Силабус освітнього компонента
Програма навчальної дисципліни

Захист систем електронної комерції та мультисервісних систем

Шифр та назва спеціальності
К4 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Управління інформаційною безпекою

Тип дисципліни
Вибіркова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
4

Мова викладання
Українська

Викладачі, розробники

ПОГАСІЙ Сергій Сергійович
Serhii.Pohasii@khpi.edu.ua
Доктор технічних наук, доцент, професор кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 95, з них патентів на корисну модель 2, 6 монографій, з яких 4 колективних монографій, 4 навчальних посібників, з яких 4 з грифом Міністерства освіти і науки України, 65 статті у закордонних виданнях та фахових виданнях України, з них 11 у наукометричній базі Scopus. Гарант освітньо-наукової програми «Кібербезпека» третього (доктор філософії) рівня вищої освіти, провідний лектор з дисциплін: «Аналогові та цифрові електронні пристрої», «Інтернет речей та сервісів», «Безпека хмарних технологій», «Основи побудови та захисту сучасних операційних систем», «Моделювання систем критичної інфраструктури», «Основи побудови та захисту мікропроцесорних систем», «Безпека смарт-технологій та Інтернет-речей», «Інформаційно-комунікаційні системи у сфері національної безпеки» у студентів бакалавріата та магістратури, Розділ «Інформаційна безпека хмарних сервісів», «Сучасні методи захисту соціо-кіберфізичних систем», «Моделювання механізмів кібербезпеки» для аспірантів.
Детальніше про викладача на сайті кафедри

АКСЬОНОВА Ірина Вікторівна

Iryna.Aksonova@khpi.edu.ua

Кандидат економічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 150, з них свідоцтв на авторський твір - більше 15, розділів у монографіях - 10, статей, що реферуються у науково метричних базах Scopus та WoS - 9. Лектор з дисциплін: "Теорія інформацій і кодування", "Нейронні мережі", "Моделювання інформаційних систем", "Штучний інтелект і бізнес-аналітика", "Стандартизація та сертифікація в галузі інформаційної безпеки" та інших у студентів бакалавріата та магістратури.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Захист систем електронної комерції та мультисервісних систем" є вибірковою навчальною дисципліною. Дисципліна спрямована на формування системи теоретичних і практичних знань з електронної комерції, напрямки її розвитку й способи ведення, які дадуть змогу студентам та фахівцям професійно здійснювати свою діяльність у сучасному динамічному глобальному середовищі.

Мета та цілі дисципліни

Освоєння принципів використання програмного забезпечення для тестування та виявлення вразливостей веб-додатків та веб-сервісів та створення систем захисту від виявлених вразливостей, запобігання шляхів несанкціонованого доступу до даних в мультисервісних системах та системах електронної комерції.

Формат занять

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

Компетентності

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
СК4. Здатність прогнозувати реалізації управлінських рішень щодо захисту інформації.
СК5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
СК8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.

Результати навчання

РН3. 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.
РН4. Вільно спілкуватися державною мовою.
РН7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
РН8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.

РН10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
РН13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.
РН11. 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.
РН12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
РН16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
РН17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
РН18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
РН19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
РН21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
РН22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

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)

Інформаційна безпека держави, Основи соціальної інженерії.

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. Електронний ринок, поняття електронного бізнесу та електронної комерції. Історія розвитку електронної комерції.	2
Тема 2. Базові технології електронної комерції. Класифікація Web-сайтів. CMS системи. Платні системи з відкритим(закритим) кодом.	2
Тема 3. Способи організації Інтернет – магазинів. Принципи функціонування та керування Інтернет – магазином.	1

Тема 4. Послуги в електронній комерції. Туристичні послуги в Інтернеті. Інтернет-страхування. Посилення конкуренції.	1
Тема 5. Системи електронної комерції G2C та G2B. Чотири рівні електронних систем урядового керування. Структура електронного уряду. Державні електронні торговельні-закупівельні майданчики.	1
Тема 6. Інтернет маркетинг. Сайтопромоутінг. Закони Інтернет-маркетингу. Інтернет реклама (таргетинг, медіапланування).	1
Тема 7. E-mail реклама. Вірусний маркетинг. Переваги E-mail-реклами. Індивідуальні листи. Списки розсилань. Дискусійні листи. Спам. Безкоштовне поширення товарів та послуг.	1
Тема 8. Види загроз електронної комерції. Загальна класифікація загроз електронної комерції.	1
Тема 9. Заходи безпеки органів державного управління. Безпека взаємовідносин державних установ з іншими суб'єктами засобами електронної комунікації. Модель потенційного порушника.	1
Тема 10. Зарубіжний досвід технологій створення захищеного простору суб'єкта підприємницької діяльності. Зарубіжний досвід технологій створення захищеного простору суб'єкта підприємницької діяльності (США, Велика Британія, Німеччина, Україна).	1
Тема 11. Заходи безпеки фінансових установ. Безпека платіжних систем. Аналіз ризику. Поширені загрози безпеки та методи їх усунення.	1
Тема 12. Програмні заходи безпеки. Захист окремих елементів мережевого обміну даними. Інструменти безпеки від Google. Шифрування SSL у Gmail. Застереження щодо зловмисних завантажень у Chrome. Найпоширеніші способи шахрайства в Інтернеті.	1
Тема 13. Електронні злочини в Інтернеті та способи їх уникнення. HYIP-фонди. Сайти-двійники. Провокаційні сайти-двійники. Кардінг.	1
Тема 14. Шахрайство у фінансовій сфері. Комплекс шахрайських прийомів у сфері інвестицій. Фінансові піраміди. Афери з цінними паперами.	1
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Визначення міри захищеності інформаційної системи, що обслуговує суб'єктів електронної комерції. Основні критерії оцінювання захищеності ІС. Методи аналізу інформаційних ризиків. Використання стандартів ISO/IEC 27001 для визначення рівня захищеності. Практичні інструменти моніторингу захищеності систем. Формування звіту про рівень кіберзахисту.	8	1
Тема 2. Вивчення основних державних Інтернет-ресурсів України. Огляд державних порталів (Дія, Prozorro, ЄДР тощо).	8	1

Безпекові механізми державних сервісів. Перевірка захищеності вебресурсів (HTTPS, сертифікати SSL/TLS). Потенційні загрози державним інформаційним системам. Аналіз практичних кейсів кібератак на державні ресурси.		
Тема 3. Вивчення фінансових Інтернет-ресурсів України та розрахунок пари кодів за алгоритмом RSA. Основні фінансові Інтернет-ресурси (банківські сервіси, платіжні системи). Методи захисту електронних фінансових операцій. Теоретичні основи алгоритму RSA. Практичний розрахунок відкритого та закритого ключів RSA. Використання RSA у захисті електронних транзакцій.	8	1
Тема 4. Визначення можливих небезпек на підприємстві, яке працює в режимі електронної комерції та вивчення роботи програми PortablePGP. Потенційні загрози електронній комерції (шкідливе ПЗ, фішинг, DDoS). Методи ідентифікації небезпек на підприємстві. Огляд технологій шифрування в електронній комерції. Практичне використання PortablePGP для генерації ключів. Шифрування та дешифрування повідомлень у PortablePGP.	8	1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 4$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Методи та засоби забезпечення захисту інформаційних систем в електронній комерції. Аналіз ризиків та загроз для бізнесу в цифровому середовищі. Використання криптографічних алгоритмів (RSA, AES, PGP) у захисті транзакцій. Практика застосування стандартів інформаційної безпеки (ISO/IEC 27001, PCI DSS).	1,5
Тема 2. Захист державних та фінансових Інтернет-ресурсів: проблеми та перспективи. Основні вимоги до безпеки вебресурсів. Механізми аутентифікації та електронних довірчих послуг. Приклади кібератак на державні та фінансові ресурси України та світу.	1,5
Загалом	$\sum_{i=1}^{m} b_i = 3$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріал

Теми для самостійного вивчення	Кількість годин
Тема 1. Протоколи безпечної електронної комерції (SSL/TLS, SET). Принципи роботи. Використання в сучасних платіжних системах.	15
Тема 2. Захист електронних платіжних систем. Механізми безпечної обробки транзакцій. Захист від шахрайства у фінансових операціях.	15
Тема 3. Механізми аутентифікації в системах електронної комерції. Паролі, токени, біометричні методи. Двофакторна та багатофакторна	14

автентифікація.	
Тема 4. Криптографічні методи забезпечення конфіденційності та цілісності даних. Симетричні та асиметричні алгоритми. Електронний цифровий підпис.	14
Тема 5. Правове забезпечення захисту інформації в електронній комерції. Законодавство України у сфері електронної комерції та кіберзахисту. Міжнародні норми і стандарти.	14
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. Про електронні довірчі послуги: Закон України від 5 жовт. 2017 р. № 2155-VIII . Поточна редакція від 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text
2. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України: Постанова Правління НБУ від 28.09.2017 р. № 95. Поточна редакція від 28.09.2017. URL: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text
3. ДСТУ ISO/IEC 27005:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки (ISO/IEC 27005:2022, IDT).
https://www.iso.org/ru/contents/data/standard/08/05/80585.html
4. Ахрамович В.М. Курс лекцій з навчальної дисципліни «Кібербезпека банківських та комерційних структур» /В.М.Ахрамович. Державний університет телекомунікацій. Київ.:ДУТ, 2019. 163 с.
https://b.twirpx.link/file/3149823/
5. Краус К.М., Краус Н.М., Манжура О.В. К 78 Електронна комерція та Інтернет-торгівля: навчально-методичний посібник. Київ: Аграр Медіа Груп, 2021. 454 с. URL: https://elibrary.kubg.edu.ua/id/eprint/37044/1/Kraus_Elektronna_komertsiia_2021.pdf
6. Безпека електронної комерції: навч. посібн. І.М. Пістунов, Є.В., Кочура; Нац. гірн. ун–т. Дніпропетровськ: НГУ, 2014. 125 с.
http://pistunovi.inf.ua/6_E_K.pdf
7. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
http://monograph.com.ua/pctc/catalog/view/978-617-7319-72-5/978-617-7319-72-5/746-2

Додаткова література

8. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
http://monograph.com.ua/pctc/catalog/view/64/52/231-1

9. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p. http://monograph.com.ua/pctc/catalog/view/978-617-7319-57-2/117/419-2.
10. Аналіз впливу Угоди про асоціацію з ЄС на комплексний розвиток електронних сфер урядування, закупівель та комерції (2018).
11. Карпенко М. Ю. Електронна комерція : конспект лекцій для студентів усіх форм навчання першого (бакалаврського) рівня вищої освіти спеціальності 073 – Менеджмент / М. Ю. Карпенко ; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Харків : ХНУМГ ім. О. М. Бекетова, 2021. 146 с. URL: https://eprints.kname.edu.ua/58976/1/2020%20%D0%BF%D0%B5%D1%87%20129%D0%9B-073-%D0%9A%D0%BE%D0%BD%D1%81%D0%BF%D0%B5%D0%BA%D1%82%D0%95%D0%BB%D0%9A%D0%BE%D0%BC%D0%BC.pdf
12. Чмир І.О. Електронна комерція: конспект лекцій. Одеса, Одеський державний екологічний університет, 2021. 148 с. URL: http://eprints.library.odeku.edu.ua/id/eprint/8564/1/%D0%A7%D0%BC%D1%8B%D1%80%D1%8C%20%D0%98.%D0%90.%20%D0%AD%D0%9A.%202021.pdf

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
0,7	0,3		

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».

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** Роман КОРОЛЬОВ