com/ developerworks/ru/library/cl-develop-secure-cloud-aware-applications/index.html.

17. Облачные стандарты: средства взаимодействия приложений в облаке [Электронный ресурс] / Кэйн Скарлетт. IBM developerWorks, 2016. – Режим доступа : http://www.ibm.com/ developerworks/ ru/library /cl-tools-to-ensure-cloud-application-interoperability/index.html.

18. Create REST applications with the Slim micro-framework [Electronic resource] / Vikram Vaswani. IBM developerWorks, 2012. – Access mode : http://www.ibm.com/developerworks/library/x-slim-rest/.

19. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною «Безпека в DevOps» [Електронний ресурс] – Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=7015.