Силабус освітнього компонента
Програма навчальної дисципліни

Промисловий та офісний шпіонаж

Шифр та назва спеціальності
К3 – Національна безпека (за окремими сферами забезпечення і видами діяльності)

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Національна безпека у сфері кіберзахисту

Тип дисципліни
Обов'язкова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
8

Мова викладання
Українська

Викладачі, розробники

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

Навчальна дисципліна "Промисловий та офісний шпіонаж" є нормативною навчальною дисципліною. Вивчення навчальної дисципліни спрямоване на засвоєння основ промислового та офісного шпіонажу, формування вмінь і навичок пошуку, обробки, аналізу, інтерпретації інформації щодо діяльності промислового підприємства та його конкурентів. Дисципліна спрямована на засвоєння базових знань для поглибленого вивчення діяльності промислових підприємств як учасників конкурентної боротьби на ринку, формування у студентів знань з загальних особливостей ведення промислового та офісного шпіонажу, отримання необхідних знань з питань організаційної та управлінської діяльності забезпечення конкурентного аналізу та промислового та офісного шпіонажу на підприємствах та в організаціях.

Мета та цілі дисципліни

Засвоєння основних рис, організації, правових основ та методів діяльності промислового та офісного шпіонажу, набуття студентами необхідних теоретичних знань і практичних навичок щодо аналітичної складової формування конкурентної стратегії бізнес-діяльності підприємства та ведення промислового та офісного шпіонажу.

Формат занять

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

Компетентності

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
СК11. Здатність використовувати практичні навички, тактику та прийоми роботи з людьми в інтересах службової діяльності.

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.
РН7. Вміти виявляти, ставити та вирішувати професійні завдання, вміти узагальнювати отримані результати, обробляти та аналізувати інформацію з різних джерел, оформлювати і презентувати результати досліджень відповідно до вимог.
РН10. Вміти аналізувати виклики та загрози національній безпеці за напрямами професійної діяльності та синтезувати інформацію щодо розроблення та реалізації стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).
РН18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
РН19. Вміти використовувати у професійній діяльності методи та інструменти організації соціальної взаємодії, співробітництва та розв'язання конфліктів у сфері професійної діяльності, практичні навички, тактику та прийоми, роботи з людьми в інтересах службової діяльності: працювати у команді з позицій лідера, радника (консультанта), помічника, планувати використання часу та визначати стимули і бар'єри ефективної роботи, здійснювати розподіл (делегування) функцій, повноважень і відповідальності між виконавцями.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 20 год., лабораторні роботи – 20 год., самостійна робота – 80 год.

Передумови вивчення дисципліни (пререквізити)

Вища математика, Математичні основи криптології, Алгоритми та структури даних.

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. Поняття, завдання та цілі промислового та офісного шпіонажу. Історія зародження та розвитку промислового та офісного шпіонажу. Поняття промислового та офісного шпіонажу. Завдання та особливості промислового та офісного шпіонажу.	2
Тема 2. Розвідувальна інформація. Характеристики і вимоги до розвідувальної інформації. Моделі промислового та офісного шпіонажу. Джерела отримання інформації. Конкуренція та конкурентне оточення.	2
Тема 3. Збір інформації з відкритих джерел. Збір інформації із засобів масової інформації. Збір інформації на виставках, конференціях, презентаціях. Збір інформації з використанням мережі Інтернет. Програми для роботи з інформацією.	2
Тема 4. Негласний збір інформації. Задачі агентурної роботи. Класифікація інформаторів. Етапи та зміст вербовочної розробки.	2
Тема 5. Зовнішнє спостереження. Історія зовнішнього спостереження. Спостереження в промисловому та офісному шпіонажі. Ведення зовнішнього спостереження. Виявлення зовнішнього спостереження.	2
Тема 6. Методика збору інформації при роботі промислового та офісного шпіонажу. Методика збору інформації про юридичну особу. Пошук «підходу» до особи, що приймає рішення. Аналіз телефонної активності.	2
Тема 7. Промисловий та офісний шпіонаж в кредитній сфері. Злиття та поглинання. Промисловий та офісний шпіонаж та торги.	2
Тема 8. Рекрутинг і промисловий та офісний шпіонаж. Шпіонаж намірів. Шпіонаж в бенчмаркінгу. Активні заходи. Дезінформація.	2
Тема 9. Створення системи промислового та офісного шпіонажу. Система економічного промислового та офісного шпіонажу суб'єкта господарської діяльності. Планування роботи промислового та офісного шпіонажу.	2
Тема 10. Інформаційно-аналітична робота. Форми представлення даних для промислового та офісного шпіонажу. Власний інтегрований банк даних служби безпеки підприємства. Історія	2

створення інтегрованого банку даних служб безпеки. Моделі представлення даних в електронних базах даних. Загальні принципи створення інформаційної системи служби безпеки підприємства. Концепція побудови інтегрованого банку даних служби безпеки підприємства.	
Загальна кількість годин	**20**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Промисловий та офісний шпіонаж: поняття, передумови виникнення та актуальність. Вивчення визначення промислового і офісного шпіонажу, економічних і соціальних передумов його виникнення, сучасних трендів. Аналіз впливу шпигунства на бізнес-процеси, репутацію та безпеку підприємства; ознайомлення з законодавчими обмеженнями та етичними аспектами.	4	0,1
Тема 2. Особливості функціонування промислового та офісного шпіонажу на підприємстві. Розгляд типових векторів і механізмів збору інформації у корпоративному середовищі (включно з внутрішніми загрозами), аналіз ролей задіяних осіб, ризиків для виробничих і бізнес-процесів. Практичні вправи з ідентифікації ризиків у організаційній структурі та оцінки можливих наслідків.	4	0,1
Тема 3. Новини та соцмережі як інструменти промислового та офісного шпіонажу. Дослідження, як публічна інформація у ЗМІ й соціальних мережах може стати джерелом витоків і корисної розвідки (OSINT). Практичні завдання — аналіз відкритих джерел на предмет випадкових витоків, розробка політик публічного інформування і рекомендацій для працівників щодо зниження ризиків.	4	0,1
Тема 4. Особливості збору інформації про юридичну та посадову особи. Огляд правових і етичних меж збору інформації про компанії та працівників. Вивчення джерел відкритої інформації, обмежень GDPR/профільного законодавства, правил документування і перевірки даних. Практична частина — розробка шаблонів запитів і процедур для легального збору інформації у рамках аудитів безпеки.	4	0,1
Тема 5. Практичні засади ведення промислового та офісного шпіонажу на підприємствах і в офісах. (Оборонна спрямованість) Моделювання сценаріїв виявлення і протидії шпигунству: внутрішні перевірки, аудит доступів, контроль фізичного і інформаційного доступу, тренінги персоналу. Розробка планів реагування на підозри про витік інформації та підготовка рекомендацій із мінімізації ризиків.	4	0,2
Загальна кількість годин	**20**	$\sum_{i=1}^{n} a_i = 0{,}6$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Методи та засоби збору інформації в промисловому та офісному шпіонажі. Розглядаються основні підходи до збору інформації з відкритих і закритих джерел, методи негласного отримання даних, організація зовнішнього спостереження та агентурної роботи. Особлива увага приділяється практичним прикладам збору інформації у конкурентному середовищі.	0,2
Тема 2. Організація системи промислового та офісного шпіонажу та інформаційно-аналітична діяльність. Досліджується структура та етапи створення системи промислового й офісного шпіонажу на підприємстві, а також роль аналітичних процесів у формуванні інтегрованого банку даних служби безпеки. Аналізуються принципи побудови інформаційної системи безпеки та способи використання розвідувальної інформації.	0,2
Загалом	$\sum_{i=1}^{m} b_i$=0,4

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Етичні та правові аспекти промислового та офісного шпіонажу.. Аналіз законодавчих обмежень і наслідків порушення норм ділової етики при зборі інформації.	8
Тема 2. Протидія промисловому шпіонажу на підприємстві. Методи виявлення, попередження та нейтралізації спроб збору конфіденційної інформації.	8
Тема 3. Використання соціальної інженерії у шпіонажі. Прийоми маніпуляції людьми для отримання даних, приклади атак через людський фактор.	8
Тема 4. Кіберрозвідка та інформаційні технології в шпіонажі. Роль сучасних IT-засобів, мережевого моніторингу та OSINT у промисловій розвідці.	8
Тема 5. Аналіз конкурентного середовища підприємства.. Методи оцінки конкурентів, стратегічної інформації та прогнозування їх дій.	8
Тема 6. Психологічні аспекти вербування інформаторів. Мотиваційні фактори, техніки впливу та побудови довіри при вербуванні.	8
Тема 7. Технології прихованого спостереження та контрспостереження. Сучасні технічні засоби фіксації інформації, правила їх застосування та виявлення.	8
Тема 8. Інформаційна безпека в офісному середовищі. Захист внутрішньої документації, електронних листів, переговорів та робочих пристроїв.	8
Тема 9. Міжнародний досвід боротьби з промисловим шпіонажем.	8

Підходи провідних країн до запобігання інформаційним витокам у бізнесі.	
Тема 10. Розробка політики безпеки підприємства проти шпіонажу. Формування внутрішніх регламентів, навчання персоналу, впровадження технічних заходів контролю.	8
Загальна кількість годин	**80**

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

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Концепція технічного захисту інформації в Україні. Постанова КМУ №1126 від 08.10.1997. https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF#Text
2. Шкільняк М.М, Овсянюк-Бердадіна О.Ф., Крисько Ж.Л., Демків І.О. Менеджмент: навчальний посібник. – Тернопіль: Крок, 2017. – 252 с. http://dspace.wunu.edu.ua/bitstream/316497/31710/1/%D0%9C%D0%B5%D0%BD%D0%B5%D0%B4%D0%B6%D0%BC%D0%B5%D0%BD%D1%82%20%D0%A8%D0%BA%D1%96%D0%BB%D1%8C%D0%BD%D1%8F%D0%BA.pdf
3. Стахова М.В., Малик О.В. Конкурентний потенціал як основа формування конкурентоспроможності підприємства / М.В. Стахова, О.В. Малик // Економіка та управління підприємством. 2017. №16. - С. 468–473. http://global-national.in.ua/issue-16-2017/24-vipusk-16-kviten-2017-r/2962-stakhova-m-v-malik-o-v-konkurentnij-potentsial-yak-osnova-formuvannya-konkurentospromozhnosti-pidpriemstva
4. Управління конкурентоспроможністю підприємства: підручник / Ю.Б. Іванов, М.О. Кизим, О.М. Тищенко, О.Ю. Іванова, О.В. Ревенко , Т.М. Чечетова-Терашвілі. Харків: ВД «ІНЖЕК», 2010. 320 с. https://ndc-ipr.org/media/ndc_old/documents/Tishtnrj-Kizim-Pidryz.pdf
5. Meloan T. International and Global Marketing / T. Meloan, J. Graham. – 2th ed. – 2000. – 439 p. https://archive.logos-science.com/index.php/conference-proceedings/article/view/1714

Додаткова література

6. National Institute of Standards and Technology Special Publication 800-100, Information Security Handbook: A Guide for Managers. Recommendations of the National Institute of Standards and Technology, October 2006. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-100.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
0,6	0,4		

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** Андрій ТКАЧОВ