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

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

ВЕБ-ТЕХНОЛОГІЇ ТА ВЕБ-ДИЗАЙН

робоча програма для студентів

Галузь знань	***12 Інформаційні технології***
Спеціальність	***121 Інженерія програмного забезпечення,*** ***122 Комп`ютерні науки***
Освітній рівень	***перший (бакалаврський)***
Освітня програма	***Інженерія програмного забезпечення,*** ***Комп`ютерні науки***

Вид дисципліни	***базова***
Мова викладання, навчання та оцінювання	***українська***

Завідувач кафедри
кібербезпеки та
інформаційних технологій _____ *Сергій ЄВСЕЄВ*

Харків
2020

ЗАТВЕРДЖЕНО
на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 2 від 31.08.2020 р.

Розробник:
Ткачов А.М., к.т.н., с.н.с., доцент кафедри КІТ.

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

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

Анотація навчальної дисципліни

Веб-простір зараз виконує функції платформи для просування товарів та послуг, поруч із забезпеченням й наданням інформаційного та розважального контенту для користувачів. Новітні технології та тенденції дизайну для розробки веб-ресурсів та веб-сервісів є основою для вивчення курсу. Застосування стандартів HTML5, CSS3 та мови програмування JavaScript дозволяє створювати чуйні веб-сторінки та сайти, що мають зручні інтерфейси та є базою для створення веб-рішень корпоративного рівня.

Метою викладання навчальної дисципліни "Веб-технології та веб-дизайн" є формування системи теоретичних знань і набуття практичних умінь і навичок щодо розробки та проектування веб-рішень, що виконуються на боці клієнта. Оволодіння навичками дизайну веб-інтерфейсів й веб-сторінок та набуття компетенцій щодо застосування технологій та інструментальних засобів розробки веб-орієнтованих систем.

Результатами вивчення даної дисципліни є придбання навичок з проектування та створення веб-інтерфейсів й веб-сторінок для малого підприємства, а також комплексних практичних навичок щодо розробки веб-додатків та інформаційних систем.

Характеристика навчальної дисципліни

Курс	**3 (підготовка бакалаврів)**
Семестр	**5**
Кількість кредитів ECTS	**5**
Форма підсумкового контролю	**екзамен**

Структурно-логічна схема вивчення навчальної дисципліни:

Пререквізити	Постреквізити
Операційні системи	Веб-програмування
Комп'ютерна графіка та візуалізація	Технології розробки та тестування програмного забезпечення
Комп'ютерні мережі	Кросплатформне програмування

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
КФ-2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки	РН-10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН-11. Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах; 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-15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН-17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок

Компетентності	Результати навчання
	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-31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН-47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
КФ-3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.	РН-9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; 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-15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН-16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; 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-20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації

Компетентності	Результати навчання
	від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; 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-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-47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН-50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
К-6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження	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-20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів 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-27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН-31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; 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

Компетентності	Результати навчання
	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-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-52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах
КФ-12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою 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-12. Розробляти моделі загроз та порушника; РН-13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН-16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; 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-30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН-33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі

Компетентності	Результати навчання
	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-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 різні 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
КФ-2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки	РН-10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН-11. Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах; 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-15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; 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

Компетентності	Результати навчання
	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-31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН-47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

Програма навчальної дисципліни

Змістовий модуль 1. Основи веб-технологій та веб-дизайну.

Тема 1. *Структура і принципи Веб. Уведення в HTML.*

Тема 2. *Технологія CSS та її підтримка браузерами.*

Тема 3. *Блокова верстка сторінок веб-сайта.*

Змістовий модуль 2. Веб-програмування на боці клієнта.

Тема 4. *Основи мови програмування Javascript.*

Тема 5. *Програмна взаємодія з HTML документами на основі DOM API.*

Тема 6. *Використання бібліотек JavaScript для розробки веб-сайтів. Бібліотека jQuery.*

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.

Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, практичні 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) модульний контроль, що проводиться у формі контрольної роботи як проміжний міні-екзамен з ініціативи викладача з урахуванням поточного контролю за відповідний змістовий модуль і має на меті інтегровану оцінку результатів навчання студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля;

3) 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:

- аналізувати та декомпозувати завдання щодо створення інформаційних систем з використанням веб-технологій;
- аналізувати зв’язки між бізнес процесами та інформаційної компоненти в межах задач що вирішуються за допомогою обраної інформаційної моделі;
- використовувати в професійній діяльності теорії, методи та сучасні практики щодо розробки та розгортання інформаційної системи малого підприємства;
- вирішувати задачі забезпечення, супроводу та підтримки веб-рішень у інформаційних системах на основі навичок та знань, щодо структурних (структурно-логічних) схем, топології, сучасних архітектур та моделей інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;
- вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків.

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.

Лекцій: за активну роботу на парі нараховуються бали, 1 бал за кожне заняття за умови виконання студентом програми навчальної дисципліни. Загальна кількість балів складає 9.

Лабораторні заняття: за умови виконання лабораторної роботи нараховується 1 бал, за умови захисту лабораторної роботи нараховується 7 балів, максимальна кількість балів становить 43, а мінімальна – 15.

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.

Модульний контроль: проводиться у формі контрольної роботи як проміжний міні-екзамен з ініціативи викладача з урахуванням поточного контролю за відповідний змістовий модуль і має на меті *інтегровану* оцінку результатів навчання студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля. За кожну контрольну роботу може бути нараховано 4 бали. Загальна кількість балів складає 8.

Підсумковий контроль:

Формою підсумкового контролю є іспит. Екзаменаційний білет охоплює програму дисципліни і передбачає визначення рівня знань та ступеня опанування студентами компетентностей. Кожен екзаменаційний білет складається із 20 тестів та 3 практичних завдань (ситуаційного, діагностичного та евристичного).

Екзаменаційний білет включає:

Тести: мах кількість балів – 14.

Ситуаційне завдання: мах кількість балів – 5.

Діагностичне завдання: мах кількість балів – 9.

Евристичне завдання: мах кількість балів – 12.

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	Мах бал
Тема 1, 2, 3, 4.	***Аудиторна робота***			
	Лекція	Тема 1. Структура і принципи Веб. Уведення в HTML	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота 1. Розробка веб-сторінок з використанням мови HTML	Активна участь у виконанні лабораторної роботи.	3
	Самостійна робота			
	Підготовка до занять	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до захисту лабораторної роботи	Захист лабораторної роботи.	7
Тема 5, 6.	***Аудиторна робота***			
	Лекція	Тема 2. Технологія CSS та її підтримка браузерами	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота 2. Розробка веб-сторінки з використанням CSS на основі макету	Активна участь у виконанні лабораторної	2

			роботи.	
	Самостійна робота			
	Підготовка до занять	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до захисту лабораторної роботи		
Тема 7, 8.	***Аудиторна робота***			
	Лекція	Тема 3. Блокова верстка сторінок веб-сайта	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота 3. Розробка веб-сайта з використанням блокової верстки	Активна участь у виконанні лабораторної роботи.	2
			Захист лабораторної роботи.	7
	Самостійна робота			
	Підготовка до занять	Пошук, підбір та огляд літературних джерел за заданою тематикою. Виконання контрольної роботи.		

Тема 9, 10, 11, 12.	***Аудиторна робота***			
	Лекція	Тема 4. Основи мови програмування Javascript	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота 4. Розробка динамічних веб-сторінок за допомогою мови Javascript	Активна участь у виконанні лабораторної роботи.	4
	Самостійна робота			
	Підготовка до занять	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до захисту лабораторної роботи та виконання контрольної роботи.	Захист лабораторної роботи.	7
			Письмова контрольна робота	4
Тема 13, 14.	***Аудиторна робота***			
	Лекція	Тема 5. Програмна взаємодія з HTML документами на основі DOM API	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота 5. Розробка динамічних веб-сторінок за допомогою мови Javascript та DOM API	Активна участь у виконанні лабораторної	2

			роботи.	
	Самостійна робота			
	Підготовка до занять	Пошук, підбір та огляд літературних джерел за заданою тематикою. Виконання контрольної роботи.		
Тема 15, 16, 17.	***Аудиторна робота***			
	Лекція	Тема 6. Використання бібліотек JavaScript для розробки веб-сайтів. Бібліотека jQuery	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота 6. Розробка динамічних веб-сторінок за допомогою Javascript-бібліотеки jQuery	Активна участь у виконанні лабораторної роботи.	2
	Самостійна робота			
	Підготовка до занять	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до захисту лабораторної роботи та виконання контрольної роботи.	Захист лабораторної роботи.	7
			Письмова контрольна робота	4
Екзамен				40

Рекомендована література

Основна

1. Самсонов В.В. Методи та засоби Інтернет-технологій : навч. посіб / В.В. Самсонов, А.Л. Єрохін. – Х. : Компанія СМІТ, 2008.– 263 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. Ньюмен С. Создание микросервисов/С.Ньюмен.– СПб.: Питер, 2016. – 304 с.

4. Пушкар О. І. Технології комп'ютерного дизайну : навч. посіб. / О. І. Пушкар. – Х. : ІНЖЕК, 2013. – 166 с.

5. Огурцов В.В. Основи веб та веб-дизайн, програмування на боці кліента : лаборат. практикум з навч. дисципліни "Веб-технології та веб-дизайн" / В.В. Огурцов. – Х. : ХНЕУ ім. С. Кузнеця, 2015. – 207 с.

Додаткова

6. Chacon S. Pro Git [Electronic resourse] / Scott Chacon, Ben Straub. Apress, 2014.– 608 p. – Mode of access: https://git-scm.com/book/uk/v2.

7. Методи та моделі розроблення комп’ютерних систем і мереж : монографія / В. С. Пономаренко, С. В. Мінухін, С. В. Кавун та ін. – Х. : Вид. ХНЕУ, 2008. – 315 с.

Інформаційні ресурси

8. Front-End Developer Handbook 2018 / Cody Lindley – Frontend Masters. – 2018. – 168 p. [Electronic resource]. – Access mode : https://legacy.gitbook.com/book/ frontendmasters/front-end-developer-handbook-2018/details.

9. HTML 5.2. W3C Recommendation, 14 December 2017 [Electronic resource]. – Access mode : https://www.w3.org/TR/html52/.

10. CSS Snapshot 2017. W3C Working Group Note, 31 January 2017 [Electronic resource]. – Access mode : https://www.w3.org/TR/css-2017/.

11. Web technology for developers – MDN Web Docs [Electronic resource]. – Access mode : https://developer.mozilla.org/en-US/docs/Web.

12. JavaScript. The Right Way [Electronic resource]. – Access mode : http://jstherightway.org/.

13. Кантор И. Современный учебник Javascript [Электронный ресурс] / И. Кантор. – Режим доступа : https://learn.javascript.ru/.

14. Friedman V. 10 Principles Of Good Website Design [Electronic resource]. – Access mode : https://www.smashingmagazine.com/2008/01/10-principles-of-effective-web-design/.

15. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Веб-технології та веб-дизайн" https://pns.hneu.edu.ua/course/view.php?id=5381.