



Силабус освітнього компонента

Програма навчальної дисципліни



Захист систем електронної комерції та мультисервісних систем

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

Вибіркова

Рівень освіти

Перший (бакалаврський)

Форма навчання

Денна, заочна

Семестр

4

Мова викладання

Українська, англійська

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@khpі.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

ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та систем захисту інформації.

СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.

СК4. Здатність забезпечувати захист інформації в інформаційних системах згідно встановленої політики кібербезпеки та захисту інформації.

СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

Результати навчання

РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недобросовісності у професійній діяльності.

PH9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

PH10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

PH11. Планувати підготовку та забезпечувати неперервність процесів в організаціях згідно встановленої політики кібербезпеки та з урахування вимог до захисту інформації.

PH12. Застосовувати методи захисту інформації в інформаційних системах згідно встановленої політики інформаційної безпеки.

PH13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних та програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних систем та\або інфраструктури організації в цілому.

PH17. Забезпечувати функціонування системи управління кібербезпекою та захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

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 проекти, 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.	1

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

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти α
Тема 1. Визначення міри захищеності інформаційної системи, що обслуговує суб'єктів електронної комерції.	8	1
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.		
Тема 2. Вивчення основних державних Інтернет-ресурсів України.	8	1
Огляд державних порталів (Дія, Prozorro, ЄДР тощо). Безпекі 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.	8	1
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.

Тема 4. Визначення можливих небезпек на підприємстві, яке працює в режимі електронної комерції та вивчення роботи програми PortablePGP.

8

1

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.

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.

1,5

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).

Тема 2. Захист державних та фінансових Інтернет-ресурсів: проблеми та перспективи.

1,5

Основні вимоги до безпеки вебресурсів. Механізми аутентифікації та електронних довірчих послуг. Приклади кібератак на державні та фінансові ресурси України та світу.

Загалом

$$\sum_{i=1}^m b_i = 3$$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення

Кількість годин

Тема 1. Протоколи безпечної електронної комерції (SSL/TLS, SET).

15

Принципи роботи. Використання в сучасних платіжних системах.

Тема 2. Захист електронних платіжних систем.

15

Механізми безпечної обробки транзакцій. Захист від шахрайства у фінансових операціях.

Тема 3. Механізми аутентифікації в системах електронної комерції.

14

Паролі, токени, біометричні методи. Двофакторна та багатофакторна автентифікація.

Тема 4. Криптографічні методи забезпечення конфіденційності та цілісності даних.

14

Симетричні та асиметричні алгоритми. Електронний цифровий підпис.

Тема 5. Правове забезпечення захисту інформації в електронній комерції.

14

Законодавство України у сфері електронної комерції та кіберзахисту. Міжнародні норми і стандарти.



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_komertsii_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->

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:

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

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»](#).

Підсумкова оцінка виставляється відповідно до розрахованої O 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

Сергій ЄВСЕЄВ