



Силабус освітнього компонента Програма навчальної дисципліни



Розробка інтерфейсу веб- додатків

Шифр та назва спеціальності

F5 – Кібербезпека та захист інформації

Спеціалізація

Освітня програма

Кібербезпека

Рівень освіти

Другий (магістерський)

Семестр

2

Інститут

ННІ комп'ютерних наук та інформаційних технологій

Кафедра

Кібербезпеки (328)

Тип дисципліни

Професійного спрямування, Вибіркова

Форма навчання

Денна, заочна

Мова викладання

Українська, англійська

Викладачі, розробники



ДУНАЄВ Сергій Владиславович

Serhii.Dunaiev@cs.khpi.edu.ua

Асистент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: 5, з них 3 статті, що реферуються у науково-метричних базах Scopus. Лектор з дисциплін: "Веб-програмування" та інших у студентів бакалавріата та магістратури.

[Детальніше про викладача на сайті кафедри](#)



ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua

Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Лауреат національної премії імені Бориса Патона.

Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти. Провідний лектор з дисциплін: Математичні основи криптології, Комп'ютерні мережі, Основи криптографічного захисту, Методи криптоаналізу, Основи кібербезпеки, Сучасні проблеми постквантової криптографії, Основи наукових досліджень, Цифрова

криміналістика, Етичний хакінг у студентів бакалавріата та магістратури, Методологія наукової та педагогічної діяльності в науках кіберзахисту для аспірантів.

[Детальніше про викладача на сайті кафедри](#)

Загальна інформація

Анотація

Курс "Розробка інтерфейсу веб-додатків" охоплює основи проектування та реалізації інтерфейсів для веб-додатків. Студенти отримають знання про принципи UX/UI дизайну, сучасні технології, методи створення прототипів та впровадження інтерактивних елементів. Курс передбачає практичні завдання, що дозволяють застосувати теоретичні знання у реальних проектах.

Мета та цілі дисципліни

Метою курсу є ознайомлення студентів із ключовими аспектами розробки інтерфейсів веб-додатків, розвиток навичок проектування з акцентом на користувацький досвід, а також вивчення сучасних інструментів і технологій для створення інтерактивних та зручних інтерфейсів.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

Компетентності

КЗ–1. Здатність застосовувати знання у практичних ситуаціях.

КЗ–2. Здатність проводити дослідження на відповідному рівні.

КЗ–4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

Результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

РН3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів у сфері інформаційної та/або кібербезпеки в цілому.

РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та/або кібербезпеки.

РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 16 год., лабораторні роботи – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Іноземна мова, Основи веб-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

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Вступ до UX/UI дизайну. Ознайомлення з принципами користувацького досвіду (UX) та інтерфейсного дизайну (UI). Розгляд ролі дизайнера, основних етапів створення інтерфейсів, критеріїв якісного UX та сучасних тенденцій візуального дизайну.	4
Тема 2. Основи проєктування інтерфейсів. Вивчення базових принципів створення структурованих і зрозумілих інтерфейсів: композиція, ієрархія, навігація, сітки, колір, типографіка. Формування логічної структури сторінок і патернів взаємодії користувача з системою.	4
Тема 3. Дослідження користувачів та тестування. Методи збору інформації про цільову аудиторію: інтерв'ю, опитування, персони, користувацькі сценарії. Аналіз поведінки користувачів і проведення юзабіліті-тестувань для оцінки ефективності розроблених інтерфейсів.	2
Тема 4. Веб-технології та фреймворки. Огляд технологій, що лежать в основі сучасних веб-інтерфейсів: HTML, CSS, JavaScript. Знайомство з популярними фреймворками (React, Vue, Angular) та принципами компонування, адаптивного дизайну і responsive-підходів.	2
Тема 5. Прототипування та дизайн систем. Створення прототипів різної деталізації (від скетчів до інтерактивних моделей). Вивчення дизайн-систем: компоненти, гайдлайни, стилі та стандарти, що забезпечують цілісність і масштабованість інтерфейсу.	2
Тема 6. Інтерактивність та анімація в інтерфейсах. Принципи створення живих, динамічних інтерфейсів: мікровзаємодії, переходи, анімації, візуальні підказки. Використання анімації для покращення UX, а також огляд інструментів для створення інтерактивного досвіду.	2
Загальна кількість годин	16

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти α
Тема 1. Створення простого веб-інтерфейсу з HTML та CSS. Ознайомлення з основами побудови веб-сторінок. Студенти	6	0,2

вчаться створювати структуру інтерфейсу за допомогою HTML та стилізувати її засобами CSS. Розглядаються базові елементи розмітки, робота з блоками, кольорами, шрифтами та компонентами інтерфейсу.

Тема 2. Розробка прототипу за допомогою Figma.

6

0,2

Вивчення інструментів Figma для створення візуальних макетів і інтерактивних прототипів. Студенти створюють дизайн-сцену, компоненти, застосовують стилі та налаштовують прості переходи між екранами для демонстрації логіки роботи інтерфейсу.

Тема 3. Дослідження користувачів.

5

0,1

Огляд методів збору інформації про потенційних користувачів продукту. Студенти вчаться формувати персони, сценарії використання, визначати потреби та поведінкові патерни, що впливають на дизайн інтерфейсів.

Тема 4. Створення адаптивного дизайну.

5

0,1

Вивчення принципів побудови інтерфейсів, що коректно відображаються на різних пристроях і розмірах екранів. Розглядаються медіа-запити, гнучкі сітки, адаптивні компоненти та підходи Mobile First і Responsive Design.

Тема 5. Інтеграція JavaScript для динамічності.

5

0,1

Основи застосування JavaScript для додавання інтерактивних елементів: модальні вікна, вкладки, валідатори форм, динамічні зміни контенту. Студенти знайомляться з DOM, базовими подіями та маніпуляцією елементами сторінки.

Тема 6. Тестування прототипів на реальних користувачах.

5

0,1

Ознайомлення з методами юзабіліті-тестування. Студенти навчаються організовувати тестові сесії, збирати зворотний зв'язок, аналізувати проблеми в інтерфейсі та вдосконалювати прототипи на основі реальної взаємодії користувачів.

Загальна кількість годин

32

$$\sum_{i=1}^n a_i = 0,8$$

Контрольні роботи

Теми контрольних робіт

Вагові

коефіцієнти b

Тема 1. Основи веб-інтерфейсів та прототипування.

0,1

Перевіряються знання з базового створення інтерфейсів у HTML/CSS, принципів адаптивного дизайну та першого етапу UX-проектування. Студент демонструє уміння побудови простої веб-сторінки, розуміння компонентів інтерфейсу, а також навички створення первинного прототипу у Figma.

Тема 2. UX-дослідження, інтерактивність і тестування.

0,1

Оцінюються здатність студента аналізувати користувацькі потреби, будувати сценарії взаємодії, додавати інтерактивність за допомогою JavaScript та проводити юзабіліті-тестування прототипів. Контрольна охоплює засади UX-досліджень, поведінкові патерни користувачів і методи оцінки якості інтерфейсу.

Загалом

$$\sum_{i=1}^m b_i = 0,2$$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Основи типографіки у веб-дизайні. Принципи вибору шрифтів, ієрархія тексту, читабельність та комбінування гарнітур.	8
Тема 2. Колірні системи та психологія кольору. Використання палітр, контрастність, доступність і вплив кольору на поведінку користувача.	8
Тема 3. Створення дизайн-систем і бібліотек компонентів. Патерни, стильові гайдлайни та робота з масштабованими UI-системами.	7
Тема 4. Доступність веб-інтерфейсів (Web Accessibility, WCAG). Підходи до створення інклюзивних інтерфейсів, ARIA-атрибути, принципи доступності.	7
Тема 5. Мікровзаємодії в інтерфейсах. Маленькі візуальні та звукові реакції, що покращують користувацький досвід.	7
Тема 6. UI-анімації: інструменти та практики. Використання CSS-анімацій, transitions, JavaScript-бібліотек та принципи плавності.	7
Тема 7. Інформаційна архітектура (IA). Структуризація інформації, навігаційні схеми, логічна організація контенту.	7
Тема 8. Створення лендингів і промо-сторінок. Структура, сценарій перегляду, UX-патерни та оптимізація для конверсій.	7
Тема 9. Оптимізація продуктивності фронтенду. Мінімізація стилів і скриптів, оптимізація зображень, прискорення завантаження UI.	7
Тема 10. Дизайн для мобільних застосунків. Особливості платформ iOS/Android, гайдлайни, адаптація веб-підходів до мобайл-UX.	7
Загальна кількість годин	72

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.

Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості.

Рекомендовані курси, тренінги, стажування

1. Онлайн-курс CISCO «Java 1»

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

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Steve Krug, Don't Make Me Think [Електронний ресурс]. – Режим доступу : <https://www.google.com.ua/books/edition/Don't+Make+Me+Think+Revisited/QlduAgAAQBAJ?hl=ru&gbpv=1&dq=Steve+Krug,+Don%27t+Make+Me+Think&printsec=frontcover>
2. Don Norman, The Design of Everyday Things [Електронний ресурс]. – Режим доступу : <https://dl.icdst.org/pdfs/files4/4bb8d08a9b309df7d86e62ec4056ceef.pdf>
3. Aaron Walter, A Book Apart: Designing for Emotion [Електронний ресурс]. – Режим доступу : https://books.google.com.ua/books/about/Designing+for+Emotion.html?id=Y4EctwAACAAJ&redir_esc=y
4. Mozilla Developer Network (MDN) - Ресурс з документацією веб-технологій [Електронний ресурс]. – Режим доступу : <https://developer.mozilla.org/ru/>
5. Jennifer Niederst Robbins, Learning Web Design [Електронний ресурс]. – Режим доступу : https://books.google.com.ua/books?id=FJkVxtXr7n0C&printsec=frontcover&redir_esc=y#v=onepage&q&f=false

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k :

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,8	0,2		

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.

Розрахунок підсумкової оцінки проводиться за формулою:

$$O = \Pi \cdot k_1 + K \cdot k_2 + I \cdot k_3 + \Pi_k \cdot k_4$$

де: Π – середньозважена середня оцінка за поточний контроль

I – оцінка за виконання індивідуального завдання

K – середньозважена оцінка за контрольні роботи

Π_k – оцінка за підсумковий контроль

$$\Pi = \frac{\Pi_1 \cdot a_1 + \Pi_2 \cdot a_2 + \dots + \Pi_n \cdot a_n}{\sum_{i=1}^n a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + \dots + K_m \cdot b_m}{\sum_{i=1}^m b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (Π , K , I , ...) виставляються за 100-бальною шкалою згідно з [положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ»](#).

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

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

Здобувач вищої освіти 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

30.08.2025



Завідувач кафедри

Сергій ЄВСЕЄВ

30.08.2025



Гарант ОП

Ольга КОРОЛЬ