



Силабус освітнього компонента
Програма навчальної дисципліни



**Захист систем електронної
комерції та мультисервісних
систем**

Шифр та назва спеціальності

257 – Управління інформаційною безпекою

Інститут

ННІ комп'ютерних наук та інформаційних технологій

Освітня програма

Управління інформаційною безпекою

Кафедра

Кібербезпеки (328)

Рівень освіти

Бакалавр

Тип дисципліни

Профільна підготовка, Вибіркова

Семестр

4

Мова викладання

Українська

Викладачі, розробники



КОРОЛЬОВ Роман Володимирович

korolevrv01@ukr.net

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

Кількість наукових публікацій: понад 80, з них патентів на корисну модель 12, 1 колективна монографія, 2 навчальних посібника, 65 статті у закордонних виданнях та фахових виданнях України, з них 5 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Бездротова та мобільна безпека», «Основи стеганографії», «Бізнес інтеллідженс», «Фізичні основи технічних засобів розвідки» у студентів бакалавріата та магістратури.

[Детальніше про викладача на сайті кафедри](#)



АКСЬОНОВА Ірина Вікторівна

Iryna.Aksonova@khi.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: «Нейронні мережі», "Моделювання систем інформаційної безпеки", "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 роботи, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ-4. Здатність спілкуватися державною мовою як усно, так і письмово.

КЗ-6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ФК-3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.

ФК-4. Здатність прогнозувати реалізації управлінських рішень щодо захисту інформації.

ФК-5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.

ФК-8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.

Результати навчання

ПРН-3. 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.

ПРН-4. Вільно спілкуватися державною мовою.

ПРН-7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.

ПРН-8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.

ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.

ПРН-13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.

ПРН-11. 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.

ПРН-12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

ПРН-16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.

ПРН-17. Вміти розв'язувати задачі управління інформаційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.

ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.

ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.

ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.

ПРН-22. 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 – 32 год., лабораторні роботи – 16 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Менеджмент інформаційної безпеки, Національна безпека держави.

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

Теми лекційних занять

Тема 1. Електронний ринок, поняття електронного бізнесу та електронної комерції.

Історія розвитку електронної комерції.

Тема 2. Базові технології електронної комерції.

Класифікація Web-сайтів. CMS системи. Платні системи з відкритим(закритим) кодом.

Тема 3. Способи організації Інтернет – магазинів.

Принципи функціонування та керування Інтернет – магазином.

Тема 4. Послуги в електронній комерції.

Туристичні послуги в Інтернеті. Інтернет-страхування. Посилення конкуренції.

Тема 5. Системи електронної комерції G2C та G2B.

Чотири рівні електронних систем урядового керування. Структура електронного уряду. Державні електронні торгово-закупівельні майданчики.

Тема 6. Інтернет маркетинг. Сайтопромоутінг.

Закони Інтернет-маркетингу. Інтернет реклама (таргетинг, медіапланування).

Тема 7. E-mail реклама. Вірусний маркетинг.

Переваги E-mail-реклами. Індивідуальні листи. Списки розсилок. Дискусійні листи. Спам.

Безкоштовне поширення товарів та послуг.

Тема 8. Види загроз електронної комерції.

Загальна класифікація загроз електронної комерції.

Тема 9. Заходи безпеки органів державного управління.

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.

Зарубіжний досвід технологій створення захищеного простору суб'єкта підприємницької діяльності (США, Велика Британія, Німеччина, Україна).

Тема 11. Заходи безпеки фінансових установ.

Безпека платіжних систем. Аналіз ризику. Поширені загрози безпеки та методи їх усунення.

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.

Тема 13. Електронні злочини в Інтернеті та способи їх уникнення.

НУІР-фонди. Сайти-двійники. Провокаційні сайти-двійники. Кардінг.

Тема 14. Шахрайство у фінансовій сфері.

Комплекс шахрайських прийомів у сфері інвестицій. Фінансові піраміди. Афери з цінними паперами.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Визначення міри захищеності інформаційної системи, що обслуговує суб'єктів електронної комерції.

Тема 2. Вивчення основних державних Інтернет-ресурсів України.

Тема 3. Вивчення фінансових Інтернет-ресурсів України та розрахунок пари кодів за алгоритмом RSA.

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

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (<http://surl.li/pxssv>), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.

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

Література та навчальні матеріали

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. – К.:ДУТ, 2019. – 163 с. іл. – Бібліограф.: 166 с. <https://b.twirpx.link/file/3149823/>
5. 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
6. Тардаскіна Т.М. Електронна комерція: Навчальний посібник / Тардаскіна Т.М., Стрельчук Є.М., Терешко Ю.В. Одеса: ОНАЗ ім. О.С. Попова, 2011. 244 с.

<https://library.kre.dp.ua/Books/2-4%20kurs/%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D0%B8%20%D0%BC%D0%B0%D1%80%D0%BA%D0%B5%D1%82%D0%B8%D0%BD%D0%B3%D1%83%20%D1%82%D0%B0%20%D0%BC%D0%B5%D0%BD%D0%B5%D0%B4%D0%B6%D0%BC%D0%B5%D0%BD%D1%82%D1%83/%D0%9E%D0%9D%D0%90%D0%97%20%D0%9F%D0%9E%D0%9F%D0%9E%D0%92%D0%90%20%D0%BF%D1%80%D0%B0%D0%BA%D1%82/%D0%95%D0%9B%D0%95%D0%9A%D0%A2%D0%A0%D0%9E%D0%9D%D0%9D%D0%90%20%D0%9A%D0%9E%D0%9C%D0%95%D0%A0%D0%A6%D0%86%D0%AF.pdf.pdf>

7. 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>

8. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlov, 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>

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>.

Додаткова література

10. E-commerce in regional small to medium enterprises. Robert MacGregor and Lejla Vrazalic, authors, Published in the United States of America by IGI Publishing, 2007. 429p.

https://books.google.com.ua/books/about/E+Commerce+in+Regional+Small+to+Medium+E.html?id=v6jde0EGRIC&redir_esc=y

11. Global e-Commerce: Impacts of National Environment and Policy. Edited by Kenneth L. Kraemer, Jason Dedrick, Nigel P. Melville, Kevin Zhu, Cambridge University Press 2006. 428p.

<https://www.google.com.ua/books/edition/Global+e+commerce/uDvPfcV2yFgC?hl=ru&gbpv=1&dq=Global+e-Commerce:Impacts+of+National+Environment+and+Policy&printsec=frontcover>

12. Web Security & Commerce. Simson Garfinkel & Eugene H. Spafford First Edition, June 1997. 506 p.

<https://www.google.com.ua/books/edition/Web+Security+Privacy+Commerce/jIBH98wwuv8C?hl=ru&gbpv=1&dq=Web+Security+%26+Commerce&printsec=frontcover>

13. E-Commerce and Web Technologies, 9th International Conference. Giuseppe Psaila, Roland Wagner (Eds.): EC-Web 2008 Turin, Italy, September 3-4, 2008 Proceedings 13, Springer Berlin Heidelberg New York. 155p.

<https://www.google.com.ua/books/edition/E+Commerce+and+Web+Technologies/BLYQcWjCeYkC?hl=ru&gbpv=1&dq=E-Commerce+and+Web+Technologies,+9th+International+Conference&printsec=frontcover>

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:

- лабораторні роботи: 30% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- контрольна робота: 20% семестрової оцінки;
- залік: 40% семестрової оцінки.

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

Студент 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

28.08.2024



Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2024



Гарант ОП
Роман КОРОЛЬОВ