Силабус освітнього компонента

Програма навчальної дисципліни

WEB-аналітика

Шифр та назва спеціальності
F5 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Кібербезпека

Тип дисципліни
Науково-професійного спрямування, Вибіркова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна

Семестр
3

Мова викладання
Українська

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 статтей 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

WEB-аналітика — це процес збору, аналізу та інтерпретації даних, які стосуються поведінки користувачів на веб-сайтах. Цей курс охоплює основи WEB-аналітики, основні інструменти та методи аналізу, які дозволяють приймати обґрунтовані рішення для поліпшення онлайн-продуктів і послуг.

Мета та цілі дисципліни

Метою курсу є ознайомлення студентів з основами WEB-аналітики, її інструментами та методами. Студенти отримають практичні навички збору та аналізу даних, що дозволять їм ефективно використовувати аналітику для покращення веб-сайтів і бізнес-процесів.

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. Провадити 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.
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

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 напряму 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.
РН24. Планувати та виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із застосуванням сучасних технологій, експериментальних і теоретичних методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики.

РН25. Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.

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, Основні поняття про аналітику.

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 WEB-аналітики: основні поняття та значення. Розглядаються базові принципи веб-аналітики, її роль у бізнесі та цифровому маркетингу. Вивчаються поняття трафіку, відвідуваності, користувацької активності та основні етапи аналітичного процесу.	4
Тема 2. Інструменти WEB-аналітики: Google Analytics та інші. Ознайомлення з популярними інструментами веб-аналітики — Google Analytics, Yandex.Metrica, Matomo, Hotjar. Розглядається процес налаштування, збору та аналізу даних із сайтів.	4
Тема 3. Збір даних: методи і технології (теги, cookies, пікселі). Вивчення механізмів збору даних про користувачів і їхню взаємодію з вебресурсом. Аналіз технологій відстеження: тегів, cookie-файлів, трекінгових пікселів і систем керування тегами (GTM).	2
Тема 4. Аналіз поведінки користувачів: метрики, KPI та їх інтерпретація. Дослідження основних метрик (час на сайті, глибина перегляду, bounce rate) та ключових показників ефективності (KPI). Формування звітів і візуалізація результатів для прийняття управлінських рішень.	2
Тема 5. Конверсія та її оптимізація: A/B тестування та його роль. Розгляд поняття конверсії, методів її підвищення, створення та проведення A/B тестів для визначення найефективніших варіантів дизайну, контенту чи структури сайту.	2
Тема 6. Пошукова оптимізація (SEO) та WEB-аналітика: взаємозв'язок та інтеграція. Вивчається взаємозв'язок між SEO та веб-аналітикою. Аналіз впливу пошукової оптимізації на трафік, ранжування сайту, поведінкові фактори користувачів і підвищення видимості ресурсу у пошукових системах.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Налаштування Google Analytics: створення облікового запису та налаштування. Студенти створюють обліковий запис у Google Analytics, налаштовують властивості сайту, визначають цілі відстеження та знайомляться з інтерфейсом інструменту.	6	0,2
Тема 2. Збір даних за допомогою тегів: впровадження тегів на веб-сайт. Виконується інтеграція тегів відстеження на веб-сторінки через Google Tag Manager або вручну. Розглядаються методи збирання даних про події, кліки та перегляди сторінок.	6	0,2
Тема 3. Аналіз звітів Google Analytics: основні метрики та їх значення. Досліджуються основні показники ефективності вебресурсу (сеанси, відмови, середня тривалість перегляду, конверсії). Студенти навчаються інтерпретувати дані для оцінки ефективності сайту.	5	0,1
Тема 4. Проведення A/B тестування: створення експериментів та аналіз результатів. Виконується налаштування та проведення A/B тестів для перевірки гіпотез щодо покращення вебінтерфейсу або контенту. Аналізуються результати та робляться висновки щодо оптимізації конверсії.	5	0,1
Тема 5. Використання Google Analytics: особливості та порівняння з іншими. Порівнюються можливості Google Analytics з іншими інструментами веб-аналітики (Matomo, Yandex.Metrica тощо). Аналізуються переваги, обмеження та сфери застосування кожного інструменту.	5	0,1
Тема 6. Створення дашбордів: візуалізація даних та аналіз звітів. Студенти створюють інтерактивні дашборди для представлення аналітичних даних. Розглядаються методи візуалізації метрик, сегментації аудиторії та створення автоматизованих звітів для прийняття рішень.	5	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Аналіз відвідуваності та поведінки користувачів вебсайту. Студенти проводять дослідження трафіку сайту за допомогою Google Analytics (або аналогічного інструменту). Аналізуються джерела відвідувань, показники залученості користувачів, сторінки виходу та поведінкові метрики. На основі результатів формується звіт із висновками та рекомендаціями щодо покращення користувацького досвіду.	0,1

Тема 2. Оцінка ефективності вебресурсу та оптимізація конверсії. Завдання полягає у виявленні ключових показників ефективності (KPI) для конкретного вебресурсу та проведенні A/B тестування або моделювання його результатів. Студенти аналізують конверсійні шляхи, виявляють слабкі місця у воронці продажів і пропонують шляхи оптимізації контенту, дизайну чи структури сайту для підвищення конверсії.	0,1
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. Веб-метрики: класифікація та вибір ключових показників. Розгляд типів веб-метрик (поведінкові, технічні, комерційні) та принципів вибору KPI залежно від цілей бізнесу.	8
Тема 2. Аналітика соціальних мереж (Social Media Analytics). Методи збору та аналізу даних із соціальних платформ (Facebook, Instagram, LinkedIn). Оцінка ефективності контенту та взаємодії з аудиторією.	8
Тема 3. Аналіз воронки продажів у веб-аналітиці. Вивчення етапів руху користувача від першого відвідування до конверсії. Виявлення «вузьких місць» у воронці.	7
Тема 4. Використання Google Data Studio (Looker Studio) для побудови звітів. Основи створення інтерактивних звітів, інтеграція з Google Analytics, Google Ads та іншими джерелами даних.	7
Тема 5. Аналіз ефективності рекламних кампаній (PPC, SEO, SMM). Методи оцінювання рентабельності рекламних каналів за допомогою метрик ROI, ROAS, CPC та CTR.	7
Тема 6. Веб-аналітика в e-commerce. Застосування аналітики для інтернет-магазинів: відстеження конверсій, середнього чеку, повторних покупок.	7
Тема 7. Користувацька сегментація та побудова аудиторій. Методи поділу відвідувачів сайту за поведінковими, демографічними та географічними ознаками.	7
Тема 8. Веб-аналітика мобільних застосунків. Інструменти та методи збору аналітичних даних у мобільних додатках (Firebase, Appsflyer).	7
Тема 9. Етика та конфіденційність у веб-аналітиці. Вивчення законодавчих вимог (GDPR, CCPA) та методів анонімізації користувацьких даних.	7
Тема 10. Використання машинного навчання у веб-аналітиці. Ознайомлення з інструментами прогнозування поведінки користувачів, персоналізацією контенту та автоматизацією аналітики.	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

За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Google Analytics for Beginners – онлайн-курс від Google. URL: https://courses.thedev.io/courses/google-analytics-dlya-nachinauschih
2. Avinash Kaushik, Web Analytics 2.0. URL: https://books.google.com.ua/books/about/Web_Analytics_2_0.html?id=IykGCqV1v20C&redir_esc=y
3. Tom Tullis and Albert Albert, Measuring the User Experience. URL: https://books.google.com.ua/books/about/Measuring_the_User_Experience.html?id=KsjpuMJ6T-YC&redir_esc=y
4. Dan Siroker and Pete Koomen, A/B Testing: The Most Powerful Way to Turn Clicks Into Customers. URL: https://books.google.com.ua/books/about/A_B_Testing.html?id=kZEAjwEACAAJ&redir_esc=y
5. Офіційна документація Google Analytics.

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:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
K – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

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

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

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

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

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

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

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** Станіслав МІЛЕВСЬКИЙ