



Силабус освітнього компонента

Програма навчальної дисципліни



Розробка веб-додатків

Шифр та назва спеціальності

125 – Кібербезпека та захист інформації

Інститут

ННІ комп'ютерних наук та інформаційних технологій

Освітня програма

Кібербезпека

Кафедра

Кібербезпеки (328)

Рівень освіти

Бакалаврї

Тип дисципліни

Спеціальна (фахова), Обов'язкова

Семестр

6

Мова викладання

Українська

Викладачі, розробники



ТКАЧОВ Андрій Михайлович

andrii.tkachov@khpi.edu.ua

Кандидат технічних наук, старший науковий співробітник кафедри кібербезпеки НТУ "ХПІ".

Кількість наукових публікацій: більше 60 публікацій, 25 статей у закордонних виданнях та фахових виданнях України, 6 патентів на корисну модель, гарант освітньо-професійної програми першого (бакалаврського) рівня вищої освіти. Провідний лектор з дисциплін: «Мережне програмування», «Розробка та аналіз алгоритмів», «Технології програмування», «Інструментальні засоби програмування», «Веб безпека», «Основи технічного захисту інформації».

[Детальніше про викладача на сайті кафедри](#)

Загальна інформація

Анотація

Навчальна дисципліна "Розробка веб-додатків" є вибірковою навчальною дисципліною. Вивчення дисципліни спрямовано на засвоєння студентами знань щодо сучасних підходів до побудови клієнт-серверних Web-додатків, основних понять забезпечення безпеки функціонування Web-додатків у відкритій мережі Інтернет, а також практичній підготовці студентів в розробці таких додатків.

Мета та цілі дисципліни

Формування у студентів системи теоретичних знань і набуття практичних умінь і навичок щодо розробки та проектування веб-додатків.

Формат занять

Лекції, лабораторні роботи, самостійна робота, курсовий проект, консультації. Підсумковий контроль – іспит.

Компетентності

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

Результати навчання

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 та/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-31 застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;

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-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-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-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.

Обсяг дисципліни

Загальний обсяг дисципліни 180 год. (6 кредитів ECTS): лекції – 36 год., лабораторні роботи – 36 год., самостійна робота – 108 год.

Передумови вивчення дисципліни (пререквізити)

Інструментальні засоби програмування, Технології програмування, Основи програмування.

Особливості дисципліни, методи та технології навчання

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 презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Основи проєктування та розробка веб-додатків.

Предмет і об'єкт курсу. Склад та призначення програмного забезпечення. Архітектура програмних систем. Інструментальні засоби веб-розробки. Інтегровані середовища розробки. Клієнт/серверна архітектура веб-додатку. Огляд технологій. Веб стандарти.

Тема 2. Мова гіпертекстової розмітки веб-сторінок.

Сутність гіпертексту. Розвиток стандартів HTML. Рівні HTML. Поняття мови HTML. Структура HTML-документу. Структура HTML-коду. Об'єкти мови. Основні теги та їх використання. Створення Web-сайту за шаблоном. Типи шаблонів сайту. HTML-шаблони. Поняття верстки. Структури веб-сайтів. Робота з фреймами.

Тема 3. Використання каскадних таблиць стилів.

Поняття каскадних таблиць стилів. Історія версій CSS. Відносини між множинними вкладеними елементами. Створення CSS стилів. Зв'язок HTML і CSS. Правила написання CSS. Каскадність CSS.

Тема 4. Технології проєктування та розробки веб-додатків.

Введення в JavaScript: основні поняття і визначення. Методи підключення JavaScript до HTML документів. Спільна робота сценаріїв та HTML. Особливості взаємодії з браузерами. Особливості урахування типу браузера. Операції та керує структури. Технології розробки веб-орієнтованих інформаційних систем. Веб-сервери в інформаційних системах та їх налаштування.

Тема 5. Системи управління базами даних та їх використання при проєктуванні та розробці веб-додатків.

Принцип роботи бази даних. Організація взаємодії з базами даних. Процедури ідентифікації користувача.

Тема 6. Супровід веб-додатків.

Створення веб-орієнтованих систем. Захист інформації.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Основи проєктування та розробка веб-додатків.

Тема 2. Мова гіпертекстової розмітки веб-сторінок.

Тема 3. Використання каскадних таблиць стилів.

Тема 4. Технології проєктування та розробки веб-додатків.

Тема 5. Системи управління базами даних та їх використання при проєктуванні та розробці веб-додатків.

Тема 6. Супровід веб-додатків.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (<http://surl.li/pxssv>), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.

Зокрема, окремі теми даної компоненти можуть бути враховано у разі успішного завершення таких курсів CISCO:

Java 1

<https://www.netacad.com/catalogs/learn?category=course>.

Література та навчальні матеріали

Основна література

1. Вивчення веб-розробки [Електронний ресурс]. – Режим доступу:

<https://developer.mozilla.org/ru/docs/Learn>.

2. КІБЕРБЕЗПЕКА: WEB-технології [Електронний ресурс]: Навчально-довідковий посібник / С.П. Євсєєв, А.М. Ткачов, В.О. Алексієв, Ю.М. Рябуха – Харків : ХНЕУ ім. С. Кузнеця, – Львів: Видавництво «Новий Світ – 2000», 2021. – 390 с. (укр. мов.).

<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBG006AnvjQHU1SdBl3xCaUju>

3. MySQL Tutorial [Електронний ресурс]. – Режим доступу:

<https://www.tutorialspoint.com/mysql/index.htm>.

4. Java EE Tutorials [Електронний ресурс]. – Режим доступу:

<https://www.oracle.com/java/technologies/jee-tutorials.html>.

Додаткова література

1. Tutorials Library [Електронний ресурс]. – Режим доступу:

<https://www.tutorialspoint.com/index.htm>.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:

- лабораторні роботи: 30% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- контрольна робота: 10% семестрової оцінки;
- курсовий проект: 20% семестрової оцінки;
- іспит: 30% семестрової оцінки

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Студент повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту. Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: <http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/>

Погодження

Силабус погоджено

28.08.2024

Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2024

Гарант ОП
Сергій ЄВСЕЄВ