Силабус освітнього компонента
Програма навчальної дисципліни

Розробка веб-додатків

Шифр та назва спеціальності
257 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Управління інформаційною безпекою

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

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

КЗ–4. Здатність спілкуватися державною мовою як усно, так і письмово.
КЗ–6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
КЗ–7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
ФК-2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
ФК-3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
ФК-4. Здатність прогнозувати реалізації управлінських рішень щодо захисту інформації.
ФК-7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
ФК-8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.

Результати навчання

ПРН-3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.
ПРН-4. Вільно спілкуватися державною мовою.
ПРН-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки
ПРН-7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
ПРН-8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.
ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
ПРН-11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.
ПРН-12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН-13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.
ПРН-16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
ПРН-17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
ПРН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

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 JavaSript: основні поняття і визначення. Методи підключення JavaSript до HTML документів. Спільна робота сценаріїв та HTML. Особливості взаємодії з браузерами. Особливості урахування типу браузера. Операції та керуючи 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 проектуванні 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 проектуванні 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. Євсеєв, 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-GBGO06AnvjQHU1SdBl3xCaUju
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 Роман КОРОЛЬОВ