Силабус курсу

Ітелектуальна безпека

Ступінь вищої освіти – магістр

Галузь знань «Цивільна безпека»
Спеціальність «Правоохоронна діяльність»
Освітньо-професійна програма «Правоохоронна діяльність»

Дні занять:
Консультації:

Рік навчання: 1, Семестр: 2

Кількість кредитів: 4 Мова викладання: українська

Керівник курсу

к.е.н., доцент, доцент кафедри

Муравська Юлія Євгенівна

Контактна інформація yakubivskay@gmail.com, +380970134613

Опис дисципліни

«Інтелектуальна безпека» є дисципліною, яка сприяє підготовці фахівців у сфері правоохоронної діяльності та економічної безпеки. Дисципліна «Інтелектуальна безпека» вивчає закономірності та організаційно-економічні механізми побудови й відтворення стану безпечного, захищеного розвитку сфери інтелектуальної власності на рівні держави і окремих суб'єктів господарювання.
Одержані теоретичні знання дадуть змогу студентам та слухачам у майбутньому як фахівцям у сфері правоохоронної діяльності вміти вирішувати такі завдання: ідентифікувати внутрішні та зовнішні загрози, виявляти ризики інтелектуальної безпеки на рівні держави; прогнозувати наслідки реалізації загроз / ризиків для національної економіки; обґрунтовувати напрями подолання загроз та нейтралізації ризиків національної економічної безпеки в сфері інтелектуальної власності; розробляти механізми узгодження інтересів суб'єктів відносин інтелектуальної власності, заходи з убезпечення інтелектуальної власності при міжнародному науково-технічному співробітництві, запобігання промисловому шпигунству; виявляти потенційні шляхи втрати об'єктів інтелектуальної власності підприємства; враховувати специфіку управління безпекою за фазами життєвого циклу об'єктів інтелектуальної власності; розробляти та координувати заходи з попередження та нейтралізації опортуністичної поведінки працівників, визначати та застосовувати інструменти закріплення і збереження на підприємстві інтерспецифічних інтелектуальних трудових ресурсів; виявляти ознаки ведення конкурентної розвідки щодо підприємства, застосовувати систему раннього конкурентного попередження; ідентифікувати відомості, що складають комерційну таємницю; розробляти систему заходів щодо захисту комерційної таємниці; приймати рішення щодо доцільності укладення договору про конфіденційність.

Структура курсу

Години (лек. / сем.)	Тема	Результати навчання	Завдання
2 / 1	1.Інтелектуальна безпека в системі національної економічної безпеки	Визначення поняття формування системи інтелектуальної безпеки в контексті національної безпеки	Питання для обговорення
2 / 1	2. Об’єкти та суб’єкти системи інтелектуальної безпеки	Засвоїти та закріпити теоретичні знання щодо питання сутності інституту інтелектуальної власності в системі інтелектуальної безпеки	Тести, питання
4 / 2	3. Авторське право в системі захисту від інтелектуальної безпеки	Засвоїти та закріпити теоретичні знання щодо питання сутності авторського права в системі інтелектуальної безпеки	Тести, задачі, питання
4 / 2	4. Правова охорона об’єктів промислової власності. Патентне право як механізм інтелектуальної безпеки	Засвоїти та закріпити теоретичні знання щодо питання сутності патентного права в системі інтелектуальної безпеки	Тести, задачі, питання
4 / 2	5. Правова охорона засобів індивідуалізації учасників цивільного обороту, товарів і послуг як механізм інтелектуальної безпеки	Навчитися досліджувати охорону засобів індивідуалізації учасників цивільного обороту, товарів і послуг	Тести, задачі, питання
2 / 1	6. Передача прав на об'єкти інтелектуальної власності як	Глибше засвоїти та закріпити теоретичні знання щодо питання передачі прав на об'єкти інтелектуальної власності як напрямку інтелектуальної безпеки	Тести, питання

	напрямок формування системи інтелектуальної безпеки		
2 / 1	7. Захист прав інтелектуальної власності як складова системи попередження інтелектуальної безпеки	Ознайомлення з особливостями захисту прав інтелектуальної власності як складової системи інтелектуальної безпеки	Тести, питання
4 / 2	8.Відповідальність за порушення законодавства про комерційну таємницю та прояви недобросовісної конкуренції	Вивчення особливостей несення відповідальності за порушення законодавства про комерційну таємницю	Тести, кейси
2 / 1	9. Технічний захист інформації як елемент інтелектуальної безпеки	Характеристика технічного захисту інформаційних об’єктів.	Тести, питання
2 / 1	10. Загрози та ризики для національної економічної безпеки в сфері інтелектуальної власності	Характеристика показників оцінки інтелектуальної безпеки.	Тести, питання
2 / 1	11.Інтелектуальна безпека підприємства	Набуття практичних навичок з планування системи захисту службою безпеки підприємства	Тести, питання
2 / 1	12. Промислове шпигунство і конкурентна	Характеристика методів та форм шпигунства та конкурентної розвідки	Тести, задачі, питання

	розвідка як загрози інтелектуальній безпеці		
2 / 1	13. Збір інформації з закритих джерел	Вивчення питань безпеки об’єктів права інтелектуальної власності в контексті технічного захисту інформаційних об’єктів інтелектуальної безпеки	Питання
2 / 1	14. Страхування об’єктів інтелектуальної власності як передумова формування ефективної системи інтелектуальної безпеки	Дослідження процесу страхування інтелектуальної власності	Кейси
2 / 1	15. Безпека інтелектуальних трудових ресурсів підприємства та руху знань як елемент інтелектуальної безпеки	Дослідження системи формування інтелектуальніх трудових іресурсів.	Тести, питання

Літературні джерела

1. Muravska Yuliia. Theoretical and conceptual approaches to defining the concept and forms of economic intelligence.in the Ukrainian scientific practice. Osteuropa-Recht. 2022. Vol. 4. P. 476-485.
2. Муравська Ю. Побудова ефективної системи національної безпеки України як передумова євроінтеграції. Наукові заходи Юридичного факультету Західноукраїнського національного університету. 2022: Пріоритети зміцнення безпеки держави та підвищення ефективності правоохоронної діяльності: національні та міжнародні контексти (Тернопіль, 6 травня 2022 р.) http://confuf.wunu.edu.ua/index.php/confuf/article/view/829
3. Муравська Ю. Поняття та сутність економічної розвідки в контексті її відмінності від бізнес-аналітики. Російсько-українська війна: право, безпека, світ [Матеріали V Міжнародної науково-практичної конференції, м. Тернопіль, Західноукраїнський національний університет, 29-30 квітня 2022 р.]. Тернопіль: ЗУНУ, 2022. С. 245-248.
4. Муравська (Якубівська) Ю. Є. Інформаційна безпека суспільства: концептуальний аналіз / Ю. Є.

Муравська (Якубівська) // Економіка та суспільство [Електронне наукове фахове видання]. - № 9. – Мукачево : Мукачівський державний університет, 2017. Режим доступу: http://www.economyandsociety.in.ua/
DSPACE: http://dspace.tneu.edu.ua/handle/316497/19378
5. Мельник В. Конкурентна розвідка та промислове шпигунство як засоби конкурентної боротьби / Вікторія Мельник, Ірина Кисельова, Марина Пучкова // Інноваційне підприємництво: стан та перспективи розвитку [Електронний ресурс] : зб. матеріалів II Всеукр. наук.-практ. конф., 29–30 берез. 2017 р. / М-во освіти і науки України, ДВНЗ «Київ. нац. екон. ун-т ім. В. Гетьмана» [та ін.] ; оргком.: Г. О. Швиданенко (голова) [та ін.]. – Електрон. текст. дані. – Київ : КНЕУ, 2017. – С. 84–87. – Назва з титул. екрану.
DSPACE: http://dspace.tneu.edu.ua/handle/316497/19381
6. Муравська (Якубівська) Ю. Є. Формування понятійного апарату у сфері кібербезпеки: іноземний досвід та нормативно-правова регламентація / Ю. Є. Муравська (Якубівська) // Україна в умовах реформування правової системи: сучасні реалії та міжнародний досвід: [Матеріали II Міжнародній науково-практичній конференції, м. Тернопіль, 21-22 квітня 2017 р.]. – Тернопіль: Економічна думка, 2017. – С.362-365.
DSPACE: http://dspace.tneu.edu.ua/handle/316497/19380

7. Муравська (Якубівська) Ю. Є. Термінологічна та нормативно-правова невизначеність у сфері кібербезпеки / Ю. Є. Муравська (Якубівська) // Збірник тез доповідей всеукраїнської науково-практичної конференції «Тактичні та стратегічні пріоритети зміцнення фінансово-економічної безпеки держави», м. Тернопіль, 21 квітня 2017 р., ТНЕУ. – Тернопіль, 2017. – С. 56-59.

DSPACE: http://dspace.tneu.edu.ua/handle/316497/24969
8 Карапетян О.М., Будник Л.А., Метельський І.Д. Кіберзлочини: типології, фінансова розвідка, використання спеціальних знань. Актуальні проблеми правознавства. 2022. Вип. 3. С. 115-120.
1. Москаленко Н.В. Теоретичні аспекти запровадження комплаєнсконтролю в Україні. Економічний вісник серія: фінанси, облік, оподаткування. УДФСУ. 2018. Вип. №2. С. 106-113
2. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII. Верховна Рада України. Відомості Верховної Ради України. 2017. № 45. Ст. 403
11. Barrachina, Alex and Tauman, Yair. 2014. Entry and espionage with noisy signals: Games and economic behavior: Elsevier, N 83, p. 127-146.
12. Charkiewicz, Szymon i Chmura, Aneta. 2008. Znaki towarowe w działalności małych i średnich przedsiębiorstw. Warszawa: Urząd patentowy Rzeczpospolitej Polskiej. (40 s.).
13. Chmielarz, Wojciech.2011. Szpiegostwo przemysłowe: duży zysk, niskie kary: Niwserwis : <http://niwserwis.pl/artykuly/szpiegostwo-przemyslowe-duzy-zysk-niskie-kary>
14. Ciecierski, Marek. 2019. Szpiegostwo przemysłowe opanowało cyberprzestrzeń: InteriaBiznes:<http://biznes.interia.pl/wiadomosci/news/szpiegostwo-przemyslowe-opanowalo-cyberprzestrzen,1885978,4199>
15. Ciecierski, Marek. 2018. Wkroczyliśmy w erę wywiadu gospodarczego : InteriaBiznes: <http://praca.interia.pl/news-wkroczylismy-w-ere-wywiadu-gospodarczego,nId,723996>

16. Commission proposes rules to help protect against the theft of confidential business information : European Commission, Press release: Brussels, 28 November 2013 : <http://europa.eu/rapid/press-release_IP-13-1176_en.htm>
17. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:157:0045:0086:EN:PDF >
18. Dyrektywa 2005/29/WE Parlamentu Europejskiego i Rady z dnia 11 maja 2005 r. o nieuczciwych praktykach handlowych dotycząca nieuczciwych praktyk handlowych stosowanych przez przedsiębiorstwa wobec konsumentów na rynku wewnętrznym oraz zmieniająca inne dyrektywy, Dz. Urz. UE L z 2005 r. Nr 149, s. 22.
19. Elliott, Sharon Mollman . 2007. The threat from within: trade secret theft by employees: Patents, Nature Publishing Group: Wisconsin, Vol. 25, N 3, p. 293-295.
20. Everett, Bernet. 2013. Optically transparent: the rise of industrial espionage and statesponsored hacking: Feature, InfoGuard, p. 13-17.
21. Glenny, Misha and Kavanagh, Camino. 2012. 800 Titles but No Policy—Thoughts on Cyber Warfare. American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy: NCAFP, p. 287-294.
22. Hare, Forrest and Goldstein, Jnathan. 2010. The independent security problem in the defense industrial base: An agent-based model on a social network: Critical infrastructure protection, Elsevier, ScienceDirect, N 3, p. 128-139.
23.Kaczmarek, Jarosław i Kwieciński, Mirosław. 2010. Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu. Toruń : Towarzystwo Naukowe Organizacji i Kierownictwa "Dom Organizatora. (313 s.)
24. Lee, Chang-Moo. 2014. The Strategic Measures for the Industrial Security of Small and Medium Business: Hindawi Publishing Corporation, Scientific World Journal, p. 1-4.
25. Ludziejewski, Zdzisław. 2013. Bezpieczeństwo informacyjne w instytucjach gospodarczych. Zeszyty naukowe WSOWL, nr. 4 (170), s. 5-58.
26. Miller, Lesley Ellis. 1999. Innovation and Industrial Espionage in Eighteenth-Century France: An Investigation of the Selling of Silks through Samples: Journal of Design History, Vol. 12, No. 3, p. 271-292.
27. Minott, Nathaniel. 2018. The Economic Espionage Act: is the law all bark and no bite? : Information & Communications Technology Law: Routledge, Vol. 20, No. 3, October 2011, p. 201–224.
28. Morris, Mel. 2010. Intelligence, knowledge and organised crime: Computer Fraud & Security: CEO, Prevx, p. 13-15.
29. CcCallion, Jane. 2013. New EU rules on industrial espionage issued: ITPro : <http://www.itpro.co.uk/hacking/20163/new-eu-rules-industrial-espionage-issued>
30. Rid, Thomas and McBurney, Peter. 2012. Cyber-Weapons:The RUSI Journal, p. 6-13.
31. Rosenfeld, Steven. 2019. Corporate Espionage Tactics Used Against Leading Progressive Groups, Activists and Whistleblowers: Alternet: <http://www.alternet.org/activism/corporate-espionage-against-progressive-nonprofits>

32. Turaliński, Kazimierz. 2018. Wywiad gospodarczy i polityczny. metodyka, taktyka i źródła pozyskiwania. Radom: "Media Polskie". (446 s.).

Політика оцінювання

- **Політика щодо дедлайнів та перескладання**: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-20 балів). Перескладання модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).
- **Політика щодо академічної доброчесності**: Усі письмові роботи перевіряються на наявність плагіату і допускаються до захисту із коректними текстовими запозиченнями не більше 20%. Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних пристроїв). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування (наприклад, програма Kahoot).
- **Політика щодо відвідування**: Відвідування занять є обов'язковим компонентом оцінювання, за яке нараховуються бали. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.

Оцінювання

Остаточна оцінка за курс розраховується наступним чином:

Види оцінювання	% від остаточної оцінки
Опитування під час занять – усно	20
Модуль 1 (теми 1-6) – обговорення кейсів	20
Модуль 2 (теми 7-12) – обговорення кейсів	20
Залік (теми 1-12) – завдання, кейси	40

Шкала оцінювання студентів:

ECTS	Бали	Зміст
A	90-100	відмінно
B	85-89	добре
C	75-84	добре
D	65-74	задовільно
E	60-64	достатньо
FX	35-59	незадовільно з можливістю повторного складання
F	1-34	незадовільно з обов'язковим повторним курсом